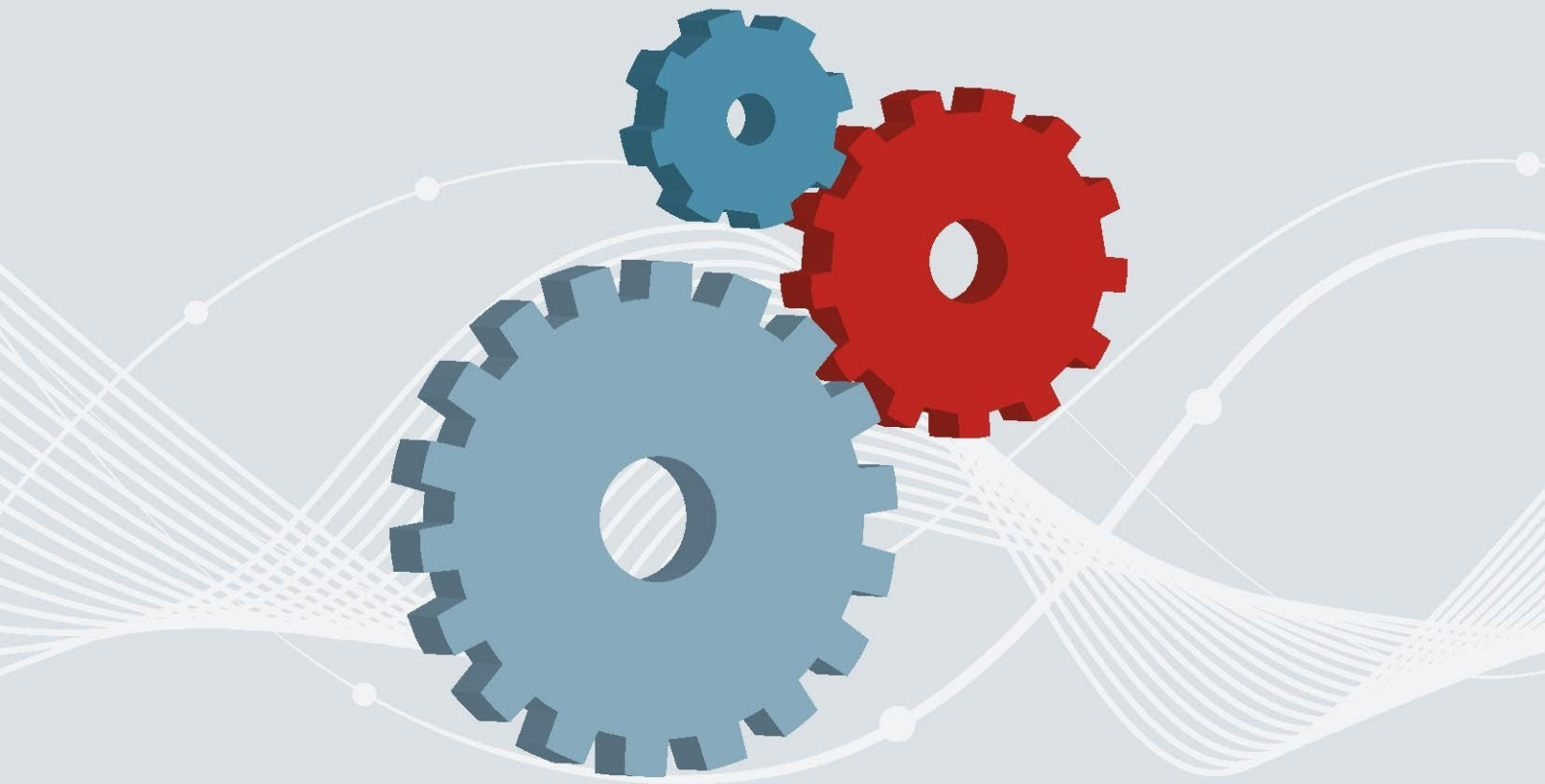
Bundesamt
für Sicherheit in der
Informationstechnik



Umsetzungshinweise zum IT-Grundschutz-Kompendium 2019

Final Draft

Inhaltsverzeichnis

Bundesamt
für Sicherheit in der
Informationstechnik

Umsetzungshinweise für die Bausteinschicht ISMS

ISMS.1 Sicherheitsmanagement **5**

IT-Grundschutz

Umsetzungshinweise zum Baustein ISMS.1 Sicherheitsmanagement

1 Beschreibung

1.1 Einleitung

Die sichere Verarbeitung von Informationen ist für nahezu alle Unternehmen und Behörden von existenzieller Bedeutung. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. Für den Schutz der Informationen reicht es nicht aus, nur technische Sicherheitslösungen einzusetzen. Ein angemessenes Sicherheitsniveau kann nur durch geplantes und organisiertes Vorgehen aller Beteiligten erreicht und aufrechterhalten werden. Voraussetzung für die sinnvolle Umsetzung und Erfolgskontrolle von Sicherheitsmaßnahmen ist eine systematische Vorgehensweise. Diese Planungs-, Lenkungs- und Kontrollaufgabe wird als Informationssicherheitsmanagement oder auch kurz als IS-Management oder Sicherheitsmanagement bezeichnet.

Ein funktionierendes Sicherheitsmanagement muss in die existierenden Managementstrukturen einer jeden Institution eingebettet werden. Daher ist es praktisch nicht möglich, eine für jede Institution unmittelbar anwendbare Organisationsstruktur für das Sicherheitsmanagement anzugeben. Vielmehr werden häufig Anpassungen an spezifische Gegebenheiten erforderlich sein.

1.2 Lebenszyklus

Im Rahmen des Sicherheitsmanagements sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über den Aufbau geeigneter Organisationsstrukturen bis hin zur regelmäßigen Revision. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt. Einer der Grundpfeiler zur Erreichung eines angemessenen Sicherheitsniveaus ist, dass die Leitungsebene hinter den Sicherheitszielen steht und sich ihrer Verantwortung für Informationssicherheit bewusst ist. Die Leitungsebene muss den Sicherheitsprozess initiieren, steuern und kontrollieren, damit dieser in der Institution auch in allen Bereichen umgesetzt wird (siehe ISMS.1.M1 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene).

Weiterhin muss ein kontinuierlicher Sicherheitsprozess etabliert und eine für die jeweilige Institution passende Sicherheitsstrategie festgelegt werden (siehe ISMS.1.M2 Festlegung der Sicherheitsziele und -strategie). Die Leitungsebene muss hierfür wie für alle weiteren Sicherheitsfragen eine Person als Hauptverantwortlichen benennen (siehe ISMS.1.M4 Benennung eines Informationssicherheitsbeauftragten). Diese ist dafür zuständig, eine geeignete Organisationsstruktur für Informationssicherheit aufzubauen und aufrechtzuerhalten (siehe ISMS.1.M6 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit). Als eine der ersten Aktionen sollte eine Leitlinie zur Informationssicherheit erstellt werden (siehe ISMS.1.M3 Erstellung einer Leitlinie zur Informationssicherheit).

Informationssicherheit muss in allen Bereichen der Institution gelebt werden (siehe ISMS.1.M9 Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse). Dazu gehört neben der Erarbeitung eines Sicherheitskonzepts (siehe ISMS.1.M10 Erstellung eines Sicherheitskonzepts) auch die Integration der Mitarbeiter in den Sicherheitsprozess (siehe ISMS.1.M8 Integration der Mitarbeiter in den Sicherheitsprozess) sowie die Erstellung von zielgruppengerechten Sicherheitsrichtlinien (siehe ISMS.1.M16 Erstellung von zielgruppengerechten Sicherheitsrichtlinien).

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Sicherheitsmanagement" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

ISMS.1.M1 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene [Institutionsleitung]

Die Führung und Lenkung eines Unternehmens oder einer Behörde und die damit verbundenen Leitungsaufgaben beinhalten eine hohe Verantwortung. Diese Verantwortung bezieht sich nicht nur auf den Grad der Zielerreichung wie beispielsweise den Geschäftserfolg, sondern auch auf die Früherkennung und Minimierung von möglichen Risiken für den Betrieb. Dazu gehören neben anderen Risiken auch solche, die aus unzureichender Informationssicherheit entstehen.

Es ist eine komplexe Aufgabe, dauerhaft ein angemessenes Sicherheitsniveau zu gewährleisten. Dies erfordert ein systematisches Vorgehen, einen kontinuierlichen und zielgerichteten Sicherheitsprozess. Es ist Aufgabe der Leitungsebene jeder Institution, diesen Prozess zu initiieren, zu steuern und zu kontrollieren. Bei kleineren Institutionen wird dies häufig durch ein Mitglied der Leitungsebene persönlich übernommen. In mittleren und großen Institutionen wird die Aufgabe "Informationssicherheit" an eine dedizierte Person, den Informationssicherheitsbeauftragten, delegiert. Je nach Größe und Art der Institution werden noch weitere Personen mit Sicherheitsaufgaben betraut, die diese ausschließlich oder zusätzlich zu anderen Aufgaben wahrnehmen. Dabei verbleibt die Gesamtverantwortung immer bei der Leitungsebene, unabhängig davon, an wie viele Personen Sicherheitsaufgaben delegiert wurden.

Die Geschäftsführung muss regelmäßig über mögliche Risiken und Konsequenzen aufgrund fehlender Informationssicherheit aufgeklärt werden. Dazu ist es empfehlenswert, die Leitungsebene auf folgende Punkte aufmerksam zu machen:

- Darstellung der Sicherheitsrisiken und der damit verbundenen Auswirkungen und Kosten
- Auswirkungen von Sicherheitsvorfällen auf die kritischen Geschäftsprozesse
- Gesetzliche und vertragliche Sicherheitsanforderungen
- Übersicht über Standard-Vorgehensweisen zur Informationssicherheit für die Branche

Auch wenn die Leitungsebene für die Erreichung der Sicherheitsziele verantwortlich ist, muss der Sicherheitsprozess von allen Beschäftigten in einer Institution mitgetragen und mitgestaltet werden. Daher sollten folgende Prinzipien eingehalten werden:

- Übernahme der Gesamtverantwortung für Informationssicherheit
  Die Initiative für Informationssicherheit geht von der Behörden- bzw. Unternehmensleitung aus. Die Aufgabe "Informationssicherheit" wird durch die Behörden- bzw. Unternehmensleitung aktiv unterstützt.

- Informationssicherheit integrieren
  Informationssicherheit muss in alle Prozesse und Projekte integriert werden. Darüber hinaus müssen alle Beteiligten über den Sicherheitsprozess ausreichend informiert und motiviert werden, damit sie diesen auch einhalten.

- Zuständigkeiten definieren
  Die Behörden- bzw. Unternehmensleitung benennt die für Informationssicherheit zuständigen Mitarbeiter und stattet sie mit den erforderlichen Kompetenzen und Ressourcen aus.

- Lenken und Überwachen
  Die Leitungsebene muss aktiv den Sicherheitsprozess initiieren, lenken und überwachen. Dazu muss das Management die Auswirkungen von Sicherheitsvorfällen auf die Geschäftstätigkeit kennen, Sicherheitsziele vorgeben und Rahmenbedingungen schaffen, die es ermöglichen, diese Ziele zu erreichen.

- Angemessene Ziele setzen
  Absolute Informationssicherheit gibt es nicht. Deswegen ist es wichtig, die Sicherheitsziele so zu setzen, dass sie einerseits mit einem vertretbaren Aufwand (Personal, Zeit, Finanzmittel) erreichbar sind und andererseits die Sicherheitsrisiken auf ein akzeptables Maß reduziert werden.

- Vorbildfunktion
  Die Leitungsebene übernimmt auch im Bereich Informationssicherheit eine Vorbildfunktion. Dazu gehört unter anderem, dass auch die Leitungsebene alle vorgegebenen Sicherheitsregeln beachtet. Die Leitungsebene muss Informationssicherheit vorleben.

- Kontinuierliche Verbesserung
  Die Angemessenheit und Wirksamkeit aller Elemente des Sicherheitsmanagements muss ständig überprüft werden. Identifizierte Schwachstellen und Verbesserungsmöglichkeiten müssen konsequent behoben bzw. umgesetzt werden. Wichtig ist auch, zukünftige Entwicklungen, veränderte Rahmenbedingungen und potentielle Gefährdungen frühzeitig zu erkennen.

- Kommunikation und Wissen
  Die Leitungsebene und das IS-Management-Team müssen die Mitarbeiter motivieren und für ausreichende Schulungs- und Sensibilisierungsmaßnahmen sorgen. Mitarbeiter müssen vor allem über Sinn und Zweck sowohl von technischen Sicherheitsmaßnahmen als auch von organisatorischen Vorgaben aufgeklärt werden. Anwender sollten in die Umsetzungsplanung von Maßnahmen mit einbezogen werden. Damit können sie Ideen einbringen und die Praxistauglichkeit von Sicherheitsmaßnahmen beurteilen.

ISMS.1.M2 Festlegung der Sicherheitsziele und -strategie [Institutionsleitung]

Informationssicherheit ist ein wichtiger Erfolgsfaktor, um die Ziele und Aufgaben eines Unternehmens bzw. einer Behörde erfüllen zu können. Informationssicherheit ist kein einmaliges Projekt, sondern ein kontinuierlicher Prozess, der auch als solcher in allen Geschäftsprozessen und den Köpfen aller Mitarbeiter verankert werden muss. Der Sicherheitsprozess muss durch die Behörden- bzw. Unternehmensleitung initiiert, etabliert und kontrolliert werden. Zunächst müssen angemessene Sicherheitsziele sowie eine Strategie für Informationssicherheit festgelegt werden. Neben den strategischen Leitaussagen müssen konzeptionelle Vorgaben erarbeitet und die organisatorischen Rahmenbedingungen geschaffen werden, um den ordnungsgemäßen und sicheren Umgang mit Informationen innerhalb aller Geschäftsprozesse des Unternehmens oder der Behörde zu ermöglichen.

Die Sicherheitsziele sollten zu Beginn jedes Sicherheitsprozesses sorgfältig bestimmt werden. Anderenfalls besteht die Gefahr, dass Sicherheitskonzepte erarbeitet werden, die nicht den Informationssicherheitsanforderungen der Behörde bzw. des Unternehmens entsprechen. Die methodische Planung der Informationssicherheit hilft, die grundlegenden Ziele und Aufgaben eines Unternehmens bzw. einer Behörde zu erreichen. Die Grundlage für die Definition der Sicherheitsziele bilden daher die generellen Ziele der Institution sowie die wesentlichen Geschäftsprozesse und Informationen. Angemessene und erreichbare Sicherheitsziele sind Voraussetzung für alle weiteren Schritte im Sicherheitsprozess. Die Ziele müssen realistisch, praxisorientiert, überzeugend und verständlich sein. Hieraus lässt sich dann im Rahmen der Sicherheitskonzeption ableiten, welchen Schutzbedarf die einzelnen Informationen, Geschäftsprozesse, Anwendungen, IT-Komponenten und Netze haben und welche Sicherheitsmaßnahmen daher umzusetzen sind.

Bei der Umsetzung von Sicherheitsmaßnahmen muss in der Regel immer ein Kompromiss zwischen Kosten und Aufwand gefunden werden. Es sollte daher transparent sein, welche Informationen und Geschäftsprozesse zur Aufgabenerfüllung beitragen und welcher Wert diesen beigemessen wird, um daraus angemessene Sicherheitsziele zu formulieren.

Die Sicherheitsziele müssen von der Unternehmens- oder Behördenleitung getragen und verantwortet werden. Sie sollten vom Informationssicherheitsmanagement-Team unter Beteiligung der Leitungsebene erarbeitet und dokumentiert werden. Je nach Organisationsstruktur ist es ratsam, die Leiter von größeren Geschäftsbereichen (z. B. Abteilungsleiter oder Bereichsleiter) in die Beratungen einzubeziehen.

Eine detaillierte Beschreibung, wie und in welcher Beschreibungstiefe Sicherheitsstrategie und -ziele festgehalten werden sollten, findet sich im BSI-Standard 100-2 Vorgehensweise nach IT-Grundschutz.

Sicherheitsziele und -strategie müssen regelmäßig daraufhin beleuchtet werden, ob sie noch aktuell und angemessen sind. Insbesondere bei Änderungen von Rahmenbedingungen, von Geschäftsprozessen oder des IT-Umfeldes müssen die Sicherheitsziele und -strategie überprüft und eventuell angepasst werden.

Der Sicherheitsprozess kann nur dann langfristig erfolgreich sein, wenn die Wirksamkeit und Effizienz der Sicherheitsstrategie regelmäßig von der Leitungsebene überprüft wird. Die daraus resultierenden Verbesserungen gehen in die Anpassung des Sicherheitsprozesses ein.

ISMS.1.M3 Erstellung einer Leitlinie zur Informationssicherheit [Institutionsleitung]

Die Leitaussagen zur Sicherheitsstrategie müssen in einer Leitlinie zur Informationssicherheit zusammengefasst werden, um die zu verfolgenden Sicherheitsziele und das angestrebte Sicherheitsniveau für alle Mitarbeiter zu dokumentieren. Mit der Sicherheitsleitlinie bekennt sich die Behörden- bzw. Unternehmensleitung sichtbar zu ihrer Verantwortung für Informationssicherheit.

Bei der Erstellung der Leitlinie zur Informationssicherheit müssen folgende Punkte beachtet werden:

Verantwortung der Behörden- bzw. Unternehmensleitung

Wichtig ist, dass die Behörden- bzw. Unternehmensleitung in vollem Umfang hinter der Leitlinie zur Informationssicherheit und den darin festgehaltenen Zielen steht. Daher muss die Sicherheitsleitlinie von der Behörden- bzw. Unternehmensleitung unterschrieben und in deren Namen veröffentlicht werden. Selbst wenn einzelne Aufgaben im Rahmen des Sicherheitsprozesses an Personen oder Organisationseinheiten delegiert werden, verbleibt die Gesamtverantwortung für die Informationssicherheit immer bei der Behörden- bzw. Unternehmensleitung.

Festlegung des Geltungsbereichs

In der Informationssicherheitsleitlinie muss beschrieben werden, für welche Bereiche diese gelten soll. Der Geltungsbereich kann die gesamte Institution umfassen oder aus Teilbereichen dieser bestehen. Wichtig ist jedoch, dass die betrachteten Fachaufgaben und Geschäftsprozesse im Geltungsbereich komplett enthalten sind.

Festlegung von Sicherheitszielen

Zu Beginn des Sicherheitsprozesses muss die Behörden- bzw. Unternehmensleitung die Sicherheitsziele festlegen, abstimmen und dokumentieren. Diese lassen sich aus den Geschäftsprozessen und Fachaufgaben, gesetzlichen Rahmenbedingungen und allgemeinen Behörden- oder Unternehmenszielen ableiten. Die Sicherheitsziele dienen als Grundlage für die Erstellung der Leitlinie zur Informationssicherheit.

Inhalt der Sicherheitsleitlinie

Die Leitlinie zur Informationssicherheit sollte kurz und bündig formuliert sein, da sich mehr als 20 Seiten in der Praxis nicht bewährt haben. Sie sollte dabei aber mindestens die folgenden Aspekte enthalten:

- Der Stellenwert der Informationssicherheit und die Bedeutung der wesentlichen Informationen, Geschäftsprozesse und IT für die Institution müssen dargestellt werden.
- Die Sicherheitsziele und der Bezug der Sicherheitsziele zu den Geschäftszielen und Aufgaben der Institution müssen dabei erläutert werden.
- Die Kernelemente der Sicherheitsstrategie sollten genannt werden.
- Die Leitungsebene muss allen Mitarbeitern aufzeigen, dass die Sicherheitsleitlinie von ihr getragen und durchgesetzt wird. Ebenso muss es Leitaussagen zur Erfolgskontrolle geben.
- Die für die Umsetzung des Sicherheitsprozesses etablierte Organisationsstruktur muss beschrieben werden.

Bekanntgabe der Leitlinie zur Informationssicherheit

Sicherheitsmaßnahmen und organisatorische Regelungen werden erfahrungsgemäß nur dann von allen Mitarbeitern befolgt, wenn diese ihren Sinn erkennen. Die Sicherheitsleitlinie muss daher veröffentlicht werden, um die Strategie des verantwortlichen Managements zu dokumentieren. Dies sollte so erfolgen, dass der Stellenwert der Informationssicherheit deutlich wird. Es ist wichtig, dass alle Mitarbeiter die Inhalte der Sicherheitsleitlinie kennen und nachvollziehen können. Neue Mitarbeiter sollten auf die Leitlinie zur Informationssicherheit hingewiesen werden, bevor sie Zugang zu geschäftsrelevanten Informationen erhalten. Müssen alle Mitarbeiter die Kenntnis der Sicherheitsleitlinie schriftlich bestätigen, wird deren Bedeutung unterstrichen. Generell sollte die Leitlinie zur Informationssicherheit so allgemein gehalten sein, dass sich alle Mitarbeiter aus den verschiedenen Organisationsbereichen einer Institution davon angesprochen fühlen. Es ist aber auch möglich, die Sicherheitsleitlinie für spezielle Anwendungen oder Bereiche innerhalb einer Institution um Inhalte zu ergänzen, die nur für einen eingeschränkten Personenkreis relevant oder die vertraulich sind. Es empfiehlt sich, diese Abschnitte in eine Anlage zur Leitlinie zu verlagern, um so flexibler und zeitnah auf erforderliche Änderungen reagieren zu können, ohne dass der allgemeine Teil der Leitlinie angepasst werden muss. Falls erforderlich, kann die Anlage separat als vertraulich gekennzeichnet und besonders geschützt werden.

Aktualisierung der Sicherheitsleitlinie

Die Leitlinie zur Informationssicherheit sollte in regelmäßigen Abständen auf ihre Aktualität hin überprüft und gegebenenfalls angepasst werden. Änderungen von Rahmenbedingungen, Geschäftszielen, Aufgaben oder der Sicherheitsstrategie sollten einfließen. Bei den häufig rasanten Entwicklungen sowohl im Bereich der IT als auch im Bereich der Sicherheit empfiehlt es sich, die Sicherheitsleitlinie alle zwei Jahre zu überarbeiten und allen Mitarbeitern erneut bekannt zu machen.

ISMS.1.M4 Benennung eines Informationssicherheitsbeauftragten [Institutionsleitung]

In jeder Institution, unabhängig von ihrer Größe, Art oder Branche muss eine Person als Informationssicherheitsbeauftragter benannt werden. Er ist für alle Belange der Informationssicherheit zuständig. Die Aufgaben des Informationssicherheitsbeauftragten sind unter anderem:

- den Informationssicherheitsprozess zu steuern und zu koordinieren,
- die Leitungsebene bei der Erstellung der Leitlinie zur Informationssicherheit zu unterstützen,
- die Erstellung des Sicherheitskonzepts, des Notfallvorsorgekonzepts und anderer Teilkonzepte und System-Sicherheitsrichtlinien zu koordinieren, sowie weitere Richtlinien und Regelungen zur Informationssicherheit zu erlassen,
- den Realisierungsplan für die Sicherheitsmaßnahmen zu erstellen und deren Realisierung zu initiieren und zu überprüfen,
- der Leitungsebene und dem IS-Management-Team über den Status Quo der Informationssicherheit zu berichten,
- sicherheitsrelevante Projekte zu koordinieren und den Informationsfluss zwischen Bereichs-IT-, Projekt- sowie IT-System-Sicherheitsbeauftragten sicherzustellen,
- sicherheitsrelevante Zwischenfälle zu untersuchen sowie
- Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit zu initiieren und zu steuern.

Der Informationssicherheitsbeauftragte muss bei allen größeren Projekten, die deutliche Auswirkungen auf die Informationsverarbeitung haben, sowie bei der Einführung neuer Anwendungen und IT-Systeme beteiligt werden, damit sichergestellt ist, dass sicherheitsrelevante Aspekte ausreichend beachtet werden. Dazu gehören z. B. die Beschaffung von IT-Systemen oder die Gestaltung von IT-gestützten Geschäftsprozessen.

Der Informationssicherheitsbeauftragte muss die Möglichkeit haben, bei Bedarf direkt an die Leitungsebene zu berichten. Um dies sicherzustellen, ist es empfehlenswert, diese Rolle als Stabsstelle einzurichten.

In kleinen Institutionen kann die Funktion des Informationssicherheitsbeauftragten auch von einem qualifizierten Mitarbeiter neben anderen Aufgaben wahrgenommen werden. Maßgeblich ist, dass dem Informationssicherheitsbeauftragten ausreichend Zeit für seine Aufgaben zugebilligt wird. Vor allem bei der erstmaligen Einrichtung des Sicherheitsprozesses müssen hierfür hinreichende zeitliche Ressourcen eingeplant werden. Auch muss schon bei der Planung der Informationssicherheitsorganisation ein qualifizierter Vertreter des Informationssicherheitsbeauftragten benannt werden.

Auswahl des Informationssicherheitsbeauftragten

Der Informationssicherheitsbeauftragte muss ausreichend qualifiziert sein und ausreichend Gelegenheit haben, sich fortzubilden. Er sollte Wissen und Erfahrung in den Gebieten Informationssicherheit und Informationstechnik besitzen. Weiterhin sollte er über die folgenden Qualifikationen und Eigenschaften verfügen:

- Überblick über Aufgaben und Ziele der Institution
- Identifikation mit den Zielsetzungen der Informationssicherheit
- Kooperations- und Teamfähigkeit (wenige andere Aufgaben erfordern so viel Fähigkeit und Geschick im Umgang mit anderen Personen)
- Fähigkeit zum selbstständigen Arbeiten
- Durchsetzungsvermögen
- Erfahrungen im Projektmanagement

ISMS.1.M5 Vertragsgestaltung bei Bestellung eines externen Informationssicherheitsbeauftragten [Institutionsleitung]

Falls ein externer Informationssicherheitsbeauftragter bestellt wird, sind die folgenden Hinweise zu beachten.

Insbesondere in kleinen Unternehmen oder Behörden kann es unter Umständen zweckmäßig sein, die Rolle des Informationssicherheitsbeauftragten nicht durch einen eigenen Mitarbeiter zu besetzen, sondern hierfür auf die Dienstleistung eines externen Informationssicherheitsbeauftragten zurückzugreifen. Hierzu muss zunächst ein geeigneter, qualifizierter Experte für Informationssicherheit ausgewählt werden. Hinweise zu den notwendigen Qualifikationen, zur Funktion und zu den Aufgaben eines Informationssicherheitsbeauftragten finden sich im BSI-Standard 100-2 sowie in der Maßnahme ISMS.1.M4 Benennung eines Informationssicherheitsbeauftragten.

Bevor ein externer Informationssicherheitsbeauftragter bestellt wird, ist zwischen dem Dienstleister und der eigenen Institution ein Vertrag zu schließen, in dem die Aufgaben des externen Informationssicherheitsbeauftragten sowie die gegenseitigen Rechte und Pflichten möglichst präzise geregelt werden müssen. Hierbei ist darauf zu achten, dass der Vertrag eine geeignete Vertraulichkeitsvereinbarung umfasst. Die Beauftragung eines externen Informationssicherheitsbeauftragten ist somit eine besondere Form des Outsourcings.

Folgende Aspekte sollten in dem Vertrag mindestens geregelt werden:

- Anforderungen an die Qualifikation des externen Informationssicherheitsbeauftragten
- Vertretungsregelungen und Mindest-Ressourcen
- Aufgaben, die der externe Informationssicherheitsbeauftragte übernehmen muss
- Melde-, Berichts- und Eskalationswege, Ansprechpartner (Rollen)
- Einbindung in Kommunikationskanäle der beauftragenden Institution
- Arbeitsorte, Räumlichkeiten und Anwesenheits- bzw. Erreichbarkeitszeiten
- Zutritts-, Zugangs- und Zugriffsrechte
- Vortragsrechte und Berichtspflichten gegenüber der Leitungsebene der beauftragenden Institution
- Mitwirkungspflichten des Auftraggebers
- Vertraulichkeitsvereinbarung
- Interessenskonflikte
- Folgen bei Vertragsverstößen
- Regelungen zur Beendigung des Vertragsverhältnisses, z. B. Übergabe von Aufgaben und Unterlagen
- Kosten

Durch den Vertrag muss der externe Informationssicherheitsbeauftragte in die Pflicht und in die Lage versetzt werden, seine Aufgaben mindestens so gut wie ein interner ISB zu erfüllen. Außerdem muss der Vertrag eine kontrollierte Beendigung des Vertragsverhältnisses einschließlich Übergabe der Aufgaben an den Auftraggeber ermöglichen.

Falls auf die Dienstleistung eines externen Informationssicherheitsbeauftragten zurückgegriffen wird, ist auch der Baustein OPS.2.1 Outsourcing-Nutzung anzuwenden. Zu beachten sind hier insbesondere die Regelungen für den Einsatz von Fremdpersonal.

ISMS.1.M6 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit [**Institutionsleitung**]

Im Folgenden werden die Aspekte beschrieben, die beim Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit zu berücksichtigen sind.

Planung und Einrichtung der Informationssicherheitsorganisation

Um einen Sicherheitsprozess erfolgreich planen und umsetzen sowie aufrechterhalten und kontinuierlich verbessern zu können, muss eine geeignete Organisationsstruktur für Informationssicherheit vorhanden sein. Es müssen also Rollen definiert sein, die die verschiedenen Aufgaben für die Erreichung der Sicherheitsziele wahrnehmen. Außerdem müssen Personen benannt sein, die qualifiziert sind und denen ausreichend Ressourcen zur Verfügung stehen, um diese Rollen auszufüllen.

Zu Beginn eines Sicherheitsprozesses kann sich herausstellen, dass innerhalb der Institution zwar bereits Verantwortliche für verschiedene Aspekte der Informationssicherheit benannt sind, es aber keine übergreifende Struktur für die Informationssicherheit gibt. In diesem Fall muss eine geeignete, übergreifende Organisationsstruktur für die Informationssicherheit aufgebaut werden.

Ist bereits eine IS-Organisation etabliert, sollte regelmäßig überlegt werden, ob diese noch angemessen ist oder an neue Rahmenbedingungen angepasst werden muss.

Funktion des Informationssicherheitsbeauftragten

Die Art und Ausprägung einer Informationssicherheitsorganisation hängt von der Größe, Beschaffenheit und Struktur der jeweiligen Institution ab. Die Funktion des Informationssicherheitsbeauftragten muss allerdings in jeder Institution eingerichtet werden, da er für alle Belange der Informationssicherheit zuständig ist. Es muss eine Person benannt werden, welche diese Rolle einnimmt. Es ist nicht erforderlich, dass hierfür eigens eine Stelle in der Institution geschaffen wird, da z. B. auch ein externer ISB beauftragt werden kann.

Ein Informationssicherheitsbeauftragter alleine kann nicht für angemessene Sicherheit in allen Bereichen einer Institution sorgen. Daher sind Kommunikations- und Präsentationsfähigkeiten wichtig. Die Leitungsebene muss in zentralen Fragen des Sicherheitsprozesses immer wieder eingebunden werden, außerdem müssen Entscheidungen eingefordert werden. Die Zusammenarbeit mit den Mitarbeitern ebenso wie mit Externen verlangt viel Geschick, da diese von der Notwendigkeit der (für sie manchmal etwas lästigen) Sicherheitsmaßnahmen überzeugt werden müssen. Mindestens genauso heikel ist die Befragung der Mitarbeiter nach sicherheitskritischen Vorkommnissen und Schwachstellen. Um bei diesen Befragungen verwertbare Ergebnisse zu erzielen, müssen die Mitarbeiter davon überzeugt sein, dass ehrliche Antworten nicht gegen sie selbst verwendet werden.

Aufbau eines Informationssicherheitsmanagement-Teams

In größeren Institutionen ist es sinnvoll, ein IS-Management-Team aufzubauen, das den Informationssicherheitsbeauftragten unterstützt und sämtliche übergreifende Belange der Informationssicherheit regelt und Pläne, Vorgaben und Richtlinien erarbeitet.

Die Größe und die Zusammenstellung des IS-Management-Teams sollten in Abhängigkeit vom Umfang des Sicherheitsprozesses und der dafür benötigten Ressourcen und Expertisen definiert werden. Im BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise sind verschiedene Varianten dargestellt, wie eine Aufbauorganisation des Informationssicherheitsmanagements aussehen kann.

Auswahl des IS-Management-Teams

Um die verschiedenen Sichten der Informationssicherheit in einer Institution zu berücksichtigen, sollten im IS-Management-Team folgende Vertreter zusammenarbeiten:

- Informationssicherheitsbeauftragter
- IT-Verantwortliche
- Vertreter der Anwender
- Datenschutzbeauftragte

Bei Bedarf sollten Vertreter der Revision, des Justiziariats, der Personalvertretung sowie der Leitungsebene der Institution hinzugezogen werden.

Benennung eines verantwortlichen Managers

Auf Leitungsebene sollte die Aufgabe Informationssicherheit eindeutig einem verantwortlichen Manager zugeordnet sein, an den der Informationssicherheitsbeauftragte direkt berichtet. In kleinen Institutionen kann auch ein Geschäftsführer diese Aufgabe übernehmen.

Definition von Zuständigkeiten (Funktionstrennung)

Zuständigkeiten und Kompetenzen innerhalb der Informationssicherheitsorganisation (oder kurz IS-Organisation) müssen klar definiert und zugewiesen werden. Für alle wichtigen Funktionen sind zudem Vertretungsregelungen sicherzustellen.

Festlegung von Kommunikationswegen

Kommunikationswege müssen geplant, beschrieben, eingerichtet und bekannt gemacht werden. Es muss für alle Aufgaben und Rollen festgelegt sein, wer wen informiert, wer bei welchen Aktionen informiert werden und in welchen Umfang dies geschehen muss.

Überprüfung der Informationssicherheitsorganisation

Eine einmal aufgebaute IS-Organisation ist nicht statisch. Geschäftsprozesse und Umfeldbedingungen ändern sich permanent, so dass auch die IS-Organisation immer wieder überdacht werden muss. Dabei sollte beispielsweise beleuchtet werden, ob die Aufgaben und Kompetenzen innerhalb des Sicherheitsprozesses ausreichend klar definiert waren, aber auch, ob vorgesehene Aufgaben wie geplant wahrgenommen werden konnten. Wichtig sind vor allem die folgenden Punkte:

- Überwachung von Verantwortlichkeiten im laufenden Betrieb
  Es muss regelmäßig überprüft werden, ob alle Verantwortlichkeiten und Zuständigkeiten eindeutig zugewiesen wurden und diese praxistauglich sind.
- Überprüfung der Einhaltung von Vorgaben
  Es muss regelmäßig geprüft werden, ob alle Prozesse und Abläufe der IS-Organisation wie vorgesehen angewendet und durchgeführt werden. Gleichzeitig sollte sichergestellt werden, dass die aufgebauten Organisationsstrukturen für Informationssicherheit den Anforderungen gerecht werden.
- Beurteilung der Effizienz von Prozessen und organisatorischen Regelungen
  Es muss regelmäßig überprüft werden, ob Prozesse und organisatorische Regelungen des Sicherheitsmanagements praxistauglich und effizient sind.
  Sobald Prozesse oder Regelungen, die aus Sicherheitsgründen eingerichtet wurden, zu kompliziert oder zeitaufwendig sind, werden sie trotz der Gefahr von Sicherheitsvorfällen häufig nicht beachtet oder bewusst umgangen.
- Managementbewertungen
  Das Management ist über die Ergebnisse der oben genannten Überprüfungen regelmäßig zu informieren. Die Berichte sind nicht nur notwendig, um dringende oder zeitkritische Probleme zu lösen, sondern enthalten wichtige Informationen, die das Management für die Steuerung des Sicherheitsprozesses benötigt.

Anpassung und Verbesserung der Informationssicherheitsorganisation

Die IS-Organisation muss regelmäßig in Bezug auf Effizienz und Effektivität optimiert werden. Haben sich Schwächen in den Prozessen oder Regelungen für die IS-Organisation gezeigt, müssen diese abgestellt werden.

Dokumentation

Die Aufgaben, Verantwortungen und Kompetenzen im Sicherheitsmanagement müssen nachvollziehbar dokumentiert sein. Dazu gehören auch die wesentlichen Arbeitsanweisungen und organisatorischen Regelungen.

ISMS.1.M7 Festlegung von Sicherheitsmaßnahmen

Aus den allgemeinen Sicherheitszielen und dem identifizierten Schutzbedarf werden konkrete Sicherheitsmaßnahmen passend zum betrachteten Informationsverbund abgeleitet. Um konkrete Sicherheitsmaßnahmen aus den Sicherheitsanforderungen der IT-Grundschutz-Bausteine abzuleiten, müssen konkrete Bausteine der IT-Grundschutz-Kataloge für die Sicherheitsanforderungen eines Informationsverbundes ausgewählt werden, um so ein spezifisches Paket von Sicherheitsmaßnahmen als Soll-Vorgabe zu erhalten.

Im Sicherheitskonzept muss beschrieben sein, in welchem Zeitraum die einzelnen Maßnahmen umzusetzen sind und welche passend kombiniert gemeinsam umgesetzt werden können. Außerdem müssen die Maßnahmen nach der Dringlichkeit der Umsetzung priorisiert werden.

Bei der Auswahl von Sicherheitsmaßnahmen ist ebenfalls deren Angemessenheit und Wirtschaftlichkeit zu beachten. Es muss nachvollziehbar sein, warum die ausgewählten Maßnahmen geeignet sind, die Sicherheitsziele und -anforderungen zu erreichen. Die Dokumentation sollte daher konkrete Angaben über Verantwortlichkeiten und Zuständigkeiten sowie geplante Aktivitäten zur Kontrolle, Revision, Überwachung enthalten.

Die Sicherheitsmaßnahmen sollten ausreichend konkret beschrieben sein, damit im Vertretungsfall ein Dritter sicherheitsspezifische Aufgaben übernehmen kann.

ISMS.1.M8 Integration der Mitarbeiter in den Sicherheitsprozess [Vorgesetzte]

Informationssicherheit betrifft ohne Ausnahme alle Mitarbeiter. Jeder Einzelne muss durch verantwortungs- und qualitätsbewusstes Handeln mithelfen, Schäden zu vermeiden und zum Erfolg der Institution beizutragen. Zur Integration der Mitarbeiter in den Sicherheitsprozess gehören folgende Aufgaben:

Motivation und Arbeitsbedingungen

Die Behörden- oder Unternehmensleitung muss ein positives Arbeitsklima schaffen und das Engagement der Mitarbeiter für die Informationssicherheit fördern. Dazu gehören unter anderem folgende Aspekte:

- Es müssen angemessene und bedienungsfreundliche Sicherheitsprodukte eingesetzt werden.
- Sicherheitskonzepte und -richtlinien müssen realistisch sein.
- Informationssicherheit muss von der Leitungsebene praktiziert werden, um eine hohe Akzeptanz bei den Mitarbeitern zu gewährleisten.

ISMS.1.M9 Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse [Institutionsleitung]

Informationssicherheit muss in alle Geschäftsprozesse integriert werden. Es muss dabei gewährleistet sein, dass nicht nur bei neuen Projekten, sondern auch bei laufenden alle erforderlichen Sicherheitsaspekte berücksichtigt werden.

Vor allem in größeren Institutionen existiert häufig bereits ein übergreifendes Risikomanagementsystem. Dabei sind operationelle Risiken inklusive der IT-Risiken integraler Bestandteil des Risikomanagements. Informationssicherheit ist ebenso eine grundlegende und prozessübergreifende Anforderung an Institutionen. Daher sollten die Methoden zum Management von Risiken aus dem Bereich der Informationssicherheit mit den bereits etablierten Methoden zum Risikomanagement abgestimmt werden. Wichtig ist, dass Arbeitsanweisungen oder Dienstvereinbarungen aus unterschiedlichen Bereichen einer Institution sich nicht widersprechen dürfen. Arbeitsanweisungen und Dienstvereinbarungen dürfen auch mit geltenden Sicherheitsmaßnahmen nicht im Widerspruch stehen.

Der BSI-Standard 100-2 zur IT-Grundschutz-Vorgehensweise sowie die Bausteine der IT-Grundschutz-Kataloge enthalten Anforderungen zur Organisation des Sicherheitsprozesses. Im Folgenden werden daher nur beispielhaft wichtige übergreifende Sicherheitsmaßnahmen kurz genannt:

Zuweisung der Verantwortung für Geschäftsprozesse, Informationen, Anwendungen und IT-Systeme

Für alle wesentlichen Geschäftsprozesse, Informationen, IT-Systeme und Anwendungen, aber auch für Gebäude und Räume müssen verantwortliche Personen benannt werden. Je nach Bereich und Sprachgebrauch werden diese verantwortlichen Personen z. B. als Informationseigentümer, Geschäftsprozessverantwortliche oder Fachverantwortliche bezeichnet. Die Fachverantwortlichen müssen die Erarbeitung und Umsetzung der Sicherheitsstrategie unterstützen.

Integration der Mitarbeiter in den Sicherheitsprozess

Informationssicherheit betrifft ohne Ausnahme alle Mitarbeiter. Jeder Einzelne muss durch verantwortungs- und qualitätsbewusstes Handeln mithelfen, Schäden zu vermeiden, und zum Erfolg beitragen. Dies betrifft nicht nur die festangestellten Mitarbeiter, sondern alle, die innerhalb der Institution beschäftigt sind, also beispielsweise auch Pförtner und Praktikanten.

Ebenso sollten auch Personen einbezogen werden, die von außerhalb auf Geschäftsprozesse, Anwendungen oder IT-Systeme zugreifen, also z. B. mobile Mitarbeiter. Wichtige Sicherheitsmaßnahmen, die beim Personalmanagement zu beachten sind, also beginnend bei der Personalauswahl und Einstellung bis hin zum Wechsel in andere Bereiche oder dem Weggang aus der Institution, sind im Baustein ORP.2 Personal beschrieben.

Darüber hinaus müssen alle Mitarbeiter innerhalb ihres Aufgabenbereiches in die erforderlichen Sicherheitsmaßnahmen eingewiesen werden. Sie sollten regelmäßig für Sicherheitsaspekte sensibilisiert werden, um das Bewusstsein für Risiken und Schutzvorkehrungen im alltäglichen Umgang mit Informationen zu schärfen. Auch das Management muss in das Sensibilisierungskonzept einbezogen werden. Vertiefende Ausführungen hierzu finden sich im Baustein ORP.3 Sensibilisierung und Schulung zur Informationssicherheit .

Einbindung externer Dienstleister in den Sicherheitsprozess

Das Sicherheitsmanagement sollte einen Überblick besitzen über alle Arten von Dienstleistern, die Aufgaben für die Institution wahrnehmen. Dies können Dienstleistungen sein, die unmittelbar die Verarbeitung geschäftsrelevanter Informationen betreffen, wie der Betrieb eines Rechenzentrums, aber auch allgemeine Unterstützungsdienstleistungen wie Wachdienst. Hierbei spielt es keine Rolle, an welchem Standort die Dienstleistung erbracht wird (Institution oder Dienstleister).

Das Sicherheitsmanagement sollte für jeden Dienstleister einschätzen, ob dessen Tätigkeit sicherheitsrelevante Auswirkungen haben kann und welche Sicherheitsvorkehrungen in diesem Rahmen zu treffen sind. Werden IT-Systeme, Anwendungen oder Geschäftsprozesse zu einem externen Dienstleister ausgelagert, ist der Baustein OPS.2.1 Outsourcing-Nutzung anzuwenden. In die Sicherheitskonzeption müssen außerdem auch Mitarbeiter von Dienstleistern einbezogen werden, die über längere Zeit in den Räumlichkeiten der Institution Aufgaben wahrnehmen.

Einbeziehung von Sicherheitsaspekten in alle Geschäftsprozesse

Das Management muss einen Überblick über die geschäftskritischen Informationen, Fachaufgaben und Geschäftsprozesse haben. Die zuständigen Fachverantwortlichen und das Informationssicherheitsmanagement-Team müssen konkrete Regeln zum Umgang mit den relevanten Sicherheitsaspekten für alle Geschäftsprozesse aufstellen (z. B. Schutzmaßnahmen, Klassifizierung und Kennzeichnung von Informationen).

Rechte und Berechtigungen

Zum Schutz der Werte müssen der Zutritt zu Räumen, der Zugang zu IT-Systemen und Anwendungen sowie der Zugriff auf Informationen geregelt werden. Nähere Informationen finden sich im Baustein ORP.4 Identitäts- und Berechtigungsmanagement.

Änderungsmanagement

Änderungsmanagement beschäftigt sich mit der Planung von Änderungen an Hard- und Software sowie Prozessen. Es muss durch organisatorische Vorgaben sichergestellt werden, dass dabei Aspekte der Informationssicherheit berücksichtigt werden. Näheres findet sich z. B. im Baustein OPS.1.2.1 Änderungsmanagement.

Konfigurationsmanagement

Konfigurationsmanagement umfasst alle Maßnahmen und Strukturen, die erforderlich sind, um den Zustand der betrachteten Objekte zu überwachen, beginnend von der Identifikation, über die Bestandsführung und Aktualisierung bis hin zur Außerbetriebnahme.

Betrachtete Objekte (Konfigurationselemente) können dabei ganze Infrastrukturbereiche, konkrete Anwendungen und IT-Systeme, aber auch einzelne Komponenten davon (beispielsweise Dokumentationen) sein.

Im Rahmen des Konfigurationsmanagements müssen Prozesse und Regelungen eingeführt werden, die beschreiben, wie Informationen über die Eigenschaften der eingesetzten Konfigurationselemente sowie Informationen über sicherheitsrelevante Störungen, Probleme und Änderungen im Zusammenhang mit Konfigurationselementen verwaltet werden. Typische Tätigkeiten sind beispielsweise die Aktualisierung der Liste der IT-Systeme oder die Anpassung von sicherheitsrelevanten Dokumentationen nach Änderungen von Geschäftsprozessen oder Anwendungen. Empfehlungen zum Konfigurationsmanagement finden sich in Baustein OPS1.1.1 Ordnungsgemäße IT-Administration.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Sicherheitsmanagement".

ISMS.1.M10 Erstellung eines Sicherheitskonzepts

Ein Informationssicherheitskonzept dient der Umsetzung der Sicherheitsstrategie und beschreibt die geplante Vorgehensweise, um die gesetzten Sicherheitsziele einer Institution zu erreichen. Das Sicherheitskonzept ist das zentrale Dokument im Sicherheitsprozess eines Unternehmens bzw. einer Behörde. Jede konkrete Maßnahme muss sich letztlich darauf zurückführen lassen. Aus diesem Grund muss ein Sicherheitskonzept sorgfältig geplant und umgesetzt sowie regelmäßig überprüft werden. Die einzelnen, im Folgenden kurz angerissenen Aspekte werden ausführlich im BSI-Standard 200-2 IT-Grundschutz-Vorgehensweise behandelt.

Nicht alle Bereiche einer Institution müssen durch ein einziges Sicherheitskonzept abgedeckt werden. Stellt die Umsetzung des IT-Grundschutzes in einem großen Schritt eine unübersichtliche Aufgabe dar, kann es sinnvoll sein, zunächst in ausgewählten Bereichen das erforderliche Sicherheitsniveau herzustellen. Von dieser Basis ausgehend sollte sich dann der Sicherheitsprozess auf die Gesamtorganisation ausweiten. Vor allem bei großen Behörden und Unternehmen kann es mehrere Sicherheitskonzepte geben, die verschiedene Organisationsbereiche abdecken. Dann muss jedoch gewährleistet sein, dass alle Bereiche einer Institution durch angemessene Sicherheitskonzepte abgedeckt werden.

Komplexe Geschäftsprozesse oder Anwendungen können in eigenen Sicherheitskonzepten behandelt werden. Dies empfiehlt sich vor allem bei der Einführung neuer Aufgaben oder Anwendungen.

Der festgelegte Geltungsbereich wird im Weiteren als Informationsverbund bezeichnet und stellt detailliert den Bereich dar, für den das Sicherheitskonzept umgesetzt werden soll. Ein Informationsverbund kann sich somit auf Fachaufgaben, Geschäftsprozesse oder Organisationseinheiten beziehen. Er umfasst alle infrastrukturellen, organisatorischen, personellen und technischen Komponenten, die der Aufgabenerfüllung in diesem Anwendungsbereich der Informationsverarbeitung dienen.

Der Informationsverbund muss so festgelegt sein, dass die betrachteten Geschäftsprozesse und Informationen diesem Bereich vollständig zugeordnet werden können. Die Abhängigkeiten aller sicherheitsrelevanten Prozesse sind zu berücksichtigen. Die Schnittstellen zu den anderen Bereichen müssen klar definiert werden, sodass der Informationsverbund im Gesamtunternehmen eine sinnvolle Mindestgröße einnimmt.

Das Sicherheitsmanagement muss eine Methode zur Risikobewertung auswählen, die es ermöglicht, potentielle Schäden durch Sicherheitsvorfälle zu analysieren und zu bewerten. Es können auch mehrere, aufeinander aufbauende Verfahren zur Risikobewertung gewählt werden.

In der Vorgehensweise nach IT-Grundschutz wird implizit eine Risikobewertung für Bereiche mit normalem Schutzbedarf durchgeführt.

In bestimmten Fällen, beispielsweise wenn der betrachtete Informationsverbund Komponenten mit hohem oder sehr hohem Schutzbedarf enthält, muss jedoch eine explizite Risikoanalyse durchgeführt werden. Die hierfür notwendigen Arbeitsschritte sind in den BSI-Standards 200-2 und 200-3 erläutert.

Basis jeder Risikobewertung ist die Beschreibung der zu schützenden Informationen und Geschäftsprozesse. Um einen Überblick über die für die Geschäftsprozesse wichtigen organisatorischen oder technischen Strukturen zu bekommen, ist der Informationsverbund strukturiert zu erfassen. Neben den technischen Komponenten, den Anwendungen und den verarbeitenden Informationen sind auch die räumliche Infrastruktur und die Vernetzung aufzunehmen. Dabei müssen auch die Abhängigkeiten der verschiedenen Komponenten untereinander festgehalten werden.

In der Schutzbedarfsfeststellung sind folgende Schritte enthalten:

- Es wird analysiert, welche Gefährdungen bzw. Risiken für die Institution als Folge unzureichender Informationssicherheit bestehen.
- Mögliche Schäden durch Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit werden identifiziert.
- Die potentiellen Auswirkungen auf die Geschäftstätigkeit oder die Aufgabenerfüllung durch Sicherheitsvorfälle und andere Sicherheitsrisiken werden analysiert und bewertet.

Anhand dieser Betrachtungen lässt sich das Risiko für das Unternehmen bzw. die Behörde abschätzen und der Schutzbedarf für Informationen, Anwendungen und IT-Systeme festlegen.

Aus den allgemeinen Sicherheitszielen, dem identifizierten Schutzbedarf und der Risikobewertung werden konkrete Sicherheitsmaßnahmen passend zum betrachteten Informationsverbund abgeleitet (siehe ISMS.1.M7 Festlegung von Sicherheitsmaßnahmen). Sicherheitsprozess und Sicherheitskonzept müssen die individuell geltenden Vorschriften und Regelungen berücksichtigen. Um konkrete Sicherheitsmaßnahmen abzuleiten, müssen konkrete Bausteine der IT-Grundschutz-Kataloge für die Sicherheitsanforderungen eines Informationsverbundes ausgewählt werden, um so ein spezifisches Paket von Sicherheitsmaßnahmen als Soll-Vorgabe zu erhalten.

Um zu ermitteln, welche der Sicherheitsmaßnahmen bereits umgesetzt und an welchen Stellen noch Lücken sind, wird ein Basis-Sicherheitscheck durchgeführt.

Die Umsetzung der nach IT-Grundschutz vorgeschlagenen Maßnahmen ist in der Regel für typische Geschäftsprozesse, Anwendungen und Komponenten mit normalem Schutzbedarf ausreichend. Jedoch ist eine Risikoanalyse erforderlich für Elemente des Informationsverbunds, die

- einen hohen oder sehr hohen Schutzbedarf in mindestens einem der drei Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit haben oder
- mit den existierenden Bausteinen der IT-Grundschutz-Kataloge nicht hinreichend abgebildet (modelliert) werden können oder
- in Einsatzszenarien (z. B. in Umgebungen oder mit Anwendungen) betrieben werden, die im Rahmen des IT-Grundschutzes nicht vorgesehen sind.

Auf der Grundlage der Gefährdungslage werden im Rahmen der Risikoanalyse gegebenenfalls Ergänzungen oder Korrekturen am Sicherheitskonzept vorgenommen. Risiken, für deren Minderung keine geeigneten oder wirtschaftlichen Gegenmaßnahmen ergriffen werden können, werden identifiziert und ebenfalls einer systematischen Risikobehandlung zugeführt.

Vor der Fertigstellung eines Sicherheitskonzeptes müssen die in der Risikoanalyse zusätzlich identifizierten Maßnahmen mit den IT-Grundschutz-Maßnahmen konsolidiert werden. Dabei ist für alle neu ermittelten Sicherheitsmaßnahmen zu überprüfen, ob sie die vorhandenen Maßnahmen ersetzen, ergänzen oder in ihrer Wirkung beeinträchtigen. Anschließend müssen die Ergebnisse des Basis-Sicherheitschecks vervollständigt und auf den neuesten Stand gebracht werden.

Ein Sicherheitskonzept ist nur wirksam, wenn die darin vorgesehenen Maßnahmen auch zeitnah in die Praxis umgesetzt werden. Dies muss geplant und kontrolliert werden.

Dafür ist festzuhalten, in welchem Zeitraum die einzelnen Maßnahmen umzusetzen sind und welche passend kombiniert gemeinsam umgesetzt werden können. Außerdem müssen die Maßnahmen nach der Dringlichkeit der Umsetzung priorisiert werden. Die Umsetzungsplanung sollte entweder im Sicherheitskonzept oder in einem beigefügten Realisierungsplan festgehalten werden. Hierin sollten unbedingt Umsetzungsreihenfolge und Verantwortlichkeiten enthalten sein:

- Festlegung von Prioritäten (Umsetzungsreihenfolge): Alle Sicherheitsmaßnahmen sollten nach Wichtigkeit und Effektivität priorisiert werden. Grundsätzlich sollten Maßnahmen gegen besonders schwerwiegende Gefährdungen vorrangig umgesetzt werden. Dies ist besonders wichtig, wenn gegen diese Gefährdungen bisher nur wenig Schutz besteht. Können z. B. aus finanziellen Gründen nicht alle Maßnahmen sofort umgesetzt werden, sollten die Maßnahmen mit der größten Breitenwirkung zuerst umgesetzt werden.
- Bei der Umsetzungsreihenfolge sollten mögliche Zusammenhänge zwischen Maßnahmen berücksichtigt werden.
- Verantwortlichkeiten: Für jede Maßnahme ist festzulegen, wer für deren Initialisierung, Umsetzung und Kontrolle (z. B. Audit) oder Revision verantwortlich ist.

Bei der Auswahl von Sicherheitsmaßnahmen ist ebenfalls deren Angemessenheit und Wirtschaftlichkeit zu beachten. Es muss nachvollziehbar sein, warum die ausgewählten Maßnahmen geeignet sind, die Sicherheitsziele und -anforderungen zu erreichen. Die Dokumentation sollte daher konkrete Angaben über Verantwortlichkeiten und Zuständigkeiten sowie geplante Aktivitäten zur Kontrolle, Revision, Überwachung enthalten.

Die Reihenfolge für die Umsetzung offener Aktivitäten ist festzuhalten. Außerdem sind die geplanten bzw. eingesetzten Ressourcen für die Umsetzung der einzelnen Sicherheitsmaßnahmen zu dokumentieren.

Da Informationssicherheit ein kontinuierlicher Prozess ist, genügt es nicht, die Sicherheitsmaßnahmen einmal umzusetzen. Die Informationssicherheit muss kontinuierlich verbessert werden. Im Rahmen des Sicherheitsprozesses muss daher auf neue technische Entwicklungen reagiert werden. Schwachstellen sowie neu aufgedeckte Sicherheitslücken müssen berücksichtigt werden. Der Sicherheitsprozess sollte daher regelmäßig überprüft, aktualisiert und alle Änderungen sollten dokumentiert werden. Wichtige Verfahren sind dabei die Einführung von regelmäßigen Berichten (siehe ISMS.1.A12 Management-Berichte zur Informationssicherheit) und Meldeprozesse.

Eine Zertifizierung des Sicherheitsprozesses dokumentiert die Einhaltung einer definierten Vorgehensweise und kann als unabhängiges Review-Verfahren in den Sicherheitsprozess integriert werden.

Das Sicherheitskonzept wird in der Praxis häufig herangezogen, um konkrete Sicherheitsmaßnahmen bezüglich ihrer Umsetzung oder ihrer Aktualität zu überprüfen. Daher sollte es so strukturiert sein, dass

- spezifische Bereiche schnell gefunden werden können, und
- es mit minimalem Aufwand aktualisiert werden kann (hierfür bietet sich die Nutzung eines Tools an).

Außerdem sollten die einzelnen Sicherheitsmaßnahmen ausreichend konkret beschrieben sein, damit im Vertretungsfall ein Dritter sicherheitsspezifische Aufgaben übernehmen kann.

Ein Sicherheitskonzept kann vertrauliche Informationen beinhalten, wie z. B. Angaben über noch nicht beseitigte Schwachstellen oder Informationen zu Maßnahmen, die helfen, diese Maßnahmen zu umgehen oder zu überwinden. Solche vertraulichen Informationen dürfen ausschließlich an die zuständigen Personen weitergegeben werden. Das Sicherheitskonzept sollte daher so gegliedert werden, dass die Bereiche, die einen breiten Adressatenkreis betreffen, von denen getrennt werden, die nur eingeschränkt weitergegeben werden dürfen. Jeder Mitarbeiter sollte zumindest über die ihn unmittelbar betreffenden Teile des Sicherheitskonzepts informiert sein.

Es ist wichtig, ein gemeinsames Verständnis für Informationssicherheit in einer Institution herzustellen. Dazu gehört auch die Verwendung einheitlicher und klarer Begriffe. Daher sollte frühzeitig ein Glossar mit den wichtigsten Begriffen rund um Informationssicherheit erstellt werden. Dieses Glossar hilft bei der Erstellung aller sicherheitsrelevanten Dokumente. Es kann im Sicherheitskonzept oder auch einzeln veröffentlicht werden.

ISMS.1.M11 Aufrechterhaltung der Informationssicherheit

Im Sicherheitsprozess geht es nicht nur darum, das angestrebte Sicherheitsniveau zu erreichen, sondern dieses auch dauerhaft zu gewährleisten. Um das bestehende Sicherheitsniveau aufrechtzuerhalten und fortlaufend zu verbessern, sollten alle Sicherheitsmaßnahmen regelmäßig überprüft werden.

Sowohl die korrekte Umsetzung als auch die Umsetzbarkeit eines Sicherheitskonzepts müssen regelmäßig überprüft werden. Dabei ist zu unterscheiden zwischen der Prüfung, ob bestimmte Maßnahmen geeignet und effizient sind, um die gesteckten Sicherheitsziele zu erreichen (Vollständigkeits- bzw. Aktualisierungsprüfung), und der Kontrolle, inwieweit Sicherheitsmaßnahmen in den einzelnen Bereichen umgesetzt wurden (Revision der Informationssicherheit).

Die im Sicherheitskonzept geplanten Sicherheitsmaßnahmen müssen gemäß dem Realisierungsplan umgesetzt werden. Der Umsetzungsstatus muss dokumentiert werden. Zieltermine und Ressourceneinsatz müssen überwacht und gesteuert werden. Die Leitungsebene ist dazu regelmäßig zu informieren.

Diese Überprüfungen sollten zu festgelegten Zeitpunkten (mindestens jährlich) durchgeführt werden und können auch zwischendurch erfolgen. Insbesondere Erkenntnisse aus sicherheitsrelevanten Zwischenfällen, Veränderungen im technischen oder technisch-organisatorischen Umfeld sowie Änderungen von Sicherheitsanforderungen bzw. Bedrohungen erfordern eine Anpassung der bestehenden Sicherheitsmaßnahmen. Die in den einzelnen Überprüfungen ermittelten Ergebnisse sollten dokumentiert werden. Es muss zudem festgelegt sein, wie mit den Überprüfungsergebnissen zu verfahren ist, da die Informationssicherheit nur dann wirksam aufrechterhalten werden kann, wenn aufgrund der Überprüfungsergebnisse auch die erforderlichen Korrekturmaßnahmen ergriffen werden.

Es sollten auch gelegentlich unangekündigte Überprüfungen durchgeführt werden, da angekündigte Kontrollen häufig ein verzerrtes Bild des Untersuchungsgegenstands ergeben.

Kontrollen sollten vor allen Dingen darauf ausgerichtet sein, Mängel abzustellen. Für die Akzeptanz ist es wichtig, dass dies allen Beteiligten als Ziel der Kontrollen erkennbar ist und dass die Kontrollen nicht den Charakter von Schulmeisterei haben. Es ist daher sinnvoll, während einer Kontrolle mit den Beteiligten über mögliche Problemlösungen zu sprechen und entsprechende Abhilfen vorzubereiten.

Es sollte in der Behörde bzw. im Unternehmen festgelegt werden, wie die Tätigkeiten im Zusammenhang mit diesen Überprüfungen zu koordinieren sind. Dazu ist zu regeln, welche Sicherheitsmaßnahmen wann und von wem zu überprüfen sind, auch damit Doppelarbeit vermieden wird und keine Bereiche innerhalb einer Institution ungeprüft verbleiben.

Die vorhandenen Sicherheitsmaßnahmen sollten mindestens einmal im Jahr überprüft werden. Darüber hinaus sind sie immer dann zu prüfen, wenn

- neue Geschäftsprozesse, Anwendungen oder IT-Komponenten aufgebaut werden,
- größere Änderungen der Infrastruktur vorgenommen werden (z. B. Umzug),
- größere organisatorischen Änderungen anstehen (z. B. Outsourcing),
- die Gefährdungslage sich wesentlich ändert,
- wenn gravierende Schwachstellen oder Schadensfälle bekannt werden.

Einhaltung des Sicherheitskonzeptes (Sicherheitsrevision)

Hierbei muss geprüft werden, ob Sicherheitsmaßnahmen tatsächlich so umgesetzt sind und eingehalten werden wie im Sicherheitskonzept vorgegeben. Hierbei ist auch zu untersuchen, ob technische Maßnahmen korrekt implementiert und konfiguriert wurden und ob alle vorgesehenen Detektionsmaßnahmen (z. B. Auswertung von Protokolldateien) tatsächlich durchgeführt werden.

Dabei kann sich zeigen, dass Sicherheitsmaßnahmen nicht umgesetzt worden sind oder dass sie in der Praxis nicht greifen. In beiden Fällen sollten die Ursachen für die Abweichungen ermittelt werden. Als mögliche Korrekturmaßnahmen kommen - je nach Ursache - in Frage:

- organisatorische Maßnahmen sind anzupassen,
- personelle Maßnahmen, z. B. Schulungs- und Sensibilisierungsmaßnahmen, sind zu ergreifen oder disziplinarische Maßnahmen einzuleiten,
- infrastrukturelle Maßnahmen, z. B. bauliche Veränderungen, sind zu initiieren,
- technische Maßnahmen, z. B. Änderungen an Hardware und Software oder Kommunikationsverbindungen und Netzen, sind vorzunehmen,
- Entscheidungen des verantwortlichen Vorgesetzten (bis hin zur Leitungsebene) sind einzuholen.

Auf jeden Fall sollte für jede Abweichung eine Korrekturmaßnahme vorgeschlagen werden. Außerdem sollten auch hier der Zeitpunkt und die Zuständigkeiten für die Umsetzung der Korrekturmaßnahme festgelegt werden.

Kontrollen sollen helfen, Fehlerquellen abzustellen. Es ist für die Akzeptanz von Kontrollen extrem wichtig, dass dabei keine Personen bloßgestellt werden oder als "Schuldige" identifiziert werden. Wenn die Mitarbeiter dies befürchten müssen, besteht die Gefahr, dass sie nicht offen über ihnen bekannte Schwachstellen und Sicherheitslücken berichten, sondern versuchen, bestehende Probleme zu vertuschen.

Im Vorfeld sollten aber auch die Reaktionen auf Verletzung der Sicherheitsvorgaben festgelegt werden. Es müssen angemessene Maßnahmen ergriffen werden, die dazu beitragen, dass sich Sicherheitsvorfälle nicht wiederholen. Dazu könnte beispielsweise die Einschränkung von Zugriffsrechten gehören.

Falls unzulässige Aktivitäten von Mitarbeitern entdeckt werden, sollte der jeweilige Vorgesetzte informiert werden, damit angemessene Konsequenzen angestoßen werden können.

Kontinuierliche Verbesserung des Sicherheitskonzeptes (Vollständigkeits- bzw. Aktualisierungsprüfung)

Das Sicherheitskonzept muss regelmäßig aktualisiert, verbessert und an neue Rahmenbedingungen angepasst werden. Es muss regelmäßig geprüft werden, ob die ausgewählten Sicherheitsmaßnahmen noch geeignet sind, die Sicherheitsziele zu erreichen. Dabei kann direkt untersucht werden, ob die eingesetzten Sicherheitsmaßnahmen effizient sind oder ob die Sicherheitsziele mit anderen Maßnahmen ressourcenschonender erreicht werden könnten.

Deshalb ist es wichtig, externe Wissensquellen, wie Standards oder Fachpublikationen, im Hinblick auf neue technische und regulatorische Entwicklungen auszuwerten. Auch Kontakte zu Gremien und Interessengruppen, die sich mit Sicherheitsaspekten beschäftigen, helfen dem IS-Management-Team, das vorhandene Wissen über sicherheitsrelevante Methoden und Lösungen zu erweitern und zu aktualisieren. Außerdem werden dabei auch wertvolle Kontakte zu anderen Informationssicherheitsbeauftragten geknüpft, um Lösungen anderer Institutionen kennenzulernen und Praxiserfahrungen auszutauschen. Es entstehen dadurch auch Wege, über die frühzeitig Warnungen über aufkommende Sicherheitsprobleme ausgetauscht werden können. Das IS-Management-Team sollte einen Überblick über thematisch passende Gremien und Interessengruppen haben und festlegen, wo sich aktive Mitarbeit anbietet und wo nur die Ergebnisse regelmäßig beobachtet und ausgewertet werden sollten.

Durchführung der Prüfungen

Entsprechend dem Prüfungszweck sind Umfang und Tiefe der Überprüfungen festzulegen. Als Grundlage für alle Überprüfungen dient das Sicherheitskonzept und die vorhandene Dokumentation des Sicherheitsprozesses.

Eine Überprüfung sollte von Personen mit geeigneten Qualifikationen durchgeführt werden. Diese Personen sollten jedoch nicht an der Erstellung der Konzepte beteiligt gewesen sein, um Betriebsblindheit und Konflikte zu vermeiden. Die Prüfer bzw. Auditoren müssen möglichst unabhängig und neutral sein.

Jede Überprüfung ist sorgfältig zu planen. Alle relevanten Feststellungen und Ergebnisse sind in einem Bericht festzuhalten. Dieser sollte neben einer Auswertung auch Korrekturvorschläge enthalten. Der Bericht sollte dem Leiter des überprüften Bereiches sowie dem IS-Management-Team übergeben werden, die auf dieser Basis die weiteren Schritte konzipieren müssen. Schwerwiegende Probleme sollten direkt der Leitungsebene kommuniziert werden, damit weitreichende Entscheidungen zeitnah getroffen werden können.

Werden bei der Prüfung spezielle Audit- oder Diagnosewerkzeuge eingesetzt, muss ebenso wie bei der Ergebnisdokumentation sichergestellt sein, dass nur autorisierte Personen darauf Zugriff haben. Diagnose- und Prüftools sowie die Prüfergebnisse müssen daher besonders geschützt werden.

Wenn Externe an Prüfungen beteiligt sind, muss sichergestellt werden, dass keine Informationen der Institution missbräuchlich verwenden (z. B. durch entsprechende Vertraulichkeitsvereinbarungen) und dass sie nur auf die benötigten Informationen zugreifen können (z. B. durch Zugriffsrechte oder Vier-Augen-Kontrolle). Sollten sie Prüftools einsetzen, muss deren Nutzung genau geregelt werden.

Korrekturmaßnahmen

Erkannte Fehler und Schwachstellen müssen zeitnah abgestellt werden. Der identifizierte Optimierungsbedarf bei Effizienz und Effektivität von Sicherheitsmaßnahmen muss umgesetzt werden.

Aufgrund der Überprüfungsergebnisse sind Entscheidungen über das weitere Vorgehen zu treffen. Insbesondere sind alle erforderlichen Korrekturmaßnahmen in einem Umsetzungsplan festzuhalten. Die Verantwortlichen für die Umsetzung der Korrekturmaßnahmen sind zu benennen und mit den notwendigen Ressourcen auszustatten.

ISMS.1.M12 Management-Berichte zur Informationssicherheit [Institutionsleitung]

Zu den Aufgaben des Informationssicherheitsbeauftragten gehört es, die Behörden- oder Unternehmensleitung bei der Wahrnehmung ihrer Gesamtverantwortung für die Informationssicherheit zu unterstützen. Eine wichtige Grundlage für die zu treffenden Entscheidungen sind übersichtlich und aussagekräftig aufbereitete Informationen zur aktuellen Lage der Informationssicherheit in der Institution.

Um den Sicherheitsprozess zu steuern und aufrecht zu erhalten und fortlaufend zu verbessern, muss regelmäßig seine Wirksamkeit und Effizienz überprüft werden und diese Ergebnisse auf Leitungsebene bewertet werden. Ziel hierbei ist, das weitere Vorgehen im Sicherheitsprozess mit der Leitungsebene abzustimmen. Daher sind alle erforderlichen Änderungen am Sicherheitsprozess, beispielsweise in den Sicherheitszielen oder der Sicherheitsleitlinie, aufzuzeigen. Die Ergebnisse müssen dokumentiert und die bisherigen Aufzeichnungen gepflegt werden.

Regelmäßige Management-Berichte

Damit die Unternehmens- bzw. Behördenleitung die richtigen Entscheidungen bei der Steuerung und Lenkung des Informationssicherheitsprozesses treffen kann, benötigt sie Eckpunkte über den Stand der Informationssicherheit. Diese Eckpunkte sollten in Management-Berichten aufbereitet werden, die unter anderem folgende Punkte abdecken:

- Ergebnisse von Audits und Datenschutzkontrollen
- Berichte über Sicherheitsvorfälle
- Berichte über bisherige Erfolge und Probleme beim Informationssicherheitsprozess

Die Leitungsebene sollte vom IS-Management-Team regelmäßig in angemessener Form über die Ergebnisse der Überprüfungen und den Status des IS-Prozesses informiert werden. Dabei sollten Probleme, Erfolge und Verbesserungsmöglichkeiten aufgezeigt werden.

Ein Management-Bericht sollte kurz und übersichtlich sein. Die folgenden Punkte können dabei, je nach aktueller Situation, relevant sein. Allerdings sollten nicht alle gleichzeitig in einem Management-Bericht zur Informationssicherheit betrachtet werden, um diesen nicht zu überfrachten. Es ist also zu überlegen, aufzeigen

- inwieweit die Vorgaben des Sicherheitskonzepts im Unternehmen oder in der Behörde bereits abgedeckt sind,
- an welchen Stellen noch Lücken - und damit Restrisiken - bestehen,
- welche Sicherheitsvorfälle aufgetreten sind, welche Schäden entstanden sind und welche Schäden verhindert werden konnten,
- welche Ergebnisse interne Überprüfungen und Audits erbracht haben,
- inwieweit das Sicherheitsniveau den Sicherheitsanforderungen und der Bedrohungslage der Institution genügt,
- ob sich Rahmenbedingungen geändert haben, so dass weitere Maßnahmen erforderlich sind,
- ob die Aktivitäten im Rahmen der Informationssicherheit Erfolg hatten,
- ob sich die Sicherheitsmaßnahmen zur Erreichung der Sicherheitsziele als geeignet erwiesen haben oder ob Maßnahmen geändert oder ergänzt werden müssen,
- welche Rückmeldungen es von Kunden, Geschäftspartnern, Mitarbeitern oder der Öffentlichkeit zu Sicherheitsaspekten gab,
- welche Ressourcen für Informationssicherheit aufgewendet wurden,
- ob und wie die bisherigen Management-Entscheidungen umgesetzt wurden und ob die Aktivitäten im Rahmen der Informationssicherheit Erfolg hatten.

Daneben sollte sowohl ein Ausblick auf die zu erwartende Weiterentwicklung der organisationsweiten Informationssicherheit gegeben werden, als auch auf technische Entwicklungen und Verfahrensweisen, die eventuell zur Verbesserung des Sicherheitsprozesses beitragen könnten.

Anlassbezogene Management-Berichte

Neben den regelmäßigen Management-Berichten kann es notwendig sein, bei überraschend auftretenden Sicherheitsproblemen oder aufgrund von Risiken, die aus neuen technischen Entwicklungen resultieren, anlassbezogene Management-Berichte zu erstellen. Dies ist vor allem dann der Fall, wenn diese Probleme nicht auf Arbeitsebene gelöst werden können, weil z. B. materielle Ressourcen außerhalb des bewilligten Rahmens benötigt werden oder weitergehende personelle Regelungen getroffen werden müssen.

Immer wieder erregen Sicherheitsvorfälle wie globale Malware-Attacken die Aufmerksamkeit der Massenmedien. Es hat sich als sinnvoll erwiesen, auch in diesen Fällen Management-Berichte zu erstellen, um aufzuzeigen, inwieweit die eigene Institution von diesen Sicherheitsvorfällen betroffen wurde. Auch wenn sich die Sicherheitslage ändert (z. B. durch neue Bedrohungen, neue Technologien, neue Gesetze) kann ein anlassbezogener Management-Bericht sinnvoll sein.

Bei der Abfassung der Management-Berichte sollte berücksichtigt werden, dass sich der Leserkreis in der Regel nicht aus technischen Experten zusammensetzt. Entsprechend sollte sich der Text durch größtmögliche Verständlichkeit und Knappheit auszeichnen, indem gezielt die wesentlichen Punkte, wie beispielsweise bestehende Schwachstellen, aber auch erreichte Erfolge, herausgearbeitet werden.

Am Schluss jedes Management-Berichts, vor allem bei anlassbezogenen Berichten, sollten immer klar priorisierte und mit realistischen Abschätzungen des zu erwartenden Umsetzungsaufwands versehene Maßnahmenvorschläge stehen. Damit wird sichergestellt, dass eine notwendige Entscheidung der Leitungsebene ohne unnötige Verzögerungen herbeigeführt werden kann.

Der Management-Bericht zur Informationssicherheit sollte der Leitungsebene durch ein Mitglied des IS-Management-Teams persönlich präsentiert werden. So können wesentliche Schwerpunkte wie beispielsweise bestehende oder drohende Sicherheitsmängel betont werden. Das Mitglied des IS-Management-Teams steht auch direkt für Rückfragen und weitergehende Erläuterungen zur Verfügung, was erfahrungsgemäß zu einer Beschleunigung des Entscheidungsvorgangs führt.

Darüber hinaus ist der persönliche Kontakt auch wichtig, um Leitungsentscheidungen besser vorbereiten und Probleme schon im Voraus entschärfen zu können. Hilfreich wäre es auch, wenn ein Mitglied der Leitungsebene mit entsprechendem fachlichem Hintergrund und Interesse als Ansprechpartner zur Verfügung steht. Der persönliche Kontakt bietet die Möglichkeit, einen "kleinen Dienstweg" zu etablieren, dessen Existenz sich in dringenden Notfällen als vorteilhaft erweisen kann.

Management-Entscheidungen

Das Management entscheidet auf Grundlage des Management-Berichts über die weitere Vorgehensweise im Sicherheitsprozess. Dabei wird die Behörden- oder Unternehmensleitung bei Bedarf vom Informationssicherheitsbeauftragten unterstützt. Alle Entscheidungen müssen dokumentiert werden. Dazu gehören insbesondere folgenden Punkte:

- Erforderliche Aktionen zur Verbesserungen der Effektivität des Sicherheitskonzepts sowie die dafür benötigten Ressourcen
- Höhe des Schutzbedarfs sowie die Behandlung von Restrisiken, die bei einer Risikoanalyse identifiziert wurden
- Veränderungen von sicherheitsrelevanten Prozessen, um internen oder externen Ereignissen zu begegnen, die Einfluss auf das Sicherheitskonzept haben könnten, z. B. in Hinsicht auf Änderungen bei
- Geschäftszielen
- Sicherheitsanforderungen
- Geschäftsprozessen
- externen Rahmenbedingungen (wie dem gesetzlichen Umfeld oder vertraglichen Verpflichtungen)

Zur kontinuierlichen Verfolgung des Sicherheitsprozesses sollten sämtliche Management-Berichte und Management-Entscheidungen zur Informationssicherheit in geordneter Weise archiviert werden. Diese Dokumentation sollte den Verantwortlichen bei Bedarf kurzfristig zugänglich sein (siehe ISMS.1.M11 Dokumentation des Sicherheitsprozesses).

Da die Management-Berichte zur Informationssicherheit im Allgemeinen sensitive Informationen über bestehende Sicherheitslücken und Restrisiken enthalten, ist deren Vertraulichkeit zu schützen. Es müssen angemessene Schutzvorkehrungen getroffen werden, damit keine unbefugten Personen Kenntnis über den Inhalt der Management-Berichte erlangen.

ISMS.1.M13 Dokumentation des Sicherheitsprozesses

Der Ablauf des Sicherheitsprozesses, wichtige Entscheidungen und die Arbeitsergebnisse der einzelnen Phasen sollten dokumentiert werden. Eine solche Dokumentation ist eine wesentliche Grundlage für die Aufrechterhaltung der Informationssicherheit und damit entscheidende Voraussetzung für die effiziente Weiterentwicklung des Prozesses. Sie hilft dabei, die Ursachen von Störungen und fehlgeleiteten Abläufen zu finden und zu beseitigen. Wichtig ist, dass nicht nur die jeweils aktuelle Version kurzfristig zugänglich ist, sondern auch eine zentrale Archivierung der Vorgängerversionen vorgenommen wird. Erst durch die kontinuierliche Dokumentation können die Entwicklungen und Entscheidungen im Bereich Informationssicherheit nachvollziehbar zurückverfolgt werden.

Neben Dokumenten zum Sicherheitsmanagement und dem Sicherheitsprozess gibt es weitere für das Sicherheitsmanagement relevante Dokumente. Abhängig vom Gegenstand und vom Verwendungszweck sind folgende Arten von Dokumentationen zu betrachten:

Berichte an die Leitungsebene

Damit die oberste Leitungsebene einer Behörde oder eines Unternehmens die richtigen Entscheidungen treffen kann, um Informationssicherheit auf einem angemessenen Niveau zu gewährleisten, benötigt sie die dafür notwendigen Informationen. Hierfür sollte der Informationssicherheitsbeauftragte bzw. das IS-Management-Team regelmäßig sowie anlassbezogen Management-Berichte zum Status der Informationssicherheit (siehe auch ISMS.1.M10 Management-Berichte zur Informationssicherheit) erstellen.

Dokumente zum Sicherheitsprozess

Folgende Arten von Dokumentationen zum Sicherheitsprozess sollten erstellt werden:

- Die oberste Leitungsebene muss die Leitlinie zur Informationssicherheit der Behörde bzw. des Unternehmens festlegen und veröffentlichen. Diese enthält unter anderem die Sicherheitsziele und die Sicherheitsstrategie.
- Im Sicherheitskonzept werden die erforderlichen Sicherheitsmaßnahmen beschrieben und deren Umsetzung festgelegt.
- Auf der Sicherheitsleitlinie aufbauend gibt es bereichs- und systemspezifische Sicherheitsrichtlinien und Regelungen für den ordnungsgemäßen und sicheren IT-Einsatz.
- Die wesentlichen Arbeiten des IS-Management-Teams sollten ebenfalls dokumentiert sein, dazu gehören z. B. Sitzungsprotokolle und Beschlüsse.
- Ergebnisse von Audits und Überprüfungen (z. B. Prüflisten und Befragungsprotokolle).

Dokumentation von Arbeitsabläufen

Arbeitsabläufe, organisatorische Vorgaben und technische Sicherheitsmaßnahmen müssen so dokumentiert werden, dass Sicherheitsvorfälle durch Unkenntnis oder Fehlhandlungen vermieden werden.

Es muss bei Störungen oder Sicherheitsvorfällen möglich sein, den gewünschten Soll-Zustand der Geschäftsprozesse und der IT wiederherzustellen. Technische Einzelheiten und Arbeitsabläufe sind daher so zu dokumentieren, dass dies in angemessener Zeit möglich ist.

Dokumentation von Sicherheitsvorfällen

Sicherheitsrelevante Vorfälle müssen so aufbereitet werden, dass alle damit verbundenen Vorgänge und Entscheidungen nachvollziehbar sind. Ebenso soll es die Dokumentation ermöglichen, Verbesserungen an den Notfallstrategien vorzunehmen und bekannte Fehler zu vermeiden. Zur Bearbeitung von Sicherheitsvorfällen sind außerdem technische Unterlagen, wie Protokolle oder für den Vorfall besonders relevante System-Meldungen, zu speichern und zu archivieren. Die Regelungen des Datenschutzes müssen eingehalten werden.

Technische Dokumentation

Zu dieser Art von sicherheitsrelevanten Dokumentationen gehören:

- Installations- und Konfigurationsanleitungen,
- Anleitungen für den Wiederanlauf nach einem Sicherheitsvorfall,
- Dokumentation von Test- und Freigabeverfahren und
- Anweisungen für das Verhalten bei Störungen und Sicherheitsvorfällen.

Anleitungen für Mitarbeiter

Sicherheitsmaßnahmen müssen für die Mitarbeiter verständlich dokumentiert werden. Den Mitarbeitern müssen also

- die geltenden Sicherheitsrichtlinien,
- übersichtliche Merkblätter für den verantwortungsvollen Umgang mit internen Informationen, für die sichere Nutzung von IT-Systemen und Anwendungen sowie zum Verhalten bei Sicherheitsvorfällen,
- Handbücher und Anleitungen für die eingesetzten IT-Systeme und Anwendungen

zur Verfügung stehen.

Es kann in seltenen Fällen vorkommen, dass ein Verstoß gegen eine Sicherheitsrichtlinie sinnvoll und notwendig ist. Ein solcher Verstoß muss aber auf jeden Fall zuvor durch eine autorisierte Stelle genehmigt werden. Ausnahmegenehmigungen dürfen nur nach gründlicher Prüfung und in den seltensten Fällen erteilt werden. Anschließend muss eine schriftliche Begründung verfasst werden, die vom Verantwortlichen zu unterzeichnen ist.

Informationsfluss und Meldewege

Wichtig für die Aufrechterhaltung des Sicherheitsprozesses ist die Beschreibung und zeitnahe Aktualisierung der Meldewege und der Vorgehensweise für den Informationsfluss.

Dokumentationswesen

Es ist Aufgabe des Informationssicherheitsbeauftragten bzw. des IS-Management-Teams, stets aktuelle und aussagekräftige Dokumentationen zur Informationssicherheit vorzuhalten. Für alle Dokumentationen im Rahmen des Sicherheitsprozesses sollte es daher eine geregelte Vorgehensweise geben. Dazu gehören z. B. folgende Punkte:

- Dokumentationen müssen verständlich sein. Das bedeutet auch, dass sie zielgruppengerecht gestaltet werden müssen. Berichte an die Leitungsebene haben andere Anforderungen als technische Dokumentationen für Administratoren.
- Dokumentationen müssen aktuell sein. Es muss festgelegt werden, wer sie pflegt. Sie müssen so bezeichnet und abgelegt werden, dass sie im Bedarfsfall schnell gefunden werden können. Es müssen Angaben zu Erstellungsdatum, Version, Quellen und Autoren vorhanden sein. Veraltete Unterlagen müssen sofort aus dem Umlauf genommen und archiviert werden.
- Es sollte ein definiertes Verfahren existieren, um Änderungsvorschläge (inklusive der Erstellung neuer Dokumente) einzubringen, zu beurteilen und gegebenenfalls zu berücksichtigen.
- Neben der schnellen Informationsweitergabe an Berechtigte ist andererseits die Vertraulichkeit von organisationsinternen Details sicherzustellen. Vertrauliche Inhalte müssen als solche klassifiziert werden und die Dokumente sicher verwahrt und bearbeitet werden.

Bei der Pflege der Vielzahl sicherheitsrelevanter Dokumente kann ein Dokumentenmanagement hilfreich sein.

Dokumentationen müssen nicht immer in Papierform vorliegen. Das Dokumentationsmedium kann je nach Bedarf gewählt werden. Zur Dokumentation können Übersichtsdiagramme (z. B. Netzplan), kurze Sitzungsprotokolle (z. B. jährliche Sitzung der Geschäftsführung zur Diskussion der Sicherheitsstrategie), handschriftliche Notizen oder Software-Tools (z. B. zur Dokumentation des Sicherheitskonzepts) genutzt werden.

ISMS.1.M14 Sensibilisierung zur Informationssicherheit

Eine weitere Aufgabe, die den gesamten Sicherheitsprozess begleiten muss, ist die Organisation und Durchführung von Schulungs- und Sensibilisierungsmaßnahmen. Das Unternehmen oder die Behörde sollte ein Schulungs- und Sensibilisierungskonzept erarbeiten. Eine ausführliche Behandlung dieses Themas ist im Baustein ORP.3 Sensibilisierung und Schulung zur Informationssicherheit genauer nachzulesen.

ISMS.1.M15 Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit

Die gesteckten Sicherheitsziele können nur erreicht werden, wenn dafür angemessene Ressourcen bereitgestellt werden.

Bereitstellung von Ressourcen für Informationssicherheit

Informationssicherheit erfordert ausreichende finanzielle und personelle Ressourcen sowie eine geeignete Ausstattung. Diese müssen dem Informationssicherheitsmanagement-Team von der Behörden- bzw. Unternehmensleitung in angemessenem Umfang bereitgestellt werden.

Es ist zu empfehlen, dass das IS-Management-Team anhand der Sicherheitsziele die für die Umsetzung aller identifizierten Maßnahmen benötigten Ressourcen aufzeigt. Dies dient einerseits als Grundlage für Management-Entscheidungen über die Zuteilung der Ressourcen und andererseits zur Festlegung der Projektpläne und der Umsetzungszeiträume.

Zugriff auf externe Ressourcen

Die internen Sicherheitsexperten sind häufig mit ihren Routinetätigkeiten so ausgelastet, dass sie bei neuen Aufgaben oder Entwicklungen nicht alle sicherheitsrelevanten Einflussfaktoren analysieren oder Sicherheitslösungen umsetzen können. Hierzu gehören beispielsweise geänderte gesetzliche Anforderungen, die Einführung neuer IT-Systeme sowie die Verfolgung der aktuellen technischen Entwicklungen. Um Arbeitsspitzen bewältigen zu können, müssen entweder intern zusätzliche Mitarbeiter eingesetzt oder es muss auf externe Experten zurückgegriffen werden. Der Bedarf muss von den internen Sicherheitsexperten kommuniziert werden, damit die Leitungsebene die erforderlichen Ressourcen bereit stellt.

Es ist sicherzustellen, dass alle erforderlichen Sicherheitsmaßnahmen umgesetzt werden, sei es durch den Rückgriff auf externe oder interne Kräfte.

Ressourcen für den Informationssicherheitsbeauftragten

Ohne eine funktionierende Organisationsstruktur für Informationssicherheit nützen die teuersten technischen Lösungen nichts. Die Erfahrung zeigt, dass die Berufung eines Informationssicherheitsbeauftragten die effektivste Sicherheitsmaßnahme ist. Nach der Bestellung eines Sicherheitsbeauftragten geht in den meisten Institutionen die Anzahl an Sicherheitsvorfällen signifikant zurück. Damit der Informationssicherheitsbeauftragte eine tatsächliche Verbesserung des Sicherheitsniveaus erreichen kann, muss er

- ausreichend Zeit für seine Arbeit haben,
- ausreichend in alle Geschäftsprozesse, Fachaufgaben und Projekte integriert sein,
- genügenden Zugriff auf alle erforderlichen Ressourcen haben.

In kleineren Institutionen ist es möglich, dass ein Mitarbeiter die Aufgaben des Informationssicherheitsbeauftragten in Personalunion neben seinen eigentlichen Tätigkeiten wahrnimmt.

Ressourcen für das Informationssicherheitsmanagement-Team

Ein IS-Management-Team sollte immer dann eingerichtet werden, wenn der Informationssicherheitsbeauftragte alleine nicht mehr alle Geschäftsprozesse und Projekte betreuen kann, also die Institution eine gewisse Größenordnung überschritten hat.

Die erstmalige Einrichtung des Sicherheitsprozesses ist meist mit einem erhöhten Aufwand verbunden. Häufig ist es deshalb zweckmäßig, dem IS-Management-Team für diese Phase zusätzliche personelle Ressourcen zur Verfügung zu stellen.

Bereitstellung von Ressourcen für den IT-Betrieb

Grundvoraussetzung für einen sicheren IT-Betrieb ist, dass dieser reibungslos funktioniert, also vernünftig geplant und organisiert ist. Für den IT-Betrieb müssen ausreichende Ressourcen zur Verfügung gestellt werden. Typische Probleme des IT-Betriebs (knappes Budget, überlastete Administratoren und eine unstrukturierte oder schlecht gewartete IT-Landschaft) müssen in der Regel gelöst werden, damit die eigentlichen Sicherheitsmaßnahmen wirksam und effizient umgesetzt werden können. Ob die bereitgestellten Ressourcen ausreichen, zeigt sich beispielsweise daran, ob die Benutzer angemessen betreut werden oder ob alle Hard- und Software wie vorgesehen getestet wird.

Wirtschaftlichkeitsaspekte in der Sicherheitsstrategie

Die Sicherheitsstrategie sollte von Beginn an auch Wirtschaftlichkeitsaspekte berücksichtigen. Bei der Auswahl der umzusetzenden Sicherheitsmaßnahmen sollten die zur Verfügung stehenden Ressourcen berücksichtigt werden. Wenn für bestimmte Maßnahmen keine ausreichende technische oder personelle Unterstützung vorhanden ist, muss die Strategie geändert werden. In vielen Fällen lassen sich andere Maßnahmen finden, die zu einem ähnlichen Sicherheitsniveau führen. Wenn aber die formulierten Sicherheitsziele und die vorhandenen finanziellen, technischen oder personellen Möglichkeiten zu weit auseinander liegen, müssen sowohl die Sicherheitsziele als auch die Geschäftsprozesse grundsätzlich überdacht werden. In diesem Fall muss auch die Leitungsebene über diese Diskrepanz informiert werden, damit sie gegebenenfalls Korrekturmaßnahmen veranlassen kann.

Bei der Festlegung von Sicherheitsmaßnahmen sollten immer die für die Umsetzung benötigten personellen und finanziellen Ressourcen konkret genannt werden. Hierzu gehört die Benennung von Verantwortlichen und anderen Ansprechpartnern, aber auch die Festlegung genauer Terminpläne und der zu beschaffenden Materialien. Es empfiehlt sich außerdem, bei allen geplanten Sicherheitsmaßnahmen zu dokumentieren, ob die für Informationssicherheit eingeplanten Ressourcen termingerecht bereitgestellt wurden und was die Gründe für Projektabweichungen waren. Nur so lassen sich nachhaltige Verbesserungen erreichen und Störungen vermeiden.

Ressourcen für die Überprüfung der Informationssicherheit

Alle Sicherheitsmaßnahmen müssen regelmäßig auf ihre Wirksamkeit und Eignung geprüft werden. Auch hierfür müssen ausreichende Ressourcen bereitgestellt werden. Generell sollten nicht diejenigen, die Sicherheitsmaßnahmen konzipiert haben, deren Wirksamkeit und Eignung prüfen. Hierfür kann auch externer Sachverstand hinzugezogen werden, um Betriebsblindheit zu vermeiden.

Die Frage, ob ausreichende Ressourcen für Informationssicherheit bereitgestellt werden, ist wesentlich schwieriger zu beantworten als die Überprüfung von rein technischen Aspekten.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

ISMS.1.M16 Erstellung von zielgruppengerechten Sicherheitsrichtlinien (CIA)

Zielgruppengerechte Vermittlung von Sicherheitsthemen

Ein wichtiger Erfolgsfaktor für die Erreichung eines angemessenen Sicherheitsniveaus sind verantwortungsbewusste und kompetente Mitarbeiter, die koordiniert zusammenarbeiten. Dabei bringen Management, IT-Benutzer, Administratoren und Sicherheitsexperten sehr individuelle fachliche Voraussetzungen mit und nehmen unterschiedliche Aufgaben wahr. Während die Unternehmens- bzw. Behördenleitung die Gesamtverantwortung trägt, Ziele vorgibt und Rahmenbedingungen definiert, müssen Administratoren technisch hochqualifiziert sein und Detailwissen besitzen, um IT-Systeme bedienen und sicher konfigurieren zu können.

Sicherheitsverantwortliche sind mit den IT-Grundschutz-Katalogen in der Lage, ein ganzheitliches Sicherheitskonzept zu erstellen. Dieses wird oftmals viele Seiten umfassen, wenn alle Bereiche der Informationssicherheit damit abgedeckt werden sollen. Eine zusätzliche zielgruppengerechte Aufbereitung und Vermittlung der Inhalte des Sicherheitskonzepts ist eine wichtige Aufgabe des Sicherheitsmanagements. Das Ziel ist, dass alle Mitarbeiter die sie und ihren Arbeitsbereich betreffenden Sicherheitsaspekte kennen und beachten.

Es empfiehlt sich daher, unterschiedliche Sicherheitsrichtlinien oder ausführliche Teilkonzepte zu erstellen, die einzelne Sicherheitsthemen bedarfsgerecht darstellen. Damit erhalten Mitarbeiter genau die Informationen, die sie zu einem bestimmten Thema wirklich benötigen.

Separate Sicherheitsrichtlinien für IT-Systeme oder Dienstleistungen, die sich in einem sicherheitskritischen Bereich befinden, deren Konfiguration kompliziert ist oder deren Anwendung komplex ist, können technische Anweisungen für Administratoren enthalten, die nicht allgemein verständlich sind. In den Dokumenten für die Mitarbeiter sollten Sicherheitsthemen dagegen angemessen aufbereitet und nicht mit unnötigen Details versehen sein.

Hierarchischer Aufbau von Richtlinien

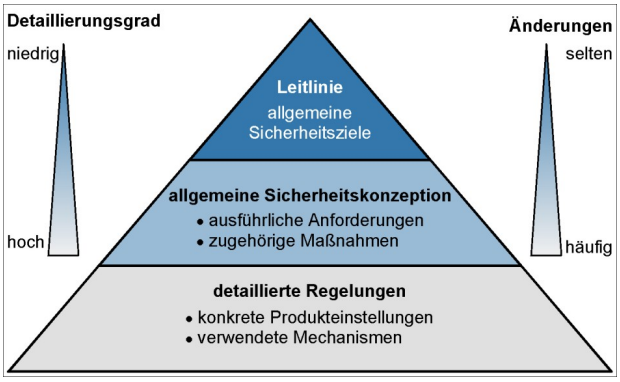
Bei der Formulierung von Richtlinien hat es sich bewährt, auf verschiedenen Ebenen zu arbeiten.

Zunächst sollten in der ersten Ebene kurz und prägnant die allgemeinen Sicherheitsziele und die Sicherheitsstrategie in einer Leitlinie zur Informationssicherheit formuliert werden (siehe ISMS.1.M3 Erstellung einer Leitlinie zur Informationssicherheit). Die Strategie enthält keine technischen Details und wird vom Management verabschiedet. In der nächsten Ebene sollten hieraus grundlegende technische Sicherheitsanforderungen abgeleitet werden.

Zur allgemeinen Sicherheitskonzeption gehören Dokumente, die verschiedene Aspekte der Informationssicherheit beschreiben (z. B. eine Richtlinie zur Internetnutzung oder ein Virenschutzkonzept), ohne auf konkrete Produkte einzugehen.

In der dritten Ebene werden technische Details, konkrete Maßnahmen und produktspezifische Einstellungen beschrieben. Sie enthält viele Dokumente, die regelmäßig geändert und typischerweise nur von den zuständigen Experten gelesen werden.

Die nachstehende Abbildung stellt den hier beschriebenen Aufbau graphisch dar.



Hierarchie von Sicherheitsrichtlinien

Inhalt von speziellen Sicherheitsrichtlinien

Folgende Themen eignen sich beispielsweise zur zielgruppengerechten Aufbereitung in spezielle Sicherheitsrichtlinien:

- Verhaltensregeln und Sicherheitshinweise für IT-Benutzer
- Verhaltensregeln und Sicherheitshinweise für Administratoren
- Sicherheitsgateways
- Virenschutz, Schadprogramme
- Notfallvorsorge
- Datensicherung
- Archivierung
- Sichere Nutzung von E-Mail und Groupware
- Outsourcing, externe Dienstleister

Sicherheitsrichtlinie zur IT-Nutzung

Oft empfiehlt es sich, die allgemeinen Zielvorgaben der Leitlinie zur Informationssicherheit in einer Sicherheitsrichtlinie zur IT-Nutzung zu konkretisieren und die wichtigsten organisationsweiten Maßnahmen des Sicherheitskonzeptes allgemeinverständlich, ohne technische Details, in einer Richtlinie zusammenzufassen. Diese Richtlinie beschreibt die Grundzüge der organisationsweiten IT-Nutzung und führt die Mitarbeiter durch das Sicherheitskonzept.

Folgende Themen könnten in einer allgemeinen Sicherheitsrichtlinie zur IT-Nutzung behandelt werden:

- Umgang mit schützenswerten Informationen (Festlegung von Informationseigentümern, Pflicht zur Klassifizierung von Informationen nach Schutzbedürftigkeit)
- relevante Gesetze und Vorgaben
- Kurzbeschreibung wichtiger Rollen (z. B. Informationssicherheitsbeauftragter, Administrator, Benutzer)
- Ausbildung des Personals
- Pflicht zur Einrichtung von Vertretungsregelungen
- Anforderungen an die Verwaltung von IT (Beschaffung, Einsatz, Wartung, Revision und Entsorgung)
- grundlegende Sicherheitsmaßnahmen (Zutritt zu Räumen und Zugang zu IT-Systemen, Verschlüsselung, Virenschutz, Datensicherung, Notfallvorsorge)
- Regelungen für spezifische IT-Dienste (Datenübertragung, Internetnutzung, Cloud-Nutzung)

Das BSI stellt auf seinen Webseiten im Bereich IT-Grundschutz verschiedene Musterrichtlinien und -konzepte als Beispiele zur Verfügung.

ISMS.1.M17 Abschließen von Versicherungen (A)

Jede Institution muss entscheiden, wie mit den Restrisiken umgegangen wird, die auch nach Umsetzung von Sicherheitsmaßnahmen verbleiben. Durch das Abschließen einer Versicherung kann der finanzielle Schaden gesenkt werden. Auch Folgeschäden, die durch den Ausfall der betroffenen Geschäftsprozesse entstehen, können durch entsprechende Versicherungen (z. B. Versicherung gegen Betriebsunterbrechungen durch Feuer) teilweise versichert werden. Zu beachten ist aber, dass es auch nicht versicherbare Restrisiken geben kann. Dies betrifft beispielsweise Imageschäden. Bei Abschluss einer Versicherung sollten daher die besonderen Rahmenbedingungen und etwaige Ausschlussklauseln berücksichtigt werden. Zu beachten ist auch, dass eventuell eine längere Zeitspanne finanziell überbrückt werden muss, bis die Versicherung den Schaden ersetzt.

Die Versicherungsarten lassen sich gliedern in:

- Drittschaden (Haftpflichtversicherung)
- Personen-, Sachschäden inklusive Umweltschäden sowie Vermögensschäden
- Eigenschaden (Sachversicherung, inklusive Softwareschäden)
- Gebäudeversicherung
- Sachinhaltsversicherung
- Ertragsausfallversicherung (Versicherung gegen Betriebsunterbrechungen)
- Elektronikversicherung
- Vertrauensschadenversicherung (z. B. Versicherung gegen Computer-Missbrauch)
- Cyber-Versicherung
- Rechtsschutzversicherung

Unter den Hilfsmitteln zum IT-Grundschutz findet sich eine Tabelle, die einen kurzen Überblick gibt, welche Versicherungen in welchen Bereichen helfen können, die finanziellen Auswirkungen von potenziellen Schäden zu reduzieren.

3 Weiterführende Informationen

3.1 Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Sicherheitsmanagement" finden sich unter anderem in folgenden Veröffentlichungen:

[27000] ISO/IEC 27000:2016

Information technology - Security techniques - Information security management systems - Overview and vocabulary, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/SC 27, Februar 2016

[27001] ISO/IEC 27001:2013

Information technology-Security techniques-Information security management systems-Requirements, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/SC 27, Oktober 2013

[BSI1] Managementsysteme für Informationssicherheit (ISMS)

BSI-Standard 200-1, Version 1.0, Oktober 2017, https://www.bsi.bund.de/grundschutz

[BSI2] IT-Grundschutz-Methodik

BSI Standard 200-2, Version 1.0, Oktober 2017, https://bsi.bund.de/grundschutz

[GSKHÜB] Tabelle Versicherungs-Check für IT-Unternehmen und Rechenzentren

Hilfmittel IT-Grundschutz, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Hilfsmittel/ChecklistenundFormulare/checklistenundformulare_node.html, zuletzt abgerufen am 05.10.2018

[ISF] The Standard of Good Practice for Information Security:

Information Security Forum (ISF), June 2018

[NIST80053] Security and Privacy Controls for Federal Information Systems and Organizations

NIST Special Publication 800-53, Revision 4, April 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf , zuletzt abgerufen am 30.08.2018

Bundesamt
für Sicherheit in der
Informationstechnik

Umsetzungshinweise für die Bausteinschicht ORP

Umsetzungshinweise zum Baustein ORP.1 Organisation

1 Beschreibung

1.1 Einleitung

Jedes Unternehmen und jede Behörde muss eine Organisation haben, die das Zusammenspiel der verschiedenen Rollen und Einheiten mit den Geschäftsprozessen und Ressourcen in der Institution steuert. Die meisten Institutionen haben eine Organisationseinheit, die für Regelung und Steuerung des allgemeinen Betriebs sowie für Planung, Organisation und Durchführung aller Verwaltungsdienstleistungen verantwortlich ist. Diverse Aufgaben der Informationssicherheit müssen von dieser Einheit umgesetzt oder mitgetragen werden.

1.2 Lebenszyklus

Ein angemessenes Sicherheitsniveau kann in einer Institution nur erreicht werden, wenn übergreifende Regelungen zur Informationssicherheit verbindlich festgelegt werden. Hierzu sind eine Reihe von Maßnahmen umzusetzen, beginnend mit Festlegung und Zuweisung von verantwortlichen Personen für einzelne Objekte (z. B. Informationen, Geschäftsprozesse, Anwendungen, IT-Komponenten) über entsprechende organisatorische Sicherheitsrichtlinien und Handlungsanweisungen bis hin zur Behandlung von schützenswerten Betriebsmitteln. Die Schritte, die dabei im Sinne eines kontinuierlichen, sich wiederholenden Informationssicherheitsprozesses durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Planung und Konzeption

Für die Initiierung und die Umsetzung der sich aus den Sicherheitszielen und Sicherheitsrichtlinien ergebenden Prozesse sind organisatorische und personelle Festlegungen zu treffen. Hierbei sind gegebenenfalls die Mitbestimmungsrechte der Personalvertretung zu wahren (siehe ORP.1.M10 Rechtzeitige Beteiligung des Personal-/Betriebsrates). Die verschiedenen Organisationsebenen und die hier tätigen Personen benötigen konkrete Handlungsanweisungen und Verantwortlichkeiten zur Abwicklung der sie betreffenden Prozesse (siehe ORP.1.M2 Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten).

Die strategischen Überlegungen sind in einem Betriebskonzept bezüglich ihrer Umsetzung im Unternehmen bzw. in der Behörde zu detaillieren.

Der Einsatz der erforderlichen Betriebsmittel ist auf die Aufgabenerfüllung und die Sicherheitsanforderungen abzustimmen und über eine Betriebsmittelverwaltung (siehe ORP.1.M7 Betriebsmittelverwaltung) zu dokumentieren. Diese muss vollständig sein und durch entsprechende Prozesse auch jederzeit aktuell gehalten werden.

Voraussetzung für eine funktionierende Infrastruktur, die auch auf Störungen adäquat reagieren kann, sind Regelungen für Ersatzteilbeschaffung, Reparaturen und Wartungsarbeiten (siehe ORP.1.M11 Regelungen für Wartungs- und Reparaturarbeiten). In Wartungsverträgen ist die terminliche und inhaltliche Wartung einzelner IT-Systeme (oder Gruppen) verbindlich zu regeln, ebenso wie die erforderlichen Zugänge (Remote, vor Ort) und die an die Sicherheitsanforderungen angepassten Reaktionszeiten des mit der Wartung beauftragten Personals.

Die Aufgabenverteilung und die hierfür erforderlichen Funktionen (siehe ORP.1.M4 Funktionstrennung zwischen operativen und kontrollierenden Aufgaben) sind so zu strukturieren, dass operative und kontrollierende Funktionen auf verschiedene Personen verteilt werden, um Interessenskonflikte bei den handelnden Personen zu minimieren oder ganz auszuschalten.

Betrieb

Die festgelegten Konzeptionen werden in konkrete Handlungsanweisungen gefasst und für den Betrieb verbindlich verabschiedet. Mitarbeiterbezogene Regelungen müssen hierbei die komplette Laufbahn eines Mitarbeiters in der Institution vom Eintritt bis zum Austritt betrachten. Durch Anwendung des Need-to-Know-Prinzips und des Vier-Augen-Prinzips ist sicher zu stellen, das Berechtigungen auf den verschiedenen Ebenen (z. B. Zutritt zu Räumen, Zugang zu Informationssystemen) zielgerichtet vergeben werden und auch praktikabel sind (siehe ORP.1.M5 Vergabe von Berechtigungen).

Diese Berechtigungen sind zu dokumentieren und durch verschiedene Methoden zu unterstützen, wie z. B. kontrollierte und nachweisbare Ausgabe von Schlüsseln nur an Berechtigte, Authentisierung von Zugriffen, Zutrittskontrollsysteme für speziell gesicherte Bereiche und Kontrolle der Aktionen Betriebsfremder (siehe ORP.1.M3 Beaufsichtigung oder Begleitung von Fremdpersonen). Werden Regelungen bewusst oder unbewusst verletzt, so müssen die hieraus ableitbaren Informations- und Eskalationsprozesse den Mitarbeitern bekannt sein, so dass eine zielgerichtete Reaktion auf die Verletzung erfolgen kann (siehe ORP.1.M9 Reaktion auf Verletzungen der Sicherheitsvorgaben).

Aussonderung

Datenträger, Betriebs- und Sachmittel, die besonderen Schutzbedingungen unterliegen, sind so zu entsorgen, dass keine Rückschlüsse auf ihre Verwendung oder Inhalte gemacht werden können (siehe ORP.1.M8 Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln). Hierzu sind entsprechende Regelungen, gegebenenfalls auch mit externen Firmen, zu treffen. Entsprechende Bestimmungen des Datenschutzes sind zu beachten.

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Organisation" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

ORP.1.M1 Festlegung von Verantwortlichkeiten und Regelungen [Institutionsleitung]

Für alle wesentlichen Aufgaben und Geschäftsprozesse in einer Institution sollten die Verantwortlichkeiten nachvollziehbar geregelt sein. Die Aufgaben sollten dabei so zugeschnitten sein, dass es keine Überschneidungen zwischen ähnlichen Aufgaben gibt, aber auch keine Zuständigkeitslücken. Dies sollte für alle Bereiche eine Selbstverständlichkeit sein, für alle sicherheitsrelevanten Aufgaben ist es aber unabdingbar.

Die sicherheitsrelevanten Aufgaben aller internen und externen Mitarbeiter und Dienstleister müssen nachvollziehbar festgelegt sein. Sie müssen mit den Sicherheitszielen der Institution abgestimmt sein. Zu den Bereichen, die geregelt werden sollten, gehören beispielsweise:

- explizite Zuweisung der Verantwortlichkeiten und Befugnisse an Rollen bzw. Organisationseinheiten bei allen sicherheitsrelevanten Aufgaben (Dabei ist sicherzustellen, dass alle Rollen konkreten Personen zugeordnet sind),
- geeigneter Umgang mit geschäftskritischen Informationen, so dass deren Vertraulichkeit, Integrität und Verfügbarkeit angemessen geschützt sind,
- Vertraulichkeitsvereinbarungen,
- Einbeziehung des Sicherheitsbeauftragten bei Aufträgen und Projekten, die geschäftskritische Informationen betreffen,
- Unterrichtungen über den geeigneten Umgang mit geschäftskritischen Informationen, beispielsweise im Kontakt mit Kunden oder auf Reisen,
- Festlegung von Verhaltensregeln und Informationspflichten bei sicherheitsrelevanten Aktionen und bei Sicherheitsvorfällen,
- Klassifikation von Informationen entsprechend ihres Schutzbedarfs.

Die Regelungen für Informationssicherheit sollten mit denen für Datenschutz und Geheimschutz in geeigneter Weise zusammengeführt werden, damit sie von den Mitarbeitern leichter adaptiert und besser wahrgenommen werden können. Wichtig ist auch, dass alle Regelungen zusammengenommen widerspruchsfrei sind.

Übergreifende Regelungen zur Informationssicherheit müssen verbindlich festgelegt werden.

Es empfiehlt sich, Regelungen unter anderem über die Themen

- Datensicherung,
- Datenarchivierung,
- Datenträgertransport,
- Datenübertragung,
- Datenträgervernichtung,
- Dokumentation von IT-Verfahren, Software, IT-Konfiguration,
- Zutritts-, Zugangs- und Zugriffsberechtigungen,
- Wartungs- und Reparaturarbeiten,
- Datenschutz,
- Schutz gegen Schadsoftware,
- Revision,
- Notfallvorsorge und
- Vorgehensweise bei der Verletzung von Sicherheitsrichtlinien

zu treffen. Weitere Hinweise dazu finden sich in den jeweils relevanten IT-Grundschutz-Bausteinen.

Sollen zwischen zwei oder mehreren Kommunikationspartnern Informationen ausgetauscht werden, so sind zu deren Schutz eine Reihe von unterschiedlichen Aspekten zu beachten. Bei jeder Art von Informationsaustausch ist zunächst zu klären,

- wie schutzbedürftig diese sind,
- mit wem diese ausgetauscht werden dürfen und
- wie diese dabei zu schützen sind.

Hierfür sollten klare und verständliche Regelungen vorliegen, die alle Formen des Informationsaustausches abdecken, also zum Beispiel den mündlichen Austausch ebenso wie Datenaustausch per Datenträger, Mail, Fax, (Mobil-) Telefon oder Internet. Generell sollte sichergestellt sein, dass Informationen nicht in falsche Hände, Augen und Ohren gelangen können und sie nicht unbemerkt verändert werden können. Allen Mitarbeitern sollte bewusst sein, dass sie dafür verantwortlich sind, interne Informationen angemessen zu schützen. Wie analoge und elektronische Informationen beim Informationsaustausch zu schützen sind, ist unter anderem ausführlich in den Bausteinen OPS.1.2.3 Informations- und Datenträgeraustausch und APP.1.1 E-Mail/Groupware beschrieben.

Die in Kraft gesetzten Regelungen sind den betroffenen Mitarbeitern in geeigneter Weise bekannt zu geben (siehe ORP.5 Anforderungsmanagement (Compliance)). Es empfiehlt sich, die Kenntnisnahme durch die Mitarbeiter zu dokumentieren. Darüber hinaus sind sämtliche Regelungen in der aktuellen Fassung an einer Stelle vorzuhalten und bei berechtigtem Interesse zugänglich zu machen.

Die getroffenen Regelungen sind regelmäßig zu aktualisieren, um Missverständnisse, ungeklärte Zuständigkeiten und Widersprüche zu vermeiden und gegebenenfalls aufzulösen. Alle Regelungen sollten deshalb auch ein Erstellungsdatum oder eine Versionsnummer enthalten.

ORP.1.M2 Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten [Informationssicherheitsbeauftragter (ISB), Institutionsleitung, Leiter IT]

Um zu einer umfassenden Gesamtsicherheit zu gelangen, ist die Beteiligung aller Mitarbeiter einer Institution an der Umsetzung der erforderlichen Sicherheitsmaßnahmen erforderlich. Für alle Informationen, Geschäftsprozesse, Anwendungen und IT-Komponenten muss daher festgelegt werden, wer für diese und deren Sicherheit verantwortlich ist. Hierfür sollte immer eine konkrete Person (inklusive Vertreter) und keine abstrakte Gruppe benannt werden, damit die Zuständigkeit jederzeit deutlich erkennbar ist. Bei komplexeren Informationen, Anwendungen und IT-Komponenten sollten alle Verantwortlichen und deren Vertreter namentlich genannt sein.

Umgekehrt sollten natürlich alle Mitarbeiter wissen, für welche Informationen, Geschäftsprozesse, Anwendungen und IT-Komponenten sie in welcher Weise verantwortlich sind.

Jeder Mitarbeiter ist dabei für das verantwortlich, was in seinem Einflussbereich liegt, es sei denn, es ist explizit anders geregelt. Beispielsweise ist die Leitungsebene der Institution verantwortlich für alle grundsätzlichen Entscheidungen bei der Einführung einer neuen Anwendung, der Leiter IT zusammen mit dem Informationssicherheitsmanagement für die Ausarbeitung von Sicherheitsvorgaben für die IT-Komponenten, die Administratoren für deren korrekte Umsetzung und die Benutzer für den sorgfältigen Umgang mit den zugehörigen Informationen, Anwendungen und Systemen.

Die Fachverantwortlichen als die "Eigentümer" von Informationen und Anwendungen müssen sicherstellen, dass

- der Schutzbedarf der Informationen, Geschäftsprozessen, Anwendungen und IT-Komponenten korrekt festgestellt wurde,
- die erforderlichen Sicherheitsmaßnahmen umgesetzt werden,
- dies regelmäßig (z. B. täglich, wöchentlich, monatlich) überprüft wird,
- die Aufgaben für die Umsetzung der Sicherheitsmaßnahmen klar definiert und zugewiesen werden,
- der Zugang bzw. Zugriff zu den Informationen, Anwendungen und IT-Komponenten geregelt ist,
- die Informationssicherheit gefährdende Abweichungen schriftlich dokumentiert werden.

Die Fachverantwortlichen müssen zusammen mit dem Informationssicherheitsmanagement entscheiden, wie mit eventuellen Restrisiken umgegangen wird.

ORP.1.M3 Beaufsichtigung oder Begleitung von Fremdpersonen [Mitarbeiter]

Personen, die nicht der Institution angehören, wie Besucher, Handwerker, Wartungs- und Reinigungspersonal sollten, außer in Räumen, die ausdrücklich dafür vorgesehen sind, nicht unbeaufsichtigt sein (siehe auch ORP.1.M5 Vergabe von Berechtigungen). Alle Mitarbeiter sollten darauf hingewiesen werden, dass sie Betriebsfremde, die sie unbeaufsichtigt innerhalb der Behörde oder des Unternehmens antreffen, von diesem Moment an unter ihre Obhut nehmen müssen. Dies dient nicht nur der Sicherheit aller, sondern ist auch ein positiver Serviceaspekt für Betriebsfremde.

Wird es erforderlich, einen Externen allein im Büro zurückzulassen, sollte ein Kollegen ins Zimmer oder der Besucher zu einem Kollegen gebeten werden.

Ist es nicht möglich, Fremdpersonen (z. B. Reinigungspersonal) ständig zu begleiten oder zu beaufsichtigen, sollten zumindest am persönlichen Arbeitsbereich keine Informationen und Geräte frei zugänglich sein, also beispielsweise Schränke abgeschlossen und bei IT-Geräten Zugriffssperren aktiviert sein, siehe auch ORP.1.M6 Der aufgeräumte Arbeitsplatz.

Für den häuslichen Arbeitsplatz gilt, dass Familienmitglieder und Besucher sich nur dann alleine im Arbeitsbereich aufhalten dürfen, wenn alle Arbeitsunterlagen verschlossen aufbewahrt sind und die IT über einen aktivierten Zugriffsschutz gesichert ist.

Die Notwendigkeit dieser Maßnahme ist den Mitarbeitern zu erläutern und in einer Sicherheitsrichtlinie festzuhalten. Eine Dokumentation über den Aufenthalt von Fremdpersonen kann in einem Besucherbuch geführt werden.

ORP.1.M4 Funktionstrennung zwischen operativen und kontrollierenden Aufgaben

In jeder Institution müssen die Aufgaben, die zur Durchführung der Geschäftsprozesse erforderlich sind, festgelegt und Rollen bzw. Personen zugewiesen werden. Dabei muss beachtet werden, dass es Aufgaben gibt, die sich nicht miteinander kombinieren lassen.

Die Verantwortlichkeiten für alle Geschäftsprozesse und der damit zusammenhängenden Aufgaben müssen eindeutig festgelegt werden (siehe ORP.1.M1 Festlegung von Verantwortlichkeiten und Regelungen). Die Abgrenzungen und Überschneidungen zwischen den verschiedenen Rollen und Funktionen müssen klar definiert sein. Die Aufgaben und die hierfür erforderlichen Rollen und Funktionen müssen so strukturiert sein, dass operative und kontrollierende Funktionen auf verschiedene Personen verteilt werden, um Interessenskonflikte bei den handelnden Personen zu verhindern (Funktionstrennung).

Es ist eine **Funktionstrennung** festzulegen und zu begründen, d. h. welche Funktionen bzw. Rollen nicht miteinander vereinbar sind, also auch nicht von **einer** Person gleichzeitig wahrgenommen werden dürfen. Vorgaben hierfür können aus den Aufgaben selbst oder aus gesetzlichen Bestimmungen resultieren. **Beispiele** dafür sind:

- Rechteverwaltung und Revision,
- Netzadministration und Revision,
- Programmierung und Test bei eigenerstellter Software,
- Datenerfassung und Zahlungsanordnungsbefugnis,
- Revision und Zahlungsanordnungsbefugnis.

Insbesondere wird deutlich, dass meistens operative Funktionen nicht mit kontrollierenden Funktionen vereinbar sind.

Nach der Festlegung der einzuhaltenden Funktionstrennung kann die Zuordnung der Funktionen zu Personen erfolgen. Vertreterregelungen sind ebenfalls zu berücksichtigen und zu dokumentieren (siehe auch ORP.2 Personal).

Die getroffenen Festlegungen sind zu dokumentieren und bei Veränderungen in Geschäftsprozessen zu aktualisieren. Sollte bei dieser Zuordnung eine Person miteinander unvereinbare Funktionen wahrnehmen müssen, so ist dies in einer entsprechenden Dokumentation über die Funktionsverteilung besonders hervorzuheben.

ORP.1.M5 Vergabe von Berechtigungen [Leiter IT]

Auf den verschiedenen Ebenen MÜSSEN angemessene und praktikable Berechtigungen vergeben werden (z. B. für den Zutritt zu Räumen, Zugang zu IT-Systemen, Zugriff auf Anwendungen). Es sollten immer nur so viele Rechte vergeben werden, wie es für die Aufgabenwahrnehmung notwendig ist. Es muss ein geregeltes Verfahren für die Vergabe, die Verwaltung und den Entzug von Berechtigungen geben (siehe auch ORP.4. Identitäts- und Berechtigungsmanagement).

Vergabe von Zutrittsberechtigungen

Vor der Vergabe von Zutrittsberechtigungen für Personen sind die schutzbedürftigen Räume eines Gebäudes zu bestimmen, z. B. Büro, Datenträgerarchiv, Serverraum, Technikraum, Rechenzentrum. Der Schutzbedarf eines Raumes leitet sich ab aus dem Schutzbedarf der im jeweiligen Raum verarbeiteten Informationen, der dort vorhandenen IT-Systeme und der Datenträger, die in diesem Raum gelagert und benutzt werden.

Anschließend ist festzulegen, welche Person zur Ausübung der wahrgenommenen Funktion welches Zutrittsrecht benötigt. Dabei ist die vorher erarbeitete Funktionstrennung (ORP.1. M4 Funktionstrennung zwischen operativen und kontrollierenden Aufgaben) zu beachten. Unnötige Zutrittsrechte sind zu vermeiden.

Um die Zahl zutrittsberechtigter Personen zu einem Raum möglichst gering zu halten, sollte der Grundsatz der Funktionstrennung berücksichtigt werden. So verhindert z. B. eine getrennte Lagerung von IT-Ersatzteilen und Datenträgern den unerlaubten Zugriff eines Wartungstechnikers auf die Datenträger.

Die Vergabe und Rücknahme von Zutrittsberechtigungen ist zu dokumentieren. Bei der Rücknahme einer Zutrittsberechtigung muss die Rücknahme der Zutrittsmittel gewährleistet sein. Zusätzlich ist zu dokumentieren, welche Konflikte bei der Vergabe der Zutrittsberechtigungen an Personen aufgetreten sind. Gründe für Konflikte können vorliegen, weil Personen Funktionen wahrnehmen, die bezüglich der Zutrittsberechtigungen der Funktionstrennung entgegenstehen, oder aufgrund räumlicher Notwendigkeiten.

Zur Überwachung der Zutrittsberechtigung können Personen (Pförtner, Schließdienst) oder technische Einrichtungen (Ausweisleser, biometrische Verfahren wie Irisscanner oder Fingerabdruck, Sicherheitstürschloss bzw. Schließanlage) eingesetzt werden (siehe INF.1 Gebäude). Der Zutritt zu schutzbedürftigen Räumen von nicht autorisiertem Personal (z. B. Besuchern, Reinigungs- und Wartungspersonal) darf nur bei Anwesenheit oder in Begleitung Zutrittsberechtigter erfolgen.

Regelungen über die Vergabe und Rücknahme von Zutrittsberechtigungen für Fremdpersonal und Besucher müssen ebenfalls getroffen werden.

Vergabe von Zugangsberechtigungen

Zugangsberechtigungen erlauben der betroffenen Person oder einem autorisierten Vertreter, bestimmte IT-Systeme bzw. System-Komponenten und Netze zu nutzen. Zugangsberechtigungen sollten möglichst restriktiv vergeben werden. Diese sind für jede nutzungsberechtigte Person aufgrund ihrer Funktion, unter Beachtung der Funktionstrennung (siehe ORP.1.M4 Funktionstrennung zwischen operativen und kontrollierenden Aufgaben), im Einzelnen festzulegen. Entsprechend der Funktion ist der Zugang zu den IT-Systemen zu definieren, z. B. Zugang zum Betriebssystem (Systemverwalter) oder Zugang zu einer IT-Anwendung (Benutzer). Ergänzend hierzu muss sichergestellt sein, dass personelle und aufgabenbezogene Änderungen unverzüglich berücksichtigt werden.

Der Zugang zu IT-Systemen oder IT-Anwendungen sollte erst nach einer Identifikation (z. B. durch Name, Benutzer-Kennung oder Chipkarte) und Authentifizierung (z. B. durch ein Passwort oder über ein Authentisierungstoken) des Nutzungsberechtigten möglich sein und protokolliert werden.

Die Ausgabe bzw. der Entzug von Zugangsmitteln wie Benutzer-Kennungen oder Chipkarten ist zu dokumentieren. Regelungen über die Handhabung von Zugangs- und Authentisierungsmitteln (z. B. Umgang mit Chipkarten, Passworthandhabung, siehe ORP.4 Identitäts- und Berechtigungsmanagement) müssen ebenfalls getroffen werden. Alle Zugangsberechtigten müssen auf den korrekten Umgang mit den Zugangsmitteln hingewiesen werden.

Zugangsberechtigungen sollten bei längeren Abwesenheiten von berechtigten Personen vorübergehend gesperrt werden, um Missbrauch zu verhindern, z. B. bei Krankheit oder Urlaub. Dies sollte zumindest bei Personen mit weitreichenden Berechtigungen wie Administratoren erfolgen.

Die korrekte Einhaltung ist sporadisch zu kontrollieren.

Vergabe von Zugriffsrechten

Über Zugriffsrechte wird geregelt, welche Personen im Rahmen ihrer Funktionen bevollmächtigt werden, IT-Anwendungen oder Daten zu nutzen. Die Zugriffsrechte (z. B. Lesen, Schreiben, Ausführen) auf IT-Anwendungen, Teilanwendungen oder Daten sind von der Funktion abhängig, die eine Person wahrnimmt, z. B. Anwenderbetreuung, Arbeitsvorbereitung, Systemprogrammierung, Anwendungsentwicklung, Systemadministration, Revision, Datenerfassung, Sachbearbeitung. Dabei sollten immer nur so viele Zugriffsrechte vergeben werden, wie es für die Aufgabenwahrnehmung notwendig ist ("Need-to-know-Prinzip"). Umgesetzt werden müssen die Zugriffsrechte durch die Rechteverwaltung der jeweiligen IT-Systeme.

Eine Vielzahl von IT-Systemen lässt es zu, dass verschiedene Rechte als Gruppenrechte bzw. als Rechteprofil definiert werden (z. B. Gruppe Datenerfassung). Diese Definition entspricht der technischen Umsetzung der Rechte, die einer Funktion zugeordnet werden. Für die Administration der Rechte eines IT-Systems ist es vorteilhaft, solche Gruppen oder Profile zu erstellen, da damit die Rechtezuteilung und deren Aktualisierung erheblich vereinfacht werden kann.

Die Festlegung und Veränderung von Zugriffsrechten ist vom jeweils Verantwortlichen zu veranlassen und zu dokumentieren. Aus der Dokumentation muss hervorgehen:

- welche Funktion unter Beachtung der Funktionstrennung (siehe ORP.1.M4 Funktionstrennung zwischen operativen und kontrollierenden Aufgaben) mit welchen Zugriffsrechten ausgestattet wird,
- welche Gruppen bzw. Profile eingerichtet werden,
- welche Person welche Funktion wahrnimmt,
- welche Zugriffsrechte eine Person im Rahmen welcher Rolle erhält (hierbei sollten auch die Zugriffsrechte von Vertretern erfasst werden) und
- welche Konflikte bei der Vergabe von Zugriffsrechten aufgetreten sind. Diese Konflikte können z. B. daraus resultieren, dass eine Person unvereinbare Funktionen wahrnimmt oder daraus, dass abhängig vom IT-System die Trennung bestimmter Zugriffsrechte nicht vorgenommen werden kann.
- welche Personen in einem Notfall welche Zugriffsrechte erhalten, z. B. da sie zum Krisenstab gehören.

Die Vorgehensweise bei der Funktionstrennung und der Rechtevergabe wird am nachfolgenden Beispiel erläutert.

Die betrachtete Anwendung ist ein Reisekosten-Abrechnungssystem. Die relevanten Räume sind in nachfolgender Graphik erläutert. Das IT-System besteht aus einem LAN, an dem neben einem Server und der Bedienkonsole drei PCs als Arbeitsplatzrechner angeschlossen sind.

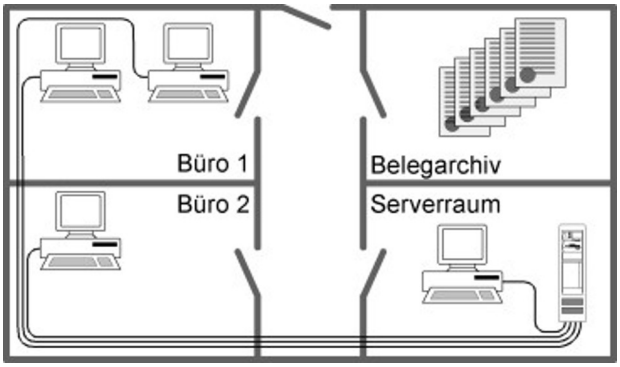


Abbildung: Aufgabenverteilung und Funktionstrennung

Schritt 1: Aufgabenverteilung und Funktionstrennung

Folgende Funktionen sind für das betrachtete Reisekosten-Abrechnungssystem notwendig:

1 LAN-Administration
2 Revision
3 Datenerfassung
4 Sachbearbeitung mit Feststellung der rechnerischen Richtigkeit
5 Sachbearbeitung mit Feststellung der sachlichen Richtigkeit
6 Sachbearbeitung mit Anordnungsbefugnis

Folgende Funktionen sind aufgrund der Sachzwänge nicht miteinander vereinbar:

- Funktion 1 und Funktion 2 (die Administration darf sich nicht selbst kontrollieren)
- Funktion 2 und Funktion 6 (der Anordnungsbefugte darf sich nicht selbst kontrollieren)
- die Kombination der Funktionen 4 oder 5 mit 6 (das Vier-Augen-Prinzip wäre verletzt für Zahlungsanweisungen)

Diese Funktionen werden durch folgende Personen wahrgenommen:

		Hr. Mayer	Fr. Schmidt	Hr. Müller	Fr. Fleiß
1.	LAN-Administration	X			
2.	Revision		X		
3.	Datenerfassung			X	
4.	Sachbearbeitung rechn.			X	
5.	Sachbearbeitung sachl.			X	
6.	Anordnungs-befugnis				X

Tabelle 1: Beispiel für Aufgabenverteilung und Funktionstrennung

Schritt 2: Vergabe von Zutrittsrechten

Nachfolgend wird der Schutzbedarf der einzelnen Räume begründet und in der Tabelle die Vergabe der Zutrittsrechte dokumentiert:

- Serverraum:
  Der unbefugte Zutritt zum Server muss verhindert werden, weil die Verfügbarkeit, Integrität und Vertraulichkeit der gesamten Anwendung von dieser zentralen Komponente abhängig ist.
- Belegarchiv: Für die Rechnungslegung müssen die Reisekostenabrechnungen längerfristig aufbewahrt werden. Es ist sicherzustellen, dass die Belege vollständig und unverändert aufbewahrt werden.B
- Büro 1: In diesem Büro werden die notwendigen Daten erfasst sowie die rechnerische und sachliche Richtigkeit festgestellt. Für die Gewährleistung der Korrektheit dieser Vorgänge muss verhindert werden, dass Unbefugte Zutritt zu den Arbeitsplatzrechnern erhalten.
- Büro 2: Hier wird die Auszahlung der Reisekosten am APC angeordnet. Dieser Vorgang darf nur von einer befugten Person vorgenommen werden. Unbefugten ist der Zutritt zu verwehren.

		Serverraum	Belegarchiv	Büro 1	Büro 2
1.	LAN-Administration	X			
2.	Revision	X	X	X	X
3.	Datenerfassung			X	

		Serverraum	Belegarchiv	Büro 1	Büro 2
4.	Sachbearbeitung rechn.		X	X	
5.	Sachbearbeitung sachl.		X	X	
6.	Anordnungs-befugnis		X	X	X

Tabelle 2: Beispiel für die Vergabe von Zutrittsberechtigungen

Schritt 3: Vergabe von Zugangsberechtigungen

Aufgrund der Funktionen ergeben sich folgende Zugangsberechtigungen:

		Betriebssystem Server	Anwendung Protokollauswertung	Anwendung Datenerfassung	Anwendung Belegbearbeitung
1.	LAN-Administration	X			
2.	Revision	X	X		X
3.	Datenerfassung			X	
4.	Sachbearbeitung rechn.				X
5.	Sachbearbeitung sachl.				X
6.	Anordnungs-befugnis				X

Tabelle 3: Beispiel für die Vergabe von Zugangsberechtigungen

Schritt 4: Vergabe von Zugriffsrechten

Im Folgenden werden die Zugriffsrechte, die eine Funktion zur Ausübung benötigt, dargestellt. Es bezeichnen:

A = Recht zur Ausführung der Anwendung/Software

L = Leserecht auf Daten

S = Schreibrecht, d.h. Erzeugen von Daten

M = Recht zum Modifizieren von Daten

Ö = Recht zum Löschen von Daten

U = Recht zum Unterschreiben von Zahlungsanweisungen

		Betriebssystem Server	Protokollauswertung	Anwendung Datenerfassung	Anwendung Belegbearbeitung
1.	LAN-Administration	A,L,S,M,Ö			
2.	Revision	A,L	A,L,Ö		A,L
3.	Datenerfassung			A,S	

		Betriebssystem Server	Protokollauswertung	Anwendung Datenerfassung	Anwendung Belegbearbeitung
4.	Sachbearbeitung rechn.				A,L,M
5.	Sachbearbeitung sachl.				A,L,M
6.	Anordnungs-befugnis				A,L,U

Tabelle 4: Beispiel für die Vergabe von Zugriffsberechtigungen

Eine solche Dokumentation erleichtert die Rechteverteilung. Angenommen, dass Frau Schmidt den Arbeitgeber wechseln würde und ihre Stelle neu besetzt werden müsste, so lässt sich anhand der obigen Tabellen einfach feststellen, welche der ehemaligen Rechte Frau Schmidts zu löschen und für die neue Kraft einzurichten sind. Wenn die neue Kraft zusätzlich vertretungsweise die Funktion Sachbearbeitung mit Anordnungsbefugnis übernehmen soll, so wird anhand der durchzuführenden Rechteverteilung der Konflikt offenbar, dass die neue Kraft im Vertretungsfall Manipulationen unbemerkt durchführen könnte.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Organisation".

ORP.1.M6 Der aufgeräumte Arbeitsplatz [Mitarbeiter]

Alle Mitarbeiter sollten dazu angehalten werden, ihren Arbeitsplatz "aufgeräumt" zu hinterlassen. Unbefugte dürfen keine Möglichkeit haben, an fremden Arbeitsplätzen Einsicht in vertrauliche Informationen zu nehmen oder Geschäftsprozesse bzw. IT-Systeme zu manipulieren. Die Mitarbeiter müssen daher dafür sorgen, dass Unbefugte keinen Zugang zu IT-Anwendungen oder Zugriff auf Daten erhalten. Alle Mitarbeiter müssen mit der gleichen Sorgfalt ihre Arbeitsplätze überprüfen und sicherstellen, dass keine sensiblen Informationen frei zugänglich sind und die Verfügbarkeit, Vertraulichkeit oder Integrität von Daten nicht negativ beeinflusst werden kann. Es darf nicht möglich sein, dass Unbefugte auf Datenträger oder Unterlagen (z. B. Ausdrucke) zugreifen können.

Für eine kurze Abwesenheit während der Arbeitszeit ist es ausreichend, den Raum, sofern möglich, zu verschließen und/oder IT-Systeme so zu sperren, dass Zugriffe nur nach erfolgreicher Authentisierung möglich sind. Bei geplanter Abwesenheit eines Mitarbeiters (z. B. längere Besprechungen, Dienstreisen, Urlaub, Fortbildungsveranstaltungen) ist der Arbeitsplatz so aufzuräumen, dass keine schutzbedürftigen Datenträger oder Unterlagen unverschlossen am Arbeitsplatz zurückgelassen werden. Dafür benötigen die Mitarbeiter ausreichend dimensionierte und verschließbare Staumöglichkeiten, wie z. B. stabile Schränke.

Auch Passwörter dürfen auf keinen Fall sichtbar (als Klebezettel am Monitor, an einem leicht zu erratenden Ort wie z. B. unter der Schreibtischauflage oder in der unverschlossenen Schreibtischschublade) aufbewahrt werden (siehe ORP.1. A7 Betriebsmittelverwaltung).

Vorgesetzte und Mitarbeiter des Sicherheitsmanagements sollten sporadisch Arbeitsplätze überprüfen, ob dort schutzbedürftige Informationen offen zugreifbar sind und die Mitarbeiter auf korrektes Aufräumen hinweisen.

ORP.1.M7 Geräteverwaltung [Leiter Haustechnik, Leiter IT, Leiter Produktion und Fertigung]

In Institutionen werden je nach Branche unterschiedlichste Geräte eingesetzt, um die Geschäftsprozesse zu unterstützen. Neben IT-Systemen, die unmittelbar als solche zu identifizieren sind, können auch viele andere Arten von Geräten Einfluss auf die Informationssicherheit haben. Zu solchen Geräten gehören beispielsweise

- ICS-Komponenten
- Klimaanlagen und andere Geräte der Haustechnik
- Kaffeemaschinen

Auch Geräte wie Kaffeemaschinen, die nicht der direkten Unterstützung der Informationsverarbeitung oder anderer Geschäftsprozesse dienen, können die Informationssicherheit beeinträchtigen, z. B. wenn ein Kabelbrand Folgeschäden nach sich zieht, aber auch, wenn Geräte dieser Art zur besseren Ressourcensteuerung ins IT-Netz integriert werden.

Daher sollte die Institution einen Überblick darüber haben, welche Geräte wo eingesetzt werden und welche Anforderungen an die Informationssicherheit sich hieraus ergeben können, wie regelmäßige Überprüfung der Betriebssicherheit, Wartung oder Einspielen von Patches.

Zur Geräteverwaltung gehören die folgenden Aufgaben:

- Beschaffung
- Prüfung vor Einsatz
- Kennzeichnung
- Bestandsführung

Bei der **Beschaffung** von Geräten egal welcher Art sollten sich die Verantwortlichen auch immer die Frage stellen, ob diese Geräte Auswirkungen auf die Informationssicherheit haben könnten. Es empfiehlt sich, dass der ISB sich gelegentlich mit den Beschaffern darüber austauscht, welche Arten von Geräten in der Institution aktuell beschafft werden oder in der Planung sind. Außerdem sollte er sie dafür sensibilisieren, dass auch Nicht-IT-Systeme IT-Funktionalitäten enthalten können (Internet of Things) und welche Arten von Cyber-Angriffen hierüber möglich sind.

Bei der Beschaffung von Geräten sollte auch geklärt werden, ob Mitarbeiter für deren Einsatz geschult werden müssen und in welchen Intervallen welche Wartungsaktivitäten erforderlich sind.

Vor Einsatz der Geräte sollten diese mit einem geregelten **Prüfverfahren** auf Betriebssicherheit und Informationssicherheit überprüft werden. Außerdem sollten folgende Schritte durchgeführt werden:

- Die Vollständigkeit von Lieferungen sollte überprüft werden, um die Verfügbarkeit aller Lieferteile zu gewährleisten.
- Mit Testläufen sollte die Betriebsfähigkeit überprüft werden.
- Die Kompatibilität neuer Komponenten mit vorhandenen sollte vor der Beschaffung überprüft werden, damit es nicht zu Fehlkäufen kommt.
- Vor dem Einsatz sollten die Geräte ein Genehmigungs- und Freigabeverfahren durchlaufen. Hierbei ist darauf zu achten, dass auch die nicht zentral beschafften Geräte ein Genehmigungs- und Freigabeverfahren durchlaufen. Auch die Nutzung privater Geräte sollte hierüber geregelt werden.

Es sollte eine **Übersicht** über die Arten und die Einsatzorte aller vorhandenen Geräte geben. Anhand einer Übersicht ist es auch möglich Vollständigkeitskontrollen durchzuführen, zu überprüfen, ob nicht genehmigte Geräte in der Institution eingesetzt werden oder ob Geräte entwendet wurden. Hierzu empfiehlt sich eine eindeutige **Kennzeichnung** der wesentlichen Geräte mit eindeutigen Identifizierungsmerkmalen (z. B. gruppierte fortlaufende Inventarnummern).

Eine solche Übersicht sollte Auskunft geben können über:

- Identifizierungsmerkmale,
- Beschaffungsquellen, Lieferzeiten,
- Verbleib der Geräte,
- Wartungsverträge, Wartungsintervalle.

Um den Missbrauch von Daten zu verhindern, muss die Löschung oder Vernichtung von Geräten geregelt sein, wenn diese in der Lage sind, Informationen zu speichern, siehe Baustein CON.6 Löschen und Vernichten.

Internet of Things (IoT)

IoT-Geräte sind häufig dadurch gekennzeichnet, dass sie überschaubare, begrenzte Außenmaße haben, oftmals preislich unterhalb von Grenzen liegen, die einen aufwendigen Beschaffungsvorgang in Institutionen nach sich ziehen, und/oder die Internet-Funktionalität nicht hervorsticht. Daher ist es wahrscheinlich, dass bei jeder Art von Übersicht oder Bestandserhebung IoT-Geräte übersehen werden. Es ist wichtig, sich darüber einen Überblick zu verschaffen, welche IoT-Geräte in der Institution derzeit oder demnächst eingesetzt werden.

Dafür kann es ein sinnvoller Ansatz für den ISB sein, in verschiedene Räumlichkeiten der Institution zu gehen und zu überlegen, welche der dort vorhandenen Komponenten Strom benötigen und ob diese über IT-Netze vernetzt sein könnten. Der ISB sollte insbesondere mit den Kollegen der Haustechnik, aber auch den anderen Geräte-Verantwortlichen sprechen und sich die Funktionalitäten der verschiedenen Geräte erläutern lassen. Die Vernetzung könnte beispielsweise über IT-Verkabelung oder WLAN mit dem LAN erfolgen, über Mobilfunk mit dem Internet, aber auch über freie WLANs in der Umgebung oder andere Funkschnittstellen wie Bluetooth erfolgen. Zusätzlich sollten regelmäßig Netzscans durchgeführt werden und dabei nach Anomalien im Netzverkehr und nach nicht zuordenbaren Geräten gesucht werden.

Geräte mit IoT-Funktionalitäten können in Institutionen beispielsweise sein:

- Durch Mitarbeiter oder Externe mitgebrachte private Geräte, z. B. Smartwatches, Fitnessarmbänder und andere Gadgets.
- Durch die Institution beschaffte und betriebene Geräte wie Brand-, Gas- und andere Warnmelder, Kaffeemaschinen oder Elemente der Gebäudesteuerung. Die Übergänge zu ICS-Systemen sind hier fließend.

Dabei sind IoT-Geräte nicht immer auf den ersten Blick als solche zu erkennen, beispielsweise wenn die IoT-Funktionalität kein kaufentscheidendes Merkmal ist, aber für den Hersteller dadurch eine für ihn gewinnbringende Datensammlung möglich wird, z. B. über Art und Menge der Verbrauchsmaterialien.

Ein Beispiel für Geräte, in denen sich IoT-Funktionalitäten verstecken könnten, sind Komfortmöbel, die sich automatisch an die jeweiligen Benutzer anpassen und nicht nur lokal die Einstellungen speichern, sondern diese über IT-Netze mit anderen Arbeitsplätzen austauschen, so dass Mitarbeiter an beliebigen Arbeitsplätzen arbeiten können ("Smart Workplaces").

ORP.1.M8 Betriebsmittelverwaltung [Leiter IT]

Als Betriebsmittel (oder Sachmittel) werden alle Arbeitsmittel bezeichnet, die zur Erfüllung einer Aufgabe oder eines Geschäftsprozesses erforderlich sind. Dazu gehören beispielsweise alle erforderlichen Werkzeuge, Einrichtungen und Möbel. Betriebsmittel für den IT-Einsatz sind Mittel wie Hardware-Komponenten (Rechner, Tastatur, Drucker usw.), Software (Systemsoftware, Individualprogramme, Standardprogramme und Ähnliches), Verbrauchsmaterial (Papier, Toner, Druckerpatronen), Datenträger (Festplatten, Wechselplatten, CD-ROMs und Ähnliches). Die Betriebsmittelverwaltung umfasst die Abwicklung der Aufgaben:

- Beschaffung der Betriebsmittel,
- Prüfung vor Einsatz,
- Kennzeichnung und
- Bestandsführung.

Die **Beschaffung** von Betriebsmitteln ist beim Einsatz von Informationstechnik von besonderer Bedeutung. Mit einem geregelten Beschaffungsverfahren lassen sich insbesondere die Ziele unterstützen, die mit dem Einsatz von Informationstechnik angestrebt werden: Leistungssteigerung, Wirtschaftlichkeit, Verbesserung der Kommunikationsmöglichkeiten.

Neben reinen Wirtschaftlichkeitsaspekten kann durch ein geregeltes Beschaffungsverfahren - das von zentraler Stelle aus vorgenommen werden kann - auch die Neu- und Weiterentwicklung im Bereich der Informationstechnik stärker berücksichtigt werden.

Eine zentrale Beschaffung sichert darüber hinaus die Einführung und Einhaltung eines "Hausstandards", der die Schulung der Mitarbeiter und Wartungsaktivitäten vereinfacht.

Mit einem geregelten **Prüfverfahren vor Einsatz** der Betriebsmittel lassen sich unterschiedliche Gefährdungen abwenden. Beispiele sind:

- Die Vollständigkeit von Lieferungen (z. B. Handbücher oder Anschlusskabel) sollte überprüft werden, um die Verfügbarkeit aller Lieferteile zu gewährleisten.
- Neue Software sowie neue vorformatierte Datenträger sollten mit einem Computer-Viren-Schutzprogramm getestet werden.
- Es sollten Testläufe neuer Software auf speziellen Test-Systemen durchgeführt werden, damit diese reibungslos in den Betrieb übernommen werden können.
- Die Kompatibilität neuer Hardware- und Softwarekomponenten mit den vorhandenen sollte vor der Beschaffung überprüft werden, damit es nicht zu Fehlkäufen kommt.

Erst mit Hilfe einer **Bestandsführung** der eingesetzten Betriebsmittel ist es möglich, den Verbrauch zu ermitteln und rechtzeitig erforderliche Nachbestellungen zu veranlassen. Darüber hinaus ermöglicht die Bestandsführung Vollständigkeitskontrollen, Überprüfung des Einsatzes von nicht genehmigter Software oder die Feststellung der Entwendung von Betriebsmitteln. Hierzu bedarf es einer eindeutigen **Kennzeichnung** der wesentlichen Betriebsmittel mit eindeutigen Identifizierungsmerkmalen (z. B. gruppierte fortlaufende Inventarnummern). Zusätzlich sollten die Seriennummern vorhandener Geräte wie Bildschirm, Drucker, Festplatten etc. dokumentiert werden, damit sie nach einem Diebstahl identifiziert werden können.

Für die Bestandsführung müssen die Betriebsmittel in Bestandsverzeichnissen aufgelistet werden. Ein solches Bestandsverzeichnis muss Auskunft geben können über:

- Identifizierungsmerkmale,
- Beschaffungsquellen, Lieferzeiten,
- Verbleib der Betriebsmittel,
- Lagervorhaltung,
- Aushändigungsvorschriften und
- Wartungsverträge, Wartungsintervalle.

Um den Missbrauch von Daten zu verhindern, muss die Löschung oder Vernichtung von Betriebsmitteln geregelt sein. Insbesondere ist der Umgang mit Altpapier zu regeln. Es muss geeignete Entsorgungsmöglichkeit für Verbrauchsgüter mit höherem Schutzbedarf geben, z. B. so genannte Schredder oder Aktenvernichter für Papier. Alles Nähere ist im Baustein CON.6 Löschen und Vernichten beschrieben.

ORP.1.M9 Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln [Informationssicherheitsbeauftragter (ISB), Mitarbeiter]

Betriebsmittel oder Sachmittel (z. B. Druckerpapier, Magnetbänder, Festplatten, CD-ROM, DVDs, USB-Sticks, Flash-Speicher oder -karten, Tonerkassetten) werden irgendwann nicht mehr benötigt oder müssen aufgrund von Defekten ausgesondert werden. Wenn sie schützenswerte Daten enthalten, müssen sie so entsorgt werden, dass keine Rückschlüsse auf vorher gespeicherte Daten möglich sind. Bei funktionstüchtigen Datenträgern sollten die Daten physikalisch gelöscht werden. Nicht funktionierende oder nur einmal beschreibbare Datenträger wie Akten oder CD-ROMs und auch DVDs müssen mechanisch zerstört werden (siehe CON.6 Löschen und Vernichten).

Die Art der Entsorgung schutzbedürftigen Materials sollte in einer speziellen Sicherheitsrichtlinie geregelt werden. In der Institution müssen die dafür benötigten Entsorgungseinrichtungen wie Aktenvernichter vorhanden sein.

Wird schutzbedürftiges Material vor der Entsorgung gesammelt, so ist die Sammlung unter Verschluss zu halten und vor unberechtigtem Zugriff zu schützen.

Soweit im Unternehmen bzw. in der Behörde keine umweltgerechte und sichere Entsorgung durchgeführt werden kann, sind damit beauftragte Unternehmen auf die Einhaltung erforderlicher Sicherheitsmaßnahmen zu verpflichten. Ein Mustervertrag findet sich unter den Hilfsmitteln zum IT-Grundschutz auf den BSI-Webseiten. Es sollte regelmäßig geprüft werden, ob der Entsorgungsvorgang verlässlich ist.

ORP.1.M10 Reaktion auf Verletzungen der Sicherheitsvorgaben [Informationssicherheitsbeauftragter (ISB)]

Es ist festzulegen, welche Reaktion auf Verletzungen der Sicherheitsvorgaben erfolgen soll, um eine klare und sofortige Reaktion gewährleisten zu können.

Untersuchungen sollten durchgeführt werden, um festzustellen, wie und wo die Verletzung entstanden ist. Anschließend müssen die angemessenen schadensbehebenden oder -mindernden Maßnahmen durchgeführt werden. Soweit erforderlich, müssen zusätzliche schadensvorbeugende Maßnahmen ergriffen werden. Die durchzuführenden Aktionen hängen sowohl von der Art der Verletzung als auch vom Verursacher ab.

Es muss geregelt sein, wer für Kontakte mit anderen Organisationen verantwortlich ist, um Informationen über bekannte Sicherheitslücken einzuholen oder um Informationen über aufgetretene Sicherheitslücken weiterzugeben. Es muss dafür Sorge getragen werden, dass eventuell. mitbetroffene Stellen schnellstens informiert werden (siehe Baustein DER 2.1 Incident Management).

ORP.1.M11 Rechtzeitige Beteiligung der Personalvertretung [Leiter IT]

Bei allen Maßnahmen, die prinzipiell die Verhaltens- oder Leistungsüberwachung von Mitarbeitern ermöglichen, zum Beispiel Protokollierung, bedarf es der Mitbestimmung der Personalvertretung. Grundlage dessen sind in Deutschland die Betriebsverfassungs- und Personalvertretungsgesetze von Bund und Ländern. In anderen Ländern ist die Einbeziehung der Personalvertretung nicht immer erforderlich. Die rechtzeitige und umfassende Information des Betriebs- oder Personalrates empfiehlt sich aber grundsätzlich, da dies die Akzeptanz von Maßnahmen im Bereich der Informationssicherheit verbessert und Zeitverzögerungen bei deren Umsetzung verhindern kann.

Bei bereits bestehendem Verdacht, dass ein Sicherheitsvorfall (siehe Baustein DER 2.1 Incident Management) durch einen internen Mitarbeiter ausgelöst wurde und entsprechende Nachforschungen durchgeführt werden sollen, die auf Sanktionen hinauslaufen, sind die Beteiligungsrechte des Personal- beziehungsweise Betriebsrates unbedingt zu beachten. Unterbleibt eine ordnungsgemäße Beteiligung der Mitarbeitervertretung, kann das eventuell erforderliche weitere Verfahren (gegebenenfalls vor dem Arbeitsgericht) je nach Schwere des Vorfalls für eine Abmahnung oder Kündigung aufgrund von Formfehlern gravierend beeinflusst werden.

Große Outsourcing-Dienstleister berichten aus der Praxis, dass eine frühzeitige Einbindung der Personalvertretung des Auftraggebers, möglichst schon in der Angebotsphase, sehr zum Gelingen des Projektes beitragen kann. Wechselbereitschaft der Mitarbeiter, Motivation, Arbeitszufriedenheit und zügige Projektabwicklung können durch Kooperation aller Beteiligten positiv beeinflusst werden. Gleiches gilt für die geplante Nutzung von Cloud-Diensten. Als Besonderheit ist hierbei anzusehen, dass die oben genannten Vorgaben auch dann zu beachten sind, wenn sich eine Institution für eine Private Cloud entscheidet.

ORP.1.M12 Regelungen für Wartungs- und Reparaturarbeiten [Haustechnik, ICS-Informationssicherheitsbeauftragter, IT-Betrieb]

Um technische Geräte vor Störungen zu bewahren und um deren Betriebssicherheit zu gewährleisten, müssen regelmäßig Wartungsarbeiten durchgeführt werden. Dies betrifft nicht nur IT-Systeme, sondern auch ICS- und IoT-Komponenten. Die **rechtzeitige Einleitung** von Wartungsarbeiten und die Überprüfung ihrer Durchführung sollte von einer zentralen Stelle aus wahrgenommen werden (z. B. Beschaffungsstelle). Dabei sollten die Wartungsarbeiten von vertrauenswürdigen Personen oder Firmen ausgeführt werden, falls sie nicht von eigenem Personal durchgeführt werden können. Die Hinweise des Herstellers müssen dabei unbedingt beachtet werden. Bei regelmäßigen Wartungsarbeiten durch Externe kann der Abschluss eines Wartungsvertrages nötig sein.

Für jedes Gerät sollte dokumentiert werden, wann es gewartet wurde und welche Fehler dabei behoben wurden. Es empfiehlt sich außerdem, ein Informationssystem für Wartungs- und Reparaturarbeiten einzurichten. Mit einem solchen System können anstehende Arbeiten geplant und durchgeführte Arbeiten dokumentiert sowie der erfolgreiche Verlauf kontrolliert werden.

Außerdem sollte darin dokumentiert sein, wer für die Wartung oder Reparatur von Geräten verantwortlich ist.

Wartungs- und Reparaturarbeiten im Hause

Für Wartungs- und Reparaturarbeiten im Hause, vor allem wenn sie durch Externe durchgeführt werden, sind Regelungen über deren **Beaufsichtigung** zu treffen: während der Arbeiten sollte eine fachkundige Kraft die Arbeiten soweit beaufsichtigen, dass sie beurteilen kann, ob während der Arbeit unautorisierte Handlungen vollzogen werden. Weiterhin ist zu überprüfen, ob der Wartungsauftrag im vereinbarten Umfang ausgeführt wurde.

Als **Maßnahmen vor und nach Wartungs- und Reparaturarbeiten** sind einzuplanen:

- Wartungs- und Reparaturarbeiten sind gegenüber den betroffenen Mitarbeitern rechtzeitig anzukündigen.
- Wartungstechniker müssen sich auf Verlangen ausweisen.
- Der Zugriff auf Daten durch den Wartungstechniker ist soweit wie möglich zu vermeiden. Falls erforderlich, sind Speichermedien vorher auszubauen oder zu löschen (nach einer kompletten Datensicherung), insbesondere wenn die Arbeiten extern durchgeführt werden müssen. Falls das Löschen nicht möglich ist (z. B. aufgrund eines Defektes), sind die Arbeiten auch extern zu beobachten bzw. es sind besondere vertragliche Vereinbarungen zu treffen und vertrauenswürdige Firmen auszuwählen.
- Die dem Wartungstechniker eingeräumten Zutritts-, Zugangs- und Zugriffsrechte sind auf das notwendige Minimum zu beschränken und nach den Arbeiten zu widerrufen bzw. zu löschen.
- Nach der Durchführung von Wartungs- oder Reparaturarbeiten sind, je nach "Eindringtiefe" des Wartungspersonals, Passwortänderungen erforderlich. Im IT-Bereich sollte eine Überprüfung auf Schadsoftware durchgeführt werden.
- Die durchgeführten Wartungsarbeiten sind zu dokumentieren (Umfang, Ergebnisse, Zeitpunkt, Firmenname sowie eventuell Name des Wartungstechnikers).
- Beauftragte Firmen sollten schriftlich zusichern, dass sie einschlägige Sicherheitsvorschriften und Richtlinien (z. B. VdS 2008 Feuergefährliche Arbeiten, Richtlinien für den Brandschutz) beachten. Dies gilt für alle Tätigkeiten, bei denen eine direkte oder indirekte Gefahr für Gebäude oder Menschen entstehen können. Letztlich kommt es darauf an, dass das vor Ort eingesetzte Personal mit diesen Regeln vertraut ist.
- Im Anschluss an die Wartungs- oder Reparaturarbeiten ist die ordnungsgemäße Funktion der gewarteten Anlage zu überprüfen. Insbesondere die Rücknahme der für Testzwecke vorgenommenen Eingriffe ist zu kontrollieren.

Externe Wartungs- und Reparaturarbeiten

Werden IT-Systeme zur Wartung oder Reparatur außer Haus gegeben, sind alle sensitiven Daten, die sich auf Datenträgern befinden, vorher physikalisch zu löschen. Ist dies nicht möglich, weil aufgrund eines Defekts nicht mehr auf die Datenträger zugegriffen werden kann, sind die mit der Reparatur beauftragten Unternehmen auf die Einhaltung der erforderlichen Informationssicherheitsmaßnahmen zu verpflichten. Entsprechend den Anforderungen zu Vertraulichkeitsvereinbarungen aus ORP.2 Personal sind mit diesen vertragliche Regelungen über die Geheimhaltung von Daten zu treffen. Insbesondere ist festzulegen, dass Daten, die im Rahmen der Wartung extern gespeichert wurden, nach Abschluss der Arbeiten vollständig gelöscht werden. Ebenso sind die Pflichten und Kompetenzen des externen Wartungspersonals sorgfältig festzulegen.

Bei der Durchführung externer Wartungsarbeiten muss protokolliert werden, welche IT-Systeme oder Komponenten wann an wen zur Reparatur gegeben wurden, wer dies veranlasst hat, was der Wartungs- bzw. Reparaturauftrag umfasst, zu welchem Zeitpunkt die Reparatur abgeschlossen sein sollte und wann das Gerät wieder zurückgebracht wurde. Um dies nachhalten zu können, ist eine Kennzeichnung der IT-Systeme oder Komponenten erforderlich, aus der zum einem hervorgeht, welcher Institution diese gehören, und zum anderen eine eindeutige Zuordnung innerhalb der Institution möglich ist.

Beim Versand oder Transport der zu reparierenden Komponenten sollte darauf geachtet werden, dass Beschädigungen und Diebstahl vorgebeugt wird. Befinden sich auf oder in den Geräten noch sensitive Informationen, müssen sie entsprechend geschützt transportiert werden, also z. B. in verschlossenen Behältnissen oder durch Kuriere. Weiterhin müssen Nachweise über den Versand (Reparaturauftrag, Begleitzettel, Versandscheine) und den Eingang beim Empfänger (Empfangsbestätigung) geführt und archiviert werden.

Bei Geräten, die durch Passwörter geschützt sind, müssen je nach Umfang der Reparaturarbeiten und der Art der Passwortabsicherung, alle oder einige Passwörter entweder bekannt gegeben oder auf festgelegte Einstellungen wie "REPARATUR" gesetzt werden, damit die Wartungstechniker auf die Geräte zugreifen können.

Nach der Rückgabe der Geräte sind diese auf Vollständigkeit zu überprüfen. **Alle** Passwörter sind zu ändern. Alle Daten oder Programme, die sich auf dem reparierten Gerät befinden, sind auf Integrität zu überprüfen.

Regelungen für die Fernwartung können OPS.2.4 Remote Administration entnommen werden.

ORP.1.M13 Sicherheit bei Umzügen [Informationssicherheitsbeauftragter (ISB), Leiter Haustechnik, Leiter IT]

Bei einem Umzug müssen neben Möbeln auch die verschiedensten Datenträger (z. B. Papier, Magnetbänder, CD-ROMs, DVDs, Wechselfestplatten) und IT-Systeme transportiert werden. Dabei verlassen Informationen, IT-Systeme und sonstiges Material den gesicherten Bereich der Büroumgebung und werden durch Personal transportiert, das normalerweise keine Zugriffsrechte hat. Bei einem Umzug, insbesondere wenn größere Teile der Institution davon betroffen sind, ist ein gewisses Durcheinander nie auszuschließen und es kann auch nicht jede Umzugskiste permanent persönlich beaufsichtigt werden. Trotzdem ist dafür Sorge zu tragen, dass bei einem Umzug sensitive Daten weder verloren gehen, beschädigt werden, noch Unbefugten zugänglich werden.

In die Umzugsplanung sollte möglichst frühzeitig das Informationssicherheitsmanagement und der Datenschutzbeauftragte einbezogen werden, um die aus Sicht der Informationssicherheit festzulegenden Rahmenbedingungen festzulegen:

- Bei der Planung eines Umzuges muss im Vorfeld detailliert festgelegt werden, wer mit welchem Transportgut wann wohin umzieht (Erstellung eines Umzugskonzepts). Dies sollte ohnehin eine Selbstverständlichkeit sein, damit die Arbeit nach dem Umzug möglichst reibungslos wieder aufgenommen werden kann.
- In Abhängigkeit vom Schutzbedarf der Daten muss festgelegt werden, welche Randbedingungen für den Transport einzuhalten sind. Beispielsweise sollten für sensiblere Daten verschließbare Transportbehälter (siehe OPS.1.2.3 Informations- und Datenträgeraustausch) benutzt werden oder die Datenträger vor dem Transport verschlüsselt werden.
- Vor jedem Transport von IT-Systemen sollten Datensicherungen angefertigt werden. Hierbei ist neben den in OPS.1.1.5 Datensicherung beschriebenen Modalitäten insbesondere zu beachten, dass die Datensicherungen auf keinen Fall zusammen mit den gesicherten IT-Systemen transportiert werden dürfen. Hierdurch wird sichergestellt, dass nicht alle Speichermedien gleichzeitig beschädigt werden oder abhanden kommen.
- Es sollte ein Merkblatt (Umzugsmerkblatt) für alle betroffenen Mitarbeiter ausgearbeitet werden, in dem alle durchzuführenden Sicherheitsmaßnahmen genau beschrieben sind.

Bei einem Umzug ist nicht nur der Transport eine kritische Phase, sondern auch der Zeitraum kurz vor bzw. danach. In dieser Phase kommen erfahrungsgemäß viele Sachen abhanden, da zu diesem Zeitpunkt die Standardsicherheitsverfahren wie z. B. die Zutrittskontrolle noch nicht greifen. Auch während des Umzugs sollten daher gewisse organisatorische Mindestanforderungen erfüllt sein:

- Für alle zu transportierenden Materialien sollten Transportpapiere ausgestellt werden, aus denen hervorgeht,
    - ob eine bestimmte Transportart zu beachten ist (z. B. zerbrechlich, Computerspezialtransport, etc.),
    - ob eine bestimmte Verpackungsart zu wählen ist (z. B. bei Datenträgern mit vertraulichen Informationen),
    - wohin sie gebracht werden sollen (genaue Gebäude-, Etagen- und Raumbeschreibung),
    - wer berechtigte Empfänger der transportierten Gegenstände sind,
    - wer sie abgeholt bzw. angeliefert hat (inklusive Name, Datum und Uhrzeit).
-
    - wohin sie gebracht werden sollen (genaue Gebäude-, Etagen- und Raumbeschreibung),
    - wer berechtigte Empfänger der transportierten Gegenstände sind,
    - wer sie abgeholt bzw. angeliefert hat (inklusive Name, Datum und Uhrzeit).
- Das Transportgut muss so gekennzeichnet sein, dass es eindeutig identifiziert werden kann, so dass auch der Transportweg nachvollzogen werden kann. Die Kennzeichnung sollte jedoch keine Rückschlüsse auf die Sensitivität des Inhalts erlauben. Die Art der Kennzeichnung sollte so gewählt sein, dass sie nicht problemlos nachgemacht und werden kann. Hierfür könnten die Umzugsvorbereiter spezielle Etiketten zur Verfügung stellen. Hierbei ist darauf zu achten, dass sich die Etiketten von den Gegenständen auch rückstandsfrei wieder ablösen lassen, ohne das Umzugsgut zu beschädigen bzw. zu verunreinigen.
- Auch während eines Umzuges sollte kein ungeordnetes Kommen und Gehen herrschen. Die beauftragten Umzugsfirmen sollten die Personalien der vorgesehenen Mitarbeiter vorher bekannt geben. Bei plötzlichen Personalwechsel (Urlaub, Krankheit, etc.) sollten die Namen des Ersatzpersonals kurzfristig mitgeteilt werden. Mit einer Namensliste der am Umzug Beteiligten können dann die Pförtner oder andere interne Mitarbeiter je nach Liegenschaft und Gegebenheit sporadisch oder kontinuierlich kontrollieren. Die am Umzug beteiligten externen Kräfte sollten mit gut sichtbaren Ausweisen (ggf. mit Namen) versehen werden, damit klar erkennbar ist, wer zutrittsberechtigt ist.
- Das Transportgut, insbesondere die Datenträger sind vor und nach dem Umzug sicher aufzubewahren. Die Räume, in denen keine Umzugstätigkeiten stattfinden, in denen sich aber keine Mitarbeiter aufhalten, also z. B. die, die noch nicht ausgeräumt bzw. bereits eingeräumt wurden, sollten abgeschlossen werden.

Nach erfolgtem Umzug sollte möglichst rasch ein geordneter Betrieb aufgenommen werden. Als Erstes ist die infrastrukturelle und organisatorische Sicherheit in den neuen Büros wiederherzustellen, also z. B.

- sollte die Zutrittskontrolle wieder in vollem Umfang aufgenommen werden,
- sollten die Brandlasten aus den Fluren entfernt werden, d. h. die Umzugskartons in die neuen Arbeitsräume geschafft werden,
- ist das angelieferte Umzugsgut darauf zu überprüfen, ob es vollständig und voll funktionsfähig ist und nicht manipuliert wurde,
- sollte die Vollständigkeit des Umzugsgutes von jedem Mitarbeiter sofort überprüft werden und gegebenenfalls eine Verlust-Liste angefertigt werden. Hierzu könnte den Betroffenen ebenfalls ein bereits im Vorfeld vorbereitetes Formular ausgehändigt werden, in dem bereits das abtransportierte Umzugsgut aufgelistet werden kann. So kann auch der Vertreter bei Abwesenheit wegen Urlaub, Krankheit oder dringender Dienstgeschäfte der betroffenen Kollegen sofort das Fehlen von Teilen des Umzugsgutes feststellen und melden. Der zu vertretende Mitarbeiter sollte hiervon eine Kopie erhalten, um im nach hinein noch etwaige Unstimmigkeiten melden zu können.Besondere Sorgfalt sollte auf die Umzugsplanung für alle Server und Netzkoppelelemente verwendet werden, da auch bei Ausfall nur einer Komponente unter Umständen das ganze Netz nicht betriebsfähig ist.

Vor einem Umzug sollten daher auf Seiten der zentralen IT-Administration verschiedene Vorkehrungen getroffen werden, um den reibungslosen Arbeitsablauf sicherzustellen:

- Vor Beginn der Umzugsphase sollte frühzeitig ein Plan für die erforderlichen Änderungen der Benutzeranbindung erstellt werden. Hierbei sollte besonders analysiert werden, ob neue Beschaffungen für den reibungslosen Wechsel der Rechneranbindung von Mitarbeitern erforderlich sind. Auch aus Sicherheitsgründen ist es wichtig zu wissen, welche Änderungen sich durch den Umzug im Kommunikationsverhalten der IT-Systeme ergeben. Je nach dem Schutzbedarf der Arbeit von Mitarbeitern kann es beispielsweise erforderlich werden, eine Netzverbindung zu verschlüsseln oder den Zugriff auf bestimmte Datenbestände zu unterbinden.
- Bevor ein Mitarbeiter umzieht, sollte sichergestellt sein, dass er in seinem neuen Büro über das lokale Netz erreichbar ist und seine Applikationen und Dienste betriebsbereit sind. Dies erfordert gegebenenfalls neben Änderungen am Endgerät (Routing, Softwarekonfiguration etc.) auch baldige Änderungen auf Serverseite im LAN oder gar auf Routern im WAN. Hier kann es erforderlich sein, neue Adressen oder Routen einzurichten und alte zu löschen. Möglicherweise müssen vorher neue Netzkomponenten beschafft und eingerichtet werden.
- Bei einem Umzug ist es oft auch erforderlich, für die betroffenen Mitarbeiter Benutzer-Accounts auf einem neuen Server einzurichten. Es ist darauf zu achten, dass die erforderlichen Rechte und Zugriffe auf Applikationen und Protokolle eingerichtet werden. Auch die Sicherheitseinstellungen der Benutzerumgebung müssen seinem Sicherheitsprofil entsprechend gewahrt bleiben. Alte Benutzereinträge und Endgerät-Zugangseinträge müssen auf dem alten System angepasst oder gelöscht werden. Der Zugriff auf benutzereigene Datenbereiche sollte ihm dennoch für eine Übergangszeit, jedoch mit verbindlichem Hinweis auf Löschung nach einer Karenzzeit, gewährt bleiben. Nach dieser Karenzzeit muss die Löschung durch den Administrator vollzogen werden.

Besondere Vorkehrungen sind beim Umzug der Komponenten des Rechenzentrums, wie Daten- oder Kommunikationsservern, zu treffen. Im Folgenden werden Maßnahmen beschrieben, die möglichst kurze Ausfallzeiten der Komponenten gewährleisten sollen.

- Wenn möglich, sollte ein neuer Server vorab installiert und in der neuen Räumlichkeit getestet werden. Ist dies nicht möglich, so sollte der alte Server so gut wie möglich vorkonfiguriert werden und erst zu einer Zeit, zu der wenig Zugriffe zu erwarten sind, nach ausreichender Vorankündigung umgestellt werden. Hierbei sollte die alte Konfiguration immer vorab gesichert sein.
- Der Server sollte vor dem Umzug komplett gesichert werden. Wenn nicht bereits vorhanden, ist auch ein bootfähiges Sicherungsmedium zu erzeugen. Sensible Serverteile wie Festplatten sollten für den Ausfall des Originals als Image redundant vorgehalten sein und getrennt vom Server transportiert werden. Es ist darauf zu achten, dass die Datensicherung und das Image ebenso wie der Server beim Transport gesichert ist (z. B. Verschlüsselung, verschlossene Box, Bewachung).
- Vor dem Umzug ist sicherzustellen, dass die Infrastruktur in den neuen Räumlichkeiten für den einwandfreien Serverbetrieb vorhanden und getestet sind. Hier ist neben dem Vorhandensein des Netzes (Strom, LAN, WAN) auch auf die richtige Reihenfolge des Umzuges der Komponenten zu achten. Es ist beispielsweise wenig sinnvoll, zuerst den Internet-Webserver umziehen zu lassen, wenn der Firewall mit seinem Kommunikationsrouter erst wesentlich später aufgebaut wird.
- Vor dem Umzug sollte überprüft werden, ob unter den zu transportierenden IT-Komponenten solche sind, die besondere Umgebungsbedingungen während des Umzuges benötigen. Beispielsweise gibt es Controller für größere (und teurere!) IT-Systeme, die nicht nur in klimatisierten Räumen betrieben, sondern auch klimatisiert transportiert werden müssen.

Weiterhin sollte sichergestellt sein, dass die neuen Telefonnummern bereits erreichbar sind, sobald die Mitarbeiter ihre neuen Büros bezogen haben. Bei einem Umzug innerhalb eines Ortes sollte versucht werden, die alten Telefonnummern zumindest übergangsweise zu behalten. Während des Umzugs sollte sowohl in der alten als auch in der neuen Liegenschaft die telefonische Erreichbarkeit gewährleistet sein, damit bei auftretenden Problemen Rückfragen jederzeit möglich sind.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

ORP.1.M14 Kontrollgänge [Haustechnik, Informationssicherheitsbeauftragter (ISB)] (CIA)

Eine Maßnahme kann nur so gut wirken, wie sie auch tatsächlich umgesetzt wird. Kontrollgänge bieten das einfachste Mittel, die Umsetzung von Maßnahmen und die Einhaltung von Auflagen und Anweisungen zu überprüfen.

Die Kontrollgänge sollen nicht dem Finden von Tätern dienen, um diese zu bestrafen. Sinn der Kontrollen soll es in erster Linie sein, erkannte Nachlässsigkeiten möglichst sofort zu beheben (Fenster zu schließen, Unterlagen in Aufbewahrung zu nehmen etc.). In zweiter Linie können Ursachen für diese Nachlässigkeiten erkannt und eventuell in der Zukunft vermieden werden.

Die Kontrollgänge sollten durchaus auch während der Dienstzeit erfolgen und zur Information der Mitarbeiter über das Wie und Warum von Regelungen genutzt werden. So werden sie von allen Beteiligten eher als Hilfe denn als Gängelung angesehen.

3 Weiterführende Informationen

3.1 Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Organisation" finden sich unter anderem in folgenden Veröffentlichungen:

[27001A11.2] ISO/IEC 27001:2013

Information technology - Security techniques - Information security management systems - Requirements, insbesondere Annex A, A.11.2 Equipment, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/SC 27, Oktober 2013

[27001A6.1] ISO/IEC 27001:2013

Information technology - Security techniques - Information security management systems - Requirements, insbesondere Annex A, A.6.1 Internal organization, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/SC 27, Oktober 2013

[NIST80053] Security and Privacy Controls for Federal Information Systems and Organizations

NIST Special Publication 800-53, Revision 4, April 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf , zuletzt abgerufen am 30.08.2018

ORP: Organisation und Personal

Umsetzungshinweise zum Baustein ORP.2 Personal

1 Beschreibung

1.1 Einleitung

Das Personal eines Unternehmens bzw. einer Behörde bildet die Grundlage für dessen bzw. deren Erfolg oder Misserfolg. Gleichzeitig sind die Mitarbeiterinnen und Mitarbeiter ein wesentlicher Bestandteil der Informationssicherheit. Wie die Erfahrung zeigt, sind selbst die aufwendigsten Sicherheitsvorkehrungen ohne das richtige Verhalten der Mitarbeiter wirkungslos. Ein Bewusstsein dafür, was Informationssicherheit für die Institution und deren Geschäftsprozesse bedeutet und der richtige Umgang der Mitarbeiter mit den zu schützenden Informationen der Institution sind daher wesentlich.

Dieser Baustein beschäftigt sich in erster Linie mit den Sicherheitsmaßnahmen, die für und durch Mitarbeiter einer Institution umgesetzt werden sollten. Beginnend mit der Einstellung von Mitarbeitern bis hin zu deren Weggang ist eine Vielzahl von Maßnahmen erforderlich. Darüber hinaus dürfen natürlich auch nicht weitere Personengruppen, die mit den Informationen der Institution in Berührung kommen, vergessen werden, wie Mitarbeiter von Dienstleistern und Kunden. Auch für den Umgang mit Externen, wie z. B. Besuchern, Reinigungspersonal oder Wartungstechnikern, müssen angemessene Sicherheitsmaßnahmen vorhanden sein.

1.2 Lebenszyklus

Für das in einem Unternehmen oder einer Behörde tätige Personal sind eine Reihe von Maßnahmen umzusetzen, beginnend mit einer geregelten Einarbeitung neuer Mitarbeiter, über Schulungen, bis hin zu einem geregelten Ausscheiden eines Mitarbeiters. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Umsetzung

Das Unternehmen bzw. die Behörde muss neuen Mitarbeitern bestehende Regelungen und Handlungsanweisungen bekannt machen (siehe ORP.2.M1 *Geregelte Einarbeitung neuer Mitarbeiter*), damit diese zügig in die bestehenden Prozesse integriert werden können. Ebenso ist es unerlässlich, alle Mitarbeiter über Veränderungen dieser Regelungen und ihre spezifischen Auswirkungen auf einen Prozess oder auf den einzelnen Mitarbeiter zu unterrichten. Insbesondere bei sicherheitskritischen Betriebsumgebungen empfiehlt es sich, die Mitarbeiter entsprechend zu verpflichten und die Vertrauenswürdigkeit von Mitarbeitern bestätigen zu lassen (siehe ORP.2.M6 *Überprüfung von Kandidaten bei der Auswahl von Personal*, ORP.2.M7 *Überprüfung der Vertrauenswürdigkeit von Mitarbeitern*, ORP.2.M5 *Vertraulichkeitsvereinbarungen* und ORP.2.M13 *Sicherheitsüberprüfung*). Besonderes Gewicht ist hierbei auf die Vertrauenswürdigkeit von Personen mit besonderen Funktionen und Berechtigungen zu legen, wie beispielsweise Administratoren.

Betrieb

Die Motivation aller Mitarbeiter, Informationssicherheit in den Betriebsprozessen zu akzeptieren und auch eigenverantwortlich umzusetzen, muss durch geeignete Schulungen und durch detaillierte Kenntnisse der Anwendungen auf fachlicher Ebene motiviert und gefördert werden (siehe hierzu Baustein ORP.3: *Sensibilisierung und Schulung*).

Um eine kontinuierliche Verfügbarkeit wichtiger Prozesse zu erreichen, muss dafür gesorgt werden, dass Schlüsselpositionen immer besetzt sind, wenn dies von den Abläufen her gefordert wird (siehe ORP.2.M3 *Vertretungsregelungen*).

Kommunikationsprobleme, persönliche Probleme, schlechtes Betriebsklima, weitreichende organisatorische Veränderungen und Ähnliches sind ebenfalls Faktoren, die zu Sicherheitsrisiken führen können. Für solche Fälle sollten Vertrauenspersonen und Anlaufstellen eingerichtet sein (siehe ORP.2.M12 *Benennung separater Ansprechpartner*).

Funktionsänderungen

Bei Mitarbeitern, die die Institution verlassen oder andere Funktionen übernehmen, müssen bestehende Regelungen mit erhöhter Sorgfalt umgesetzt werden (siehe ORP.2.M2 *Geregelte Verfahrensweise beim Weggang von Mitarbeitern*). Bei kurzfristig ausscheidenden Mitarbeitern kann ein potentielles Risiko vorhanden sein, dass unberechtigterweise vertrauliche Informationen mitgenommen werden oder erst im Nachhinein gezielte Manipulationen an Einrichtungen, IT-Systemen oder Daten bemerkt werden.

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Personal" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

ORP.2.M1 Geregelte Einarbeitung neuer Mitarbeiter [Vorgesetzte]

Neue Mitarbeitern müssen nicht nur in ihre neuen Aufgaben eingearbeitet werden, sie müssen auch über interne Regelungen, Gepflogenheiten und Verfahrensweisen informiert werden. Ohne eine entsprechende Einweisung kennen sie ihre Ansprechpartner zu Fragen der Informationssicherheit nicht, sie wissen nicht, welche Sicherheitsmaßnahmen durchzuführen sind und welche Sicherheitsstrategie die Behörde bzw. das Unternehmen verfolgt. Daraus können Störungen und Schäden für die Institution erwachsen. Daher kommt der geregelten Einarbeitung neuer Mitarbeiter eine entsprechend hohe Bedeutung zu. Die erfahrenen Mitarbeiter sollte entsprechend sensibilisiert werden, damit sie neue Mitarbeiter unterstützen und somit Sicherheitsprobleme bereits im Vorfeld auf ein Minimum reduziert werden können. Neuen Mitarbeitern sollte ein erfahrener Kollege für Fragen zur Seite gestellt werden.

Die Einarbeitung bzw. Einweisung sollte zumindest folgende Punkte umfassen:

- Alle neuen Mitarbeiter sollten in die Benutzung der für den Arbeitsplatz wesentlichen IT-Systeme und Anwendungen eingewiesen bzw. geschult werden. Außerdem sollten alle neuen Mitarbeiter zu allen relevanten Sicherheitsmaßnahmen sensibilisiert und geschult werden (siehe auch Baustein ORP.3: Sensibilisierung und Schulung). Neue Mitarbeiter sollten ausreichend Zeit zur Einarbeitung haben.
- Es sollten alle Ansprechpartner vorgestellt werden, insbesondere die zu Fragen rund um Informationssicherheit und Datenschutz.
- Die Sicherheitsziele der Behörde bzw. des Unternehmens sollten den neuen Mitarbeitern vorgestellt werden. Alle hausinternen Regelungen und Vorschriften zur Informationssicherheit müssen erläutert werden. Für alle Arten von potentiellen Sicherheitsvorfällen sollten die Verhaltensregeln und Meldewege dargelegt werden.Hilfreich zur Durchführung der Einarbeitung ist ein Laufzettel oder eine Checkliste, aus der die einzelnen Aktivitäten und der erreichte Stand der Einarbeitung ersichtlich sind.

ORP.2.M2 Geregelte Verfahrensweise beim Weggang von Mitarbeitern [IT-Betrieb, Vorgesetzte]

Verlässt ein Mitarbeiter die Institution oder wechselt die Funktion, so ist zu beachten:

- Vor dem Weggang ist eine rechtzeitige Einweisung des Nachfolgers durchzuführen. Dafür ist es wünschenswert, dass sich die Arbeitszeiträume wenigstens kurz überschneiden.
- Von dem Ausscheidenden sind sämtliche Unterlagen (wie auch entliehene institutionseigene Bücher), ausgehändigte Schlüssel, ausgeliehene Geräte (z. B. tragbare Rechner, Speichermedien, Dokumentationen) zurückzufordern. Insbesondere sind die Behörden- bzw. Firmenausweise sowie sonstige Karten und Zutrittstokens sowie Schlüssel zur Zutrittsberechtigung einzuziehen. Ferner sind bei biometrischen Verfahren (z. B. Irisscanner, Fingerabdrücke und Handrückenerkennung) entsprechende Zutrittsberechtigungen zu löschen bzw. auf die getroffene Vertreterregelung anzupassen.
- Es sind sämtliche für den Ausscheidenden eingerichteten Zugangsberechtigungen und Zugriffsrechte zu entziehen bzw. zu löschen. Dies betrifft auch die externen Zugangsberechtigungen via Datenübertragungseinrichtungen. Wurde in Ausnahmefällen eine Zugangsberechtigung zu einem IT-System zwischen mehreren Personen geteilt (z. B. mittels eines gemeinsamen Passwortes), so ist nach Weggang einer der Personen die Zugangsberechtigung zu ändern.
- Vor der Verabschiedung sollte noch einmal explizit darauf hingewiesen werden, dass alle Verschwiegenheitserklärungen weiterhin in Kraft bleiben und keine während der Arbeit erhaltenen Informationen weitergegeben werden dürfen.
- Ist die ausscheidende Person ein Funktionsträger in einem Notfallplan, so ist der Notfallplan zu aktualisieren.
- Sämtliche mit Sicherheitsaufgaben betrauten Personen, insbesondere der Pförtnerdienst, sind über den Weggang und Funktionsänderungen von Mitarbeitern zu unterrichten.
- Ausgeschiedenen Mitarbeitern ist der unkontrollierte Zutritt zum Behörden- oder Firmengelände, insbesondere zu Räumen mit IT-Systemen, zu verwehren. Auch bei Funktionsänderungen muss unter Umständen die Zutrittsberechtigung zu bestimmten Räumlichkeiten wie Serverräumen entzogen werden.
- Optional kann sogar für den Zeitraum zwischen Aussprechen einer Kündigung und dem Weggang der Entzug sämtlicher Zugangs- und Zugriffsrechte auf IT-Systeme erfolgen sowie darüber hinaus auch das Verbot, schützenswerte Räume zu betreten, ausgesprochen und technisch umgesetzt werden.
- Alle notwendigen Aktivitäten, wenn ein Mitarbeiter die Institution verlässt oder die Funktion wechselt, sind klar zu regeln. Als ein praktikables Hilfsmittel haben sich sogenannte Laufzettel erwiesen, auf denen die einzelnen Aktivitäten des Ausscheidenden vorgezeichnet sind, die er vor Verlassen der Behörde bzw. des Unternehmens zu erledigen hat.

ORP.2.M3 Vertretungsregelungen [Vorgesetzte]

Vertretungsregelungen haben den Sinn, für vorhersehbare (Urlaub, Dienstreise) und auch unvorhersehbare Fälle (Krankheit, Unfall, Kündigung) des Personenausfalls die Fortführung der Aufgabenwahrnehmung zu ermöglichen. Daher muss vor Eintritt eines solchen Falles geregelt sein, wer wen in welchen Angelegenheiten mit welchen Kompetenzen vertritt. Dies ist besonders im Bereich der Informationsverarbeitung von Bedeutung, da dafür meist Spezialwissen erforderlich ist und eine zeitgerechte Einarbeitung unkundiger Mitarbeiter für den Vertretungsfall nicht möglich ist.

Für die Vertretungsregelungen sind folgende Randbedingungen einzuhalten:

- Für alle wesentlichen Geschäftsprozesse und Aufgaben müssen tragfähige Vertretungsregelungen vorhanden sein. Diese müssen regelmäßig aktualisiert werden.
- Die Übernahme von Aufgaben im Vertretungsfall setzt voraus, dass der Verfahrens- oder Projektstand hinreichend dokumentiert ist.
- Das Benennen eines Vertreters reicht in der Regel nicht aus, es muss überprüft werden, wie der Vertreter zu schulen ist, damit er die Aufgaben inhaltlich übernehmen kann. Stellt sich heraus, dass es Personen gibt, die aufgrund ihres Spezialwissens nicht kurzfristig ersetzbar sind, so bedeutet deren Ausfall eine gravierende Gefährdung des Normalbetriebes. Hier ist es von besonders großer Bedeutung, einen Vertreter zu schulen.
- Es muss festgelegt sein, welcher Aufgabenumfang im Vertretungsfall von wem wahrgenommen werden soll.
- Der Vertreter darf die erforderlichen Zugangs-, Zugriffs- und Zutrittsberechtigungen nur im Vertretungsfall erhalten.
- Ist es in Ausnahmefällen nicht möglich, für Personen einen kompetenten Vertreter zu benennen oder zu schulen, sollte frühzeitig überlegt werden, welche externen Kräfte für den Vertretungsfall eingesetzt werden können.

ORP.2.M4 Regelungen für den Einsatz von Fremdpersonal

Häufig wird in Behörden oder Unternehmen auf externe Unterstützung zurückgegriffen, falls die entsprechenden personellen Ressourcen nicht im eigenen Haus vorhanden sind. Dies kann im Extremfall dazu führen, dass Fremdpersonal über so lange Zeiträume im eigenen Haus eingesetzt wird, dass viele Mitarbeiter schon nicht mehr genau wissen, ob es sich um eigene oder externe Mitarbeiter handelt. Hier bietet es sich an, sowohl interne als auch externe Mitarbeiter auf das Tragen entsprechender Ausweise zu verpflichten.

Externe Mitarbeiter, die über einen längeren Zeitraum in einer oder für eine Organisation tätig sind und eventuell Zugang zu vertraulichen Unterlagen und Daten bekommen könnten, sind schriftlich auf die Einhaltung der geltenden einschlägigen Gesetze, Vorschriften und internen Regelungen zu verpflichten.

Beim Einsatz von externen Mitarbeitern muss außerdem auf jeden Fall sichergestellt sein, dass sie bei Beginn ihrer Tätigkeit - ähnlich wie eigene Mitarbeiter - in ihre Aufgaben eingewiesen werden. Sie sind - soweit es zur Erfüllung ihrer Aufgaben und Verpflichtungen erforderlich ist - über hausinterne Regelungen und Vorschriften zur Informationssicherheit sowie organisationsweite Richtlinien zur Informationssicherheit zu unterrichten. Dies gilt in besonderem Maß, wenn sie innerhalb der Liegenschaften des Auftraggebers arbeiten.

Daneben sollte sichergestellt sein, dass auch für externe Mitarbeiter Vertretungsregelungen existieren. Ebenso sollte gewährleistet sein, dass sich diese mit den von ihnen eingesetzten IT-Anwendungen auskennen und auch die erforderlichen Sicherheitsmaßnahmen beherrschen.

Bei Beendigung des Auftragsverhältnisses muss eine geregelte Übergabe der Arbeitsergebnisse und der erhaltenen Unterlagen und Betriebsmittel erfolgen. Es sind außerdem sämtliche eingerichteten Zugangs-, Zugriffs- und Zutrittsberechtigungen und Zugriffsrechte zu entziehen bzw. zu löschen. Außerdem sollte der Ausscheidende explizit darauf hingewiesen werden, dass die Verschwiegenheitsverpflichtung auch nach Beendigung der Tätigkeit bestehen bleibt.

Kurzfristig oder einmalig zum Einsatz kommendes Fremdpersonal ist wie Besucher zu behandeln, d. h. beispielsweise dass der Aufenthalt in sicherheitsrelevanten Bereichen nur in Begleitung von Mitarbeitern der Behörde bzw. des Unternehmens erlaubt ist.

ORP.2.M5 Vertraulichkeitsvereinbarungen für den Einsatz von Fremdpersonal

Externe Mitarbeiter erhalten häufig für die Erfüllung ihrer Aufgaben Zugang zu vertraulichen Informationen oder erzielen Ergebnisse, die vertraulich behandelt werden müssen. In diesen Fällen müssen sie verpflichtet werden, diese entsprechend zu behandeln. Hierüber sollten Vertraulichkeitsvereinbarungen (Non-Disclosure-Agreements) abgeschlossen werden, die vom externen Mitarbeiter unterzeichnet wird.

In einer Vertraulichkeitsvereinbarung sollte beschrieben sein,

- welche Informationen vertraulich behandelt werden müssen,
- für welchen Zeitraum diese Vertraulichkeitsvereinbarung gilt,
- welche Aktionen bei Beendigung dieser Vereinbarung vorgenommen werden müssen, z. B. Vernichtung oder Rückgabe von Datenträgern,
- wie die Eigentumsrechte an Informationen geregelt sind,
- welche Regelungen für den Gebrauch und die Weitergabe von vertraulichen Informationen an weitere Partner gelten, falls dies notwendig ist,
- welche Konsequenzen bei Verletzung der Vereinbarung eintreten.

In der Vertraulichkeitsvereinbarung kann auch auf die relevanten Sicherheitsrichtlinien und weitere Richtlinien der Organisation hingewiesen werden. In dem Fall, dass externe Mitarbeiter Zugang zu organisationsinternen IT-Infrastruktur haben, sollten diese neben der Vertraulichkeitsvereinbarung auch die Sicherheitsrichtlinien für die Nutzung der jeweiligen IT-Systeme unterzeichnen.

Eine Vertraulichkeitsvereinbarung bietet die rechtliche Grundlage für die Verpflichtung externer Mitarbeiter zur vertraulichen Behandlung von Informationen. Aus diesem Grund muss sie alle relevanten Gesetze und Bestimmungen für die Organisation in dem speziellen Einsatzbereich berücksichtigen, klar formuliert sein und aktuell gehalten werden.

Es kann sinnvoll sein, verschiedene Vertraulichkeitsvereinbarungen je nach Einsatzzweck zu verwenden. In diesem Fall muss klar definiert werden, welche Vereinbarung für welche Fälle notwendig ist.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Personal".

ORP.2.M6 Überprüfung von Kandidaten bei der Auswahl von Personal

Bereits bei der Formulierung der Anforderungen sollten die erforderlichen Qualifikationen und Fähigkeiten genau beschrieben sein. Ob diese bei Bewerbern tatsächlich vorhanden sind, sollte zunächst anhand der Unterlagen nachgeprüft, anschließend im Gespräch geklärt werden.

Personen, die sicherheitsrelevante Aufgaben ausüben sollen (beispielsweise Sicherheitsverantwortliche, Datenschutzbeauftragte, Administratoren, Mitarbeiter mit Zugang zu finanzwirksamen oder vertraulichen Informationen), müssen besonders vertrauenswürdig und zuverlässig sein.

Besonders ist darauf zu achten, dass keine Interessenkonflikte oder Abhängigkeiten entstehen, die die Aufgabenerfüllung gefährden. Interessenkonflikte können insbesondere dann auftreten, wenn ein Mitarbeiter gleichzeitig verschiedene Rollen innehat, die ihm zu weitreichende Rechte geben oder sich ausschließen. Außerdem sollten die Aufgaben von Mitarbeitern auch nicht von Interessenkonflikten außerhalb der Behörde oder des Unternehmens beeinträchtigt werden, beispielsweise durch frühere Stellen oder durch anderweitige Verpflichtungen. Um nach einem Stellenwechsel Interessenkonflikte zu vermeiden, können Konkurrenzverbote und Karenzzeiten vereinbart werden.

Soweit die fachlichen Qualifikationen in Teilbereichen noch nicht ausreichend vorhanden sind, müssen Mitarbeiter die Gelegenheit bekommen, diese zu erweitern. Um die erforderlichen Qualifikationen und Fähigkeiten zu erhalten und zu aktualisieren, sollten alle Mitarbeiter regelmäßig geschult werden und auf die Bedeutung von Informationssicherheit hingewiesen werden (siehe auch Baustein ORP.3: *Sensibilisierung und Schulung*).

Auch bei der Auswahl von Mitarbeitern für befristete Stellen oder von Dienstleistern sollten diese Punkte berücksichtigt werden.

ORP.2.M7 Überprüfung der Vertrauenswürdigkeit von Mitarbeitern

Die Möglichkeiten, die Vertrauenswürdigkeit von neuem oder externem Personal überprüfen zu lassen, sind in Deutschland, aber auch in vielen anderen Ländern, rechtlich sehr eingeschränkt. Dazu kommt, dass die Ergebnisse meist wenig aussagekräftig sind, wie z. B. bei polizeilichen Führungszeugnissen. Grundsätzlich sollte aber vor der Übernahme von neuen oder externen Mitarbeitern in Projekte überprüft werden, ob

- diese hinreichende Referenzen haben, z. B. aus anderen, ähnlichen Projekten, und
- der vorgelegte Lebenslauf des Bewerbers aussagekräftig und vollständig ist.

Darüber hinaus kann es sinnvoll sein, sich akademische und berufliche Qualifikationen bestätigen zu lassen, beispielsweise durch Nachfragen an der Universität oder früheren Arbeitgebern oder Kunden. Auch die Identität des Bewerbers sollte verifiziert werden, z. B. durch Vorlage von Ausweispapieren.

Wenn externes Personal intern eingesetzt wird oder im Rahmen von Projekten, Kooperationen oder Outsourcing-Vorhaben auf interne Anwendungen und Daten zugreifen kann, sollten vergleichbare Überprüfungen wie für eigene Mitarbeiter durchgeführt werden. Bei der Vertragsgestaltung mit externen Dienstleistern sollte vertraglich festgehalten werden, welche Seite solche Überprüfungen durchzuführen hat, in welcher Tiefe diese erfolgen und wie diese dokumentiert werden.

Auswahl vertrauenswürdiger Administratoren

Den IT -System- oder TK -Anlagen-Administratoren und deren Vertretern muss vom Betreiber großes Vertrauen entgegengebracht werden können. Sie haben - in Abhängigkeit vom eingesetzten System - weitgehende und oftmals alle Befugnisse. Administratoren und ihre Vertreter sind in der Lage, auf alle gespeicherten Daten zuzugreifen, gegebenenfalls zu verändern und Berechtigungen so zu vergeben, dass erheblicher Missbrauch möglich wäre.

Administratoren für IT-Systeme und deren Vertreter müssen sorgfältig ausgewählt werden. Sie müssen regelmäßig darüber belehrt werden, dass die Befugnisse nur für die erforderlichen Administrationsaufgaben verwendet werden dürfen.

Da der Administrator hinsichtlich der Funktionsfähigkeit der eingesetzten Hard- und Software eine Schlüsselrolle innehat, muss auch bei seinem Ausfall die Weiterführung seiner Tätigkeiten gewährleistet sein. Hierzu müssen die benannten Vertreter über den aktuellen Stand der Systemkonfiguration verfügen sowie Zugriff auf die für die Administration benötigten Passwörter, Schlüssel und Sicherheitstoken haben.

Hat ein Unternehmen oder eine Behörde mehrere Administratoren mit vergleichbaren IT-Systemkenntnissen, so können sich diese auch wechselseitig vertreten, wenn diese dafür noch freie Kapazitäten haben. In allen Bereichen, in denen nur ein Administrator hauptverantwortlich IT-Systeme betreut, sollten zwei Stellvertreter eingearbeitet werden, da bei längerer Abwesenheit des Administrators erfahrungsgemäß auch der Stellvertreter zeitweise nicht für Administrationsaufgaben zur Verfügung steht.

Um die Funktionsfähigkeit des IT-Betriebs zu gewährleisten, muss insbesondere bei bevorstehenden Personalveränderungen oder Veränderungen der Organisationsstruktur geprüft werden, ob die erforderlichen Administrationstätigkeiten auch durch die benannten Administratoren und deren Vertreter bewältigt werden können.

Insbesondere bei bevorstehenden Umzügen kann es durch Administrationsaufgaben an einem weiteren Standort zu einem erheblichen höheren Arbeitsaufkommen der Administratoren kommen. Auch in solchen Fällen muss sichergestellt sein, dass der Produktionsbetrieb am bisherigen Standort bis zum Zeitpunkt des Umzugs nicht beeinträchtigt wird.

ORP.2.M8 Aufgaben und Zuständigkeiten von Mitarbeitern [Informationssicherheitsbeauftragter (ISB)]

Die Aufgaben und Zuständigkeiten von Mitarbeitern sind in geeigneter Weise zu dokumentieren, beispielsweise durch Arbeitsverträge oder Vereinbarungen. Hieraus leiten sich unter anderem die Berechtigungen ab, die Mitarbeitern für den Umgang mit Informationen und IT-Systemen erhalten. Bei der Zuweisung von Aufgaben und Zuständigkeiten sollte die Mitarbeiter auch direkt auf sicherheitsrelevante Aspekte hingewiesen werden, beispielsweise welche Informationen an welche interne oder externe Ansprechpartner weitergegeben werden dürfen und unter welchen Rahmenbedingungen wie z. B. Verschlüsselung dies zu erfolgen hat.

Dazu gehört auch, dass Mitarbeiter wissen, dass sie auch außerhalb der Arbeitszeit und außerhalb des Betriebsgeländes eine Verantwortlichkeit für Informationssicherheit haben.

Der Informationssicherheitsbeauftragte muss dafür sorgen, dass alle Mitarbeiter ihre Aufgaben und Zuständigkeiten im Sicherheitsprozess kennen. Dazu kann er beispielsweise mit der Personalabteilung oder den Fachvorgesetzen klären, ob die entsprechenden Prozesse dies sicherstellen.

ORP.2.M9 Schulung von Mitarbeitern

Die Mitarbeiter sollten entsprechend ihrer Tätigkeit regelmäßig geschult werden, damit sie in Bezug auf die ihnen übertragenen Tätigkeiten immer auf einem entsprechend aktuellen Stand sind. Dies ist gerade im Bereich der IT-Administration und Wartung der Informationstechnik wichtig, da sich in diesem Bereich die schnellsten Veränderungen ergeben. Aber auch in allen anderen Bereichen sollte sichergestellt werden, dass kein Mitarbeiter basierend auf einem veralteten Wissensstand seiner Arbeit nachgeht. Weiterhin sollte den Mitarbeitern während ihrer Beschäftigung die Möglichkeit gegeben werden, sich im Rahmen ihres Tätigkeitsfeldes weiterzubilden.

Alle Mitarbeiter müssen in die Geräte, Anwendungen und Aktivitäten eingewiesen sein, die zur sicheren Verarbeitung von Informationen dienen, beispielsweise Schredder, Verschlüsselungsprogramme oder Authentisierungstoken. Darüber hinaus sollten alle Mitarbeiter regelmäßig im Bereich der Informationssicherheit geschult und über alltägliche Risiken und mögliche Gegenmaßnahmen unterrichtet werden. Die Mitarbeiter sollten darüber hinaus motiviert werden, Regelungen zur Informationssicherheit eigenverantwortlich umzusetzen. Bei größerem Schulungsbedarf KANN es sinnvoll sein, einzelne Mitarbeiter gesondert zu schulen und innerhalb des Tätigkeitsbereichs als Multiplikatoren für die restlichen Mitarbeiter einzusetzen, um mögliche Ausfallzeiten durch Schulungen zu minimieren.

Dieses Thema wird ausführlich im Baustein ORP.3: *Sensibilisierung und Schulung behand*elt.

ORP.2.M10 Vermeidung von Störungen des Betriebsklimas

Durch ein positives Betriebsklima werden die Mitarbeiter einerseits zur Einhaltung von Sicherheitsmaßnahmen motiviert, andererseits wird die Gefahr von fahrlässigen oder vorsätzlichen Handlungen reduziert, die den Betrieb stören können. Störungen des Betriebsklimas können dabei eine Vielzahl von inner- und außerbetrieblichen Ursachen haben, treten jedoch häufig bei gravierenden innerbetrieblichen Veränderungen auf. Beispiele für solche Veränderungen sind Umstrukturierungen, Sanierungen, Verkauf oder Fusionen von Organisationseinheiten und Outsourcing-Vorhaben. Diese können das Betriebsklima negativ beeinflussen, da sie meistens Ängste unterschiedlicher Art (z. B. Kompetenzverlust, Versagensängste, Arbeitsplatzverlust) hervorrufen. Diese können besser bewältigt werden, wenn das Betriebsklima schon vor den Veränderungen möglichst gut ist.

Auch unter Sicherheitsaspekten sollte daher versucht werden, ein positives Betriebsklima zu erreichen und dauerhaft aufrechtzuerhalten. Die Vielzahl der Möglichkeiten kann hier nicht angeführt werden, deshalb ist hier lediglich eine Auswahl möglicher Maßnahmen genannt, deren Angemessenheit und Realisierbarkeit im Einzelnen zu prüfen wäre:

- Einrichtung eines Sozialraums,
- Vermeidung von Überstunden,
- Vermeidung von großen Resturlaubsansprüchen,
- Einhaltung von Pausenzeiten,
- geregelte Aufgabenverteilung,
- gleichmäßige Arbeitsauslastung,
- leistungsgerechte Bezahlung,
- bestehende Vertreterregelung.

Kommunikationsprobleme in einer Organisation führen fast zwangsläufig auch zu Sicherheitsproblemen. Dies kann im Extremfall zu bewussten Sicherheitsverletzungen führen. Wenn die Benutzer Sicherheitsmaßnahmen nur als "lästig" empfinden, weil sie nicht über deren Zweck informiert worden sind, kann das bereits dazu führen, dass diese umgangen werden.

Auch das Überbringen schlechter Nachrichten muss möglich sein, ohne dass der Bote deswegen Sanktionen befürchten muss. Es sollte ein Betriebsklima vorhanden sein, in dem es für jeden Betroffenen möglich ist, Sicherheitsvorfälle innerhalb des eigenen Unternehmens bzw. der eigenen Behörde zu melden. Nur so können bestehende Sicherheitsdefizite wirkungsvoll und offen angegangen werden.

Mitarbeiter können nicht nur über finanzielle Anreize motiviert werden. Wichtig ist vor allem die Anerkennung ihrer Arbeitsleistung. Mitarbeiter sollten, wo immer möglich, in Entscheidungen mit einbezogen werden.

Zumindest sollten sie über die Gründe für die getroffenen Entscheidungen informiert werden, damit sie aktiv und motiviert an deren Umsetzung mitwirken.

Häufig äußert sich z. B. Protest gegen die Auswahl bestimmter Hard- oder Software darin, dass die Benutzer zu zeigen versuchen, dass die aufgezwungene Hard- oder Software nicht so sicher ist, wie die von ihnen präferierte.

Das Betriebsklima und das Verhalten von Mitarbeitern kann besonders bei großen Veränderungen, wie etwa bei Outsourcing-Vorhaben, von besonderer Bedeutung sein: unzufriedene oder verärgerte Mitarbeiter können ein solches Vorhaben zum Scheitern verurteilen (z. B. Kündigung von Know-how-Trägern in kritischen Phasen der Veränderung oder bewusstes Ignorieren von Sicherheitsanweisungen), was für das Unternehmen in Folge existenzbedrohend sein kann. Bei größeren Umstrukturierungen oder Outsourcing-Vorhaben ist die Beachtung folgender Aspekte empfehlenswert:

- Die Mitarbeiter sollten frühzeitig in Entscheidungsprozesse wie die Auswahl eines Outsourcing-Dienstleisters eingebunden werden. Im weiteren Projektverlauf sollten sie an der Gestaltung von eventuellen Übernahmeverträgen beteiligt werden.
- Die Mitarbeiter sollten umfassend und frühzeitig über Veränderungen informiert werden und einen Ansprechpartner für Probleme und Fragen haben. Indirekte Informationen durch die Medien, z. B. über Zeitungen, statt direkte durch die Firmen- oder Behördenleitung schafft Misstrauen, zerstört die Vertrauensbasis und bereitet Spekulationen und Gerüchten den Boden.
- Bei organisatorischen Veränderungen sollten den betroffenen Mitarbeitern Zukunftsperspektiven aufgezeigt werden. Oftmals sind Outsourcing-Dienstleister darauf angewiesen, dass ein möglichst hoher Anteil der Mitarbeiter des auszulagernden Bereichs zu ihnen wechselt. Nur so kann eine befriedigende Dienstleistungsqualität garantiert werden. Mitarbeiter, die Zukunftsangst haben oder sich unfair behandelt fühlen, lassen in ihrer Arbeitsqualität nach oder verlassen sogar vorzeitig das Unternehmen.
- Anspruchsvolle oder belastende Tätigkeiten, die im Rahmen von Umstrukturierungen nicht zu vermeiden sind, sollten ausreichend gewürdigt und anerkannt werden. Die erforderliche Mehrarbeit sollte honoriert werden.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

ORP.2.M11 Analyse der Sicherheitskultur (CIA)

Zu den wichtigsten Grundpfeilern der Informationssicherheit in einer Institution gehören deren Mitarbeiter. Wie die Erfahrung zeigt, sind selbst die aufwendigsten technischen Sicherheitsvorkehrungen ohne das richtige Verhalten der Mitarbeiter wertlos. Ein Bewusstsein dafür, was Informationssicherheit für die Institution und deren Geschäftsprozesse bedeutet und der richtige Umgang der Mitarbeiter mit den zu schützenden Informationen der Institution sind dafür wesentlich.

Die für die Institution ausgewählten Sicherheitsmaßnahmen sollten sich daher immer an den Mitarbeitern orientieren. Dabei sollte deren Wissen und Umgang mit Informationen und IT einbezogen werden. Daher ist es sinnvoll, die verschiedenen Faktoren zu analysieren, die dazu beitragen, wie sich Mitarbeiter aus Sicherheitssicht verhalten. Darauf aufbauend kann dann untersucht werden, wo die personelle und organisatorische Sicherheit noch verbessert werden kann, beispielsweise durch Sensibilisierung und Schulung zur Informationssicherheit.

Folgende Aspekte sollten durchleuchtet werden:

Sicherheitskultur

Der Begriff Sicherheitskultur umfasst die sicherheitsbezogenen Einstellungen, Werte und grundlegenden Überzeugungen einer Institution und aller ihrer Mitarbeiter. Zur Sicherheitskultur gehört auch, wie offen der Umgang mit Fragen zur Informationssicherheit in der Institution gelebt wird. So ist für die effektive und effiziente Behandlung von Sicherheitsvorfällen eine vertrauensvolle und offene Kommunikationskultur wichtig, damit Sicherheitsvorfälle auch umgehend weitergemeldet und lösungsorientiert angegangen werden.

- Wie ist der Umgang in der Behörde oder dem Unternehmen mit geschäftsrelevanten Informationen und mit Risiken generell? Ist die Institution eher risiko-orientiert oder eher risiko-vermeidend? Werden Informationen eher freizügig oder nur restriktiv weitergegeben?
- Wie sind die Anforderungen an Genauigkeit und Präzision? Sind kleinere Fehler beispielsweise in Texten tragbar, weil diese ohnehin noch mehrere Abstimmprozesse durchlaufen müssen? Kann ein Eingabefehler bereits zu folgenschweren Schäden führen?
- Wie sind die Ansprüche an Verfügbarkeit? Gibt es eine Vielzahl enger Termine? Können Bearbeitungszeiten für Anfragen und Geschäftsprozesse flexibel festgelegt werden? Sind kleinere Terminüberschreitungen oder -änderungen im Allgemeinen tragbar oder führen sie zu harten Konsequenzen?

Stark beeinflusst wird die Sicherheitskultur einer Institution davon, in welcher Branche sie tätig ist. In Hochsicherheitsbereichen wird naturgemäß weniger offen mit Informationen umgegangen als in Forschungseinrichtungen.

Wissen und Können

- Wie gut kennen sich die Mitarbeiter mit IT aus? Ist IT- und Internet-Nutzung eher eine Notwendigkeit, um Geschäftsprozesse effektiver gestalten zu können, oder sind Leben und Arbeiten ohne IT und Internet nicht mehr vorstellbar?
- Welche Erfahrungen und Kenntnisse haben die Mitarbeiter über Informationssicherheit und Datenschutz? Wie sind deren Fähigkeiten zu IT-basierten Sicherheitsmaßnahmen wie Verschlüsselung? Wie ist das Wissen in den verschiedenen Bereichen der Institution verteilt?
- Wie ist der gelebte Umgang der Mitarbeiter mit Fragen der Informationssicherheit und des Datenschutzes? Wie sehen die Mitarbeiter den Bedarf, Informationen vor Veränderungen oder unbefugter Weitergabe zu schützen?
- Können Mitarbeiter aktiv ihre Ideen und Vorstellungen zur Informationssicherheit in den Sicherheitsprozess einbringen?

Sicherheitsrichtlinien

- Passen die Sicherheitsrichtlinien der Institution zu den Geschäftsprozessen und der internen Sicherheitskultur? Sind sie einfach umzusetzen? Sind sie praxisnah und den aktuellen Umgebungsbedingungen angepasst? Behindern sie Arbeitsläufe? Unterstützen sie erwünschte Verhaltensweisen?

Anwendungen und IT

- Ermöglichen die vorhandenen IT-Komponenten einen Umgang mit den geschäftsrelevanten Informationen, der sowohl deren Schutzbedarf als auch den festgelegten Sicherheitsvorgaben entspricht?

Leitungsebene

- Wie steht die Leitungsebene zur Informationssicherheit? Nehmen Vorgesetzte ihre Vorbildfunktion war? Gibt es Wünsche der Leitungsebene zur Verbesserung der Sicherheitsprozesse?

Kulturelle Hintergründe

- Auch die kulturellen Hintergründe können den Umgang mit zu schützenden Informationen und mit Sicherheitsvorgaben generell beeinflussen. Daher sollte untersucht werden, ob es regionale und nationale Unterschiede im Umgang mit Informationssicherheit gibt. Vor allem sollte auch ergründet werden, welche unterschiedlichen Herangehensweisen an Informationssicherheit es in den verschiedenen Bereichen der Institution gibt. Auch einzelne Abteilungen können bereits eigene Regeln und Verhaltensweisen im Umgang mit geschäftsrelevanten Informationen entwickeln.

Veränderungen

- Alle Arten von weitreichenden Veränderungen für die Beschäftigten können deren Umgang mit Informationen, Geschäftsprozessen und IT ändern. Dazu gehören beispielsweise Umstrukturierungen, Entlassungen, Wechsel von Aufgaben oder Vorgesetzten.

Sollte sich bei der Analyse herausstellen, dass sich Mitarbeiter anders verhalten als es aus Sicherheitssicht sinnvoll ist, gibt es verschiedene Wege, um hiermit umzugehen. Es kann z. B. versucht werden, das Verhalten zu ändern (siehe ORP.3: *Sensibilisierung und Schulung*). Andererseits kann es in vielen Fällen einfacher sein, die Sicherheitsvorgaben oder Arbeitsabläufe umzugestalten, da Änderungen von Verhaltensweisen nur langfristig zu erreichen sind. Dabei ist zu beachten, dass dem Schutzbedarf unverändert durch angemessene Sicherheitsvorgaben bzw. Maßnahmenumsetzungen Rechnung getragen wird.

ORP.2.M12 Benennung separater Ansprechpartner (CIA)

Für eine unzureichende Aufgabenerfüllung können oftmals persönliche Probleme eines Arbeitnehmers ursächlich sein. Als Probleme lassen sich beispielsweise hohe Schulden, Suchtkrankheiten aber auch Schwierigkeiten am Arbeitsplatz (Über-/Unterforderung, Mobbing) aufzählen. Um dem Betroffenen bei der Bewältigung dieser Probleme zu helfen, kann es in vielen Fällen hilfreich sein, wenn eine Vertrauensperson zur Verfügung steht. Dieser Ansprechpartner sollte dabei sowohl die Interessen des Betroffenen im Auge haben und konkrete Hilfestellung anbieten als auch die Interessen des Unternehmens bzw. Behörde wahren und gemeinsam mit dem Betroffenen nach Lösungsmöglichkeiten suchen.

An diese Vertrauensperson müssen sich aber auch Vorgesetzte und Kollegen wenden können, wenn wiederholt Auffälligkeiten Dritter wahrgenommen wurden, die auf eine verminderte Zuverlässigkeit schließen lassen. Die Vertrauensperson muss dann die Möglichkeit haben, sich an den Betroffenen zu wenden und Hilfe anzubieten.

Eine solche Stelle können Personalrat, Betriebsrat, Betriebsärzte einnehmen. Die Einrichtung einer solchen Anlaufstelle ist allen Mitarbeitern bekannt zu geben. Externe Stellen sind zum Beispiel die Beratungsstellen der gesetzlichen Krankenkassen.

ORP.2.M13 Sicherheitsüberprüfung (CIA)

Die Möglichkeiten, die Vertrauenswürdigkeit von neuem oder externem Personal überprüfen zu lassen, sind in Deutschland, aber auch in vielen anderen Ländern, rechtlich sehr eingeschränkt. Dazu kommt, dass die Ergebnisse meist wenig aussagekräftig sind, wie z. B. bei polizeilichen Führungszeugnissen. Im Hochsicherheitsbereich kann die grundlegende Überprüfung der Vertrauenswürdigkeit von Mitarbeitern, wie zuvor beschrieben nicht ausreichen. Hier sollte eine zusätzliche Sicherheitsüberprüfung durchgeführt werden.

3 Weiterführende Informationen

3.1 Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Personal" finden sich unter anderem in folgenden Veröffentlichungen:

[27001A7] ISO/IEC 27001:2013

Information technology - Security techniques - Information security management systems - Requirements, Insebsondere Annex A, A.7 Human resource security, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/SC 27, Oktober 2013

[ISFCF2] The Standard of Good Practice for Information Security

Area CF2 Human Resource Security, Information Security Forum (ISF), June 2018

[NIST80053F145] Security and Privacy Controls for Federal Information Systems and Organizations

NIST Special Publication 800-53, Revision 4, insbesondere Appendix F-PS Page F-145, Family: System and Services acquisition, Family: System and communications protection and Family: System and information integrity, April 2013

ORP: Organisation und Personal

Umsetzungshinweise zum Baustein ORP.3 Sensibilisierung und Schulung

1 Beschreibung

1.1 Einleitung

Es ist nur dann möglich, Informationssicherheit innerhalb einer Institution erfolgreich und effizient zu verwirklichen, wenn alle Mitarbeiter erkennen und akzeptieren, dass sie ein bedeutender und notwendiger Faktor für den Erfolg der Institution ist und wenn sie bereit sind, Sicherheitsmaßnahmen wirkungsvoll zu unterstützen. Hierfür müssen eine Sicherheitskultur und ein Sicherheitsbewusstsein (Awareness) aufgebaut und gepflegt werden. Mitarbeiter müssen für relevante Gefährdungen sensibilisiert werden und wissen, wie sich diese auf ihre Institution auswirken können, denn je mehr sie sich damit auskennen, desto eher akzeptieren sie entsprechende Sicherheitsmaßnahmen. Sie müssen auch über die erforderlichen Kenntnisse verfügen, um Maßnahmen richtig verstehen und anwenden zu können. Insbesondere muss ihnen bekannt sein, was von ihnen im Hinblick auf Informationssicherheit erwartet wird und wie sie in sicherheitskritischen Situationen reagieren sollten.

Um den Mitarbeitern das nötige Wissen zu vermitteln, sind gleichermaßen Sensibilisierungs- und Schulungsmaßnahmen erforderlich. Ziel der Sensibilisierung für Informationssicherheit ist es, die Wahrnehmung der Mitarbeiter für sicherheitskritische Situationen und ihre Auswirkungen zu schärfen. Durch Schulungen zur Informationssicherheit sollen die Mitarbeiter die notwendigen Kenntnisse und Kompetenzen für sicherheitsbewusstes Verhalten, für das private und berufliche Umfeld erwerben.

Eine angemessene Informationssicherheit sollte von allen Mitarbeitern als selbstverständlicher Teil ihrer Arbeitsumgebung verinnerlicht werden. Dies setzt in vielen Bereichen eine langfristige Verhaltensänderung voraus, besonders wenn Informationssicherheit mit Komfort- oder Funktionseinbußen verbunden ist. Um hier nachhaltige Ergebnisse zu erzielen, ist ein kontinuierlicher Prozess erforderlich. Daher muss die Institution ein durchgängiges Sensibilisierungs- und Schulungsprogramm zur Informationssicherheit erarbeiten und etablieren. Es sollte bereits bei der Einstellung von Mitarbeitern beginnen, unterschiedliche Zielgruppen mit deren Fähigkeiten, Arbeitsabläufen und benötigten Ressourcen berücksichtigen und die Mitarbeiter auch begleiten, wenn sich ihre Aufgaben oder Positionen verändern.

1.2 Lebenszyklus

Ein Sensibilisierungs- und Schulungsprogramm muss auf die Institution zugeschnitten sein und die dort vorhandene Kultur (siehe auch 3.1.1 Berücksichtigung sicherheitsrelevanter personeller Faktoren in den weiterführenden Informationen) sowie das notwendige Sicherheitsniveau berücksichtigen. In diesem Rahmen sind möglichst unterschiedliche und aufeinander abgestimmte Methoden und Medien zu verwenden.

Planung und Konzeption

Es ist für den Sicherheitsprozess sehr wichtig, dass dieser aktiv vom Management unterstützt wird. Hierfür muss das Management den Wert von Informationssicherheit für die Ziele der Institution erkannt und verinnerlicht haben (siehe ORP.3.M1 Sensibilisierung des Managements für Informationssicherheit).

Diese Unterstützung kann mit dem expliziten Auftrag zur Konzeption entsprechender Programme beginnen. Die notwendigen Schritte sind in der Maßnahme ORP.3.M4 Konzeption eines Schulungs- und Sensibilisierungsprogrammes zur Informationssicherheit beschrieben. Wichtig ist hier insbesondere, die Zielgruppen zu definieren (siehe ORP.3.M5 Analyse der Zielgruppen für Sensibilisierungs- und Schulungsprogramme).

Beschaffung

Um Sensibilisierungs- und Schulungsmaßnahmen vorzubereiten und durchzuführen, wird internes und/oder externes Personal benötigt (siehe hierzu 3.1.2 Auswahl von Trainern oder externen Schulungsanbietern in den weiterführenden Informationen).

Umsetzung

In der Umsetzungsphase werden die Mitarbeiter den vorher definierten Zielgruppen zugeordnet und zielgruppenspezifisch geeignete Inhalte für Sensibilisierungs- und Schulungsmaßnahmen ausgewählt (siehe ORP.3.M6 Planung und Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit). Der Lehrstoff sollte geeignet vermittelt werden, beispielsweise mit Hilfe von Planspielen (siehe 3.1.3 Durchführung von Planspielen zur Informationssicherheit). Auch sind Maßnahmen umzusetzen, wodurch die Ansprechpartner für Sicherheitsfragen bei den Mitarbeitern bekannter werden (siehe ORP.3.M2 Ansprechpartner zu Sicherheitsfragen).

Betrieb, kontinuierliche Pflege und Weiterentwicklung

Ein weiterer wichtiger Bestandteil von Schulungen zur Informationssicherheit ist der Umgang mit der Informationstechnik. Besonders wenn neue Techniken eingeführt werden, sollten die Mitarbeiter frühzeitig über diese informiert und für Gefahrenpotenziale und Sicherheitsmaßnahmen sensibilisiert werden.

Um die Präsenz von vermittelten Lehrinhalten zu verbessern, können Methoden der Lehrstoffsicherung eingesetzt werden (siehe 3.1.4 Lehrstoffsicherung). Auch sollte regelmäßig überprüft werden, ob die Sensibilisierungs- und Schulungsmaßnahmen erfolgreich sind (siehe ORP.3.M8 Messung und Auswertung des Lernerfolgs). Bei Bedarf müssen diese angepasst werden.

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Sensibilisierung und Schulung" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

ORP.3.M1 Sensibilisierung des Managements für Informationssicherheit [Institutionsleitung, Vorgesetzte]

Eine nachdrückliche und aktive Unterstützung durch die Behörden- bzw. Unternehmensleitung ist essentiell, damit Sicherheitskampagnen für die Mitarbeiter erfolgreich sein können. Daher ist es notwendig, dass vor Beginn von Sensibilisierungsmaßnahmen zur Informationssicherheit für Mitarbeiter das Management für Sicherheitsfragen sensibilisiert werden muss.

Die wichtigsten Informationen, die dem Management dabei geliefert werden müssen, sind:

- **Darstellung der Sicherheitsrisiken und damit verbundenen Kosten**
  Die Aufmerksamkeit der Entscheidungsträger kann z. B. durch Berichte über Sicherheitsvorfälle erreicht werden, welche die eigene Institution ebenso betreffen könnten. Beispiele konkreter Sicherheitsvorfälle aus der Nachbarschaft oder bei vergleichbaren Institutionen können den Grad an Rückendeckung des Managements erhöhen.. Solche Beispiele finden sich in Fachzeitschriften, in Tageszeitungen (z. B. nach Hackerangriffen oder Virenvorfällen) und recht detailliert im Internet. Tatsächliche Schadensfälle der Vergangenheit aus der eigenen Institution können ebenfalls zu diesem Ziel eingesetzt werden. Auch die spezifischen Gefährdungen aus relevanten IT-Grundschutz-Bausteinen können hier als Grundlage dienen. Die Darstellung von finanziellen Schäden in konkreten Zahlen ist schwierig. Statistiken und Auswertungen, wie sie beispielsweise von den Polizeien oder Sicherheitsfachzeitschriften von Zeit zu Zeit veröffentlicht werden, bieten in manchen Fällen geeignete Informationen.
- **Auswirkungen auf die Geschäftsprozesse**
  Es ist wichtig, dass die möglichen Auswirkungen von Informationssicherheitsvorfällen auf die geschäftskritischen Prozesse geschildert werden. Abhängigkeiten von Anwendungen und IT-Systemen sowie Industrial Control System (ICS), Internet of Things (IoT) und sonstigen Komponenten sind der Geschäftsführung nicht immer bekannt.Eine Auflistung von möglichen Sicherheitsrisiken reicht jedoch in der Regel nicht aus, um die Unterstützung des Managements zu gewinnen. Eine ausgewogene Argumentation sollte darüber hinaus auch die folgenden Punkte beinhalten.
- **Rechtliche Sicherheitsanforderungen**
  Gesetze und andere juristische Vorgaben können ebenfalls Anforderungen an die Informationssicherheit in einer Institution nach sich ziehen, hierzu gehören beispielsweise Datenschutzgesetze, Sozialgesetzbuch, Handelsgesetzbuch, Bürgerliches Gesetzbuch, Strafgesetzbuch, IT-Sicherheitsgesetz, etc.. Viele gesetzliche Formulierungen zu Anforderungen der Informationssicherheit sind allgemein gehalten und können unverbindlich erscheinen.Durch konkrete Analyse lassen sich hieraus konkrete Verpflichtungen für die Gewährleistung eines angemessenen Sicherheitsniveaus ableiten. Eine Institution muss untersuchen, welche Regularien und Gesetze zur Wirkung kommen können.
- **Vorteile einer Zertifizierung**
  Eine Zertifizierung der Informationssicherheitsprozesse bestätigt offiziell die hohe Wertschätzung der Informationssicherheit in einer Institution. Das Vertrauen der Geschäftspartner und der Öffentlichkeit in die Institution wird dadurch gestärkt. Eine Zertifizierung bringt für Vertrieb und im Marketing Wettbewerbsvorteile mit sich.
- **Standard-Vorgehensweisen zur Informationssicherheit für die Branche**
  Eine zusätzliche Motivation für den Einsatz von Informationssicherheitsstandards ist das Verhalten anderer ähnlicher Organisationen. Informationen zu Branchen-Standards können aus Fachzeitschriften der Branchen, aus Veranstaltungen oder durch Kontakte zu Kammern und Verbänden bezogen werden.

Ein geeigneter Einstieg für die Sensibilisierung der Leitungsebene ist ein kurzer Bericht (evtl. Live Hackings), gefolgt von einer Präsentation, die mit aktuellen Beispielen (extern und intern) das Thema Informationssicherheit erläutert. Hierbei sollte beispielsweise aufgezeigt werden, dass technische Maßnahmen ohne gleichzeitige personelle und organisatorische Maßnahmen sinnlos sind. Um die Unterstützung des Managements zu bekommen, ist es hilfreich, den Nutzen solcher Maßnahmen aufzuzeigen.

Informationssicherheit wird erfahrungsgemäß in einer Institution nur dann erfolgreich umgesetzt, wenn alle Vorgesetzten mit gutem Beispiel vorangehen. Sinnvoll ist es daher, alle Führungskräfte explizit darauf zu verpflichten, ihre Mitarbeiter auf die Einhaltung der Sicherheitsvorgaben hinzuweisen und zu sensibilisieren.

ORP.3.M2 Ansprechpartner zu Sicherheitsfragen

In jeder Institution muss es Ansprechpartner für Sicherheitsfragen geben, sowohl für scheinbar einfache wie auch für komplexe und technische Fragen. Das können IT-Administratoren, IT-Anwendungsverantwortliche oder der Informationssicherheitsbeauftragte sein.

Oft ist die Hemmschwelle, konkrete Sicherheitsvorfälle zu melden, hoch. Wenn der Informationssicherheitsbeauftragte den Mitarbeitern jedoch bereits als Ansprechpartner zu allgemeinen Fragen der Informationssicherheit bekannt ist, kann dies Barrieren abbauen, konkrete Sicherheitsprobleme zu melden.

Die Institution muss den Beschäftigten zudem verbindlich kommunizieren, dass die Meldung von Sicherheitsvorfällen sich nicht negativ für sie auswirkt und sie auffordern, jeden Verdacht eines Sicherheitsvorfalls zeitnah und notfalls anonym zu melden.

Da viele Sicherheitsfragen bei der privaten Nutzung von IT-Systemen auftreten, sollten Informationssicherheitsbeauftragte auch zu vermeintlich nicht dienstlichen Belangen Informationen weitergeben, z. B. zu Phishing, zur Problematik von Computer-Viren und Trojanischen Pferden bei der Internet-Nutzung oder zum Schutz von persönlichen Daten beim E-Commerce. Dadurch werden die Mitarbeiter gegenüber Sicherheitsmaßnahmen offener und der Informationssicherheitsbeauftragter wird mehr akzeptiert. Zudem treten viele vermeintlich private Probleme erfahrungsgemäß äquivalent auch im Büro auf.

Allen Mitarbeitern müssen die Ansprechpartner zu Sicherheitsfragen ebenso wie die Meldewege für Sicherheitsvorfälle bekannt sein. Die Kontaktdaten der Meldestelle sollten effizient im Intranet mit Namen, Telefonnummern und E-Mail-Adressen veröffentlicht werden. Flyer, die dauerhaft an der Arbeitsplätzen verbleiben, unterstützen die Nachhaltigkeit.

ORP.3.M3 Einweisung des Personals in den sicheren Umgang mit IT [IT-Betrieb, Personalabteilung, Vorgesetzte]

Viele Sicherheitsprobleme entstehen durch fehlerhafte Benutzung bzw. Konfiguration der IT. Um solchen Problemen vorzubeugen, müssen alle Mitarbeiter und externen Benutzer in den sicheren Umgang mit den IT-, ICS- und IoT-Komponenten der Institution eingewiesen und geschult werden, soweit dies ihre Arbeitszusammenhänge betrifft.

Allen Benutzern von IT-, ICS- und IoT-Komponenten muss deutlich gemacht werden, welche Rechte und Pflichten sie bei deren Nutzung haben. Dafür müssen ihnen spezifische Richtlinien an die Hand gegeben werden, was sie im Umgang mit den IT-, ICS- und IoT-Komponenten beachten müssen. In einer solchen Richtlinie ist zu beschreiben, welche Rahmenbedingungen es beim Einsatz der betrachteten IT-, ICS- und IoT-Komponenten gibt und welche Sicherheitsmaßnahmen zu ergreifen sind. Dabei hilft den Benutzern die klare und unmissverständliche Information darüber, was sie auf keinen Fall machen dürfen. Diese Richtlinien müssen verbindlich, verständlich, aktuell und verfügbar sein. Um die Verbindlichkeit zu dokumentieren, sollten sie von der Behörden- bzw. Unternehmensleitung oder zumindest von den Verantwortlichen für deren Betrieb unterzeichnet sein. Es empfiehlt sich auch, sie kurz und verständlich zu formulieren, sodass sie beispielsweise als Poster, Merkzettel, Flyer oder Ähnliches verteilt werden können. Zusätzlich sollten sie im Intranet abrufbar sein.

Benutzerrichtlinien sollten grundsätzlich nur Regelungen enthalten, die auch umgesetzt werden können und so positiv und nachvollziehbar wie möglich formuliert werden. Beispielsweise könnte eine Benutzerrichtlinie statt

"*Benutzer dürfen keine Software selbständig installieren.*"

besser folgendermaßen lauten:

"*Alle IT-Systeme werden in einer Standardkonfiguration ausgeliefert, die auf Ihre spezifischen Arbeitsbedingungen angepasst wurde und Ihnen maximale Sicherheit bieten. Bei Problemfällen können wir Ihnen durch eine Neuinstallation der Standardkonfiguration eine schnelle Problemlösung garantieren. Verändern Sie daher die Einstellungen nicht! Wenn Sie zusätzliche Hard- oder Software benötigen, wenden Sie sich bitte an den Benutzerservice.*"

Weitere Beispiele für Benutzerrichtlinien finden sich unter den Hilfsmitteln zum IT-Grundschutz.

Eine Benutzerrichtlinie für die allgemeine IT-Nutzung soll mindestens die folgenden Punkte umfassen:

- Hinweis, dass keine IT-Systeme, IT- oder IoT-Komponenten ohne ausdrückliche Erlaubnis benutzt werden dürfen
- Hinweis, dass nur diejenigen Mitarbeiter Informationen auf IT-Systemen ändern dürfen, die dazu autorisiert sind
- Einbringen von externen Daten in das eigene Haus (z.B. USB, Download oder Mailanhang)
- Umgang mit Passwörtern
- Nutzungsverbot nicht freigegebener Software
- Hinweis, dass dienstliche IT-Systeme nur für dienstliche Zwecke eingesetzt werden dürfen, beziehungsweise eine präzise Beschreibung möglicher Ausnahmen von dieser Regel, falls es sie gibt
- Hinweise zur sicheren Verwahrung und Aufstellung von IT-Systemen und Datenträgern
- Schutz vor Computer-Viren und anderer Schadsoftware
- Durchführung von Datensicherungen
- Nutzung von Internet- und E-Mail-Diensten

Neben solchen Richtlinien müssen klare Aussagen darüber vorliegen, welche Benutzer auf welche Informationen zugreifen dürfen, an wen diese weitergegeben werden dürfen und welche Maßnahmen bei einem Verstoß gegen diese Richtlinien unternommen werden.

Wenn ein Benutzer seinen Arbeitsplatz verlässt, sollte er sich davon überzeugen, dass jedes Arbeitsmittel (Dokumente, Datenträger, etc.) sicher verwahrt ist. Alle IT-Systeme sollten durch Passwörter gegen unbefugten Zugriff geschützt sein. Bei unbeaufsichtigten IT-Systemen ist der Computer mindestens zu sperren.

Die Grundkonfiguration aller IT-Systeme sollte möglichst eingeschränkt bzw. schlank sein. In der Standardkonfiguration von Arbeitsplatzrechnern sollten nur die Dienste vorhanden sein, die von allen Benutzern einer Gruppe benötigt werden. Weitere Programme oder Funktionen dürfen nur dann aufgespielt bzw. freigeschaltet werden, wenn die Benutzer in deren Handhabung eingewiesen und für eventuelle Sicherheitsprobleme sensibilisiert wurden.

Jede Benutzerordnung sollte in Zusammenarbeit mit Vertretern aller beteiligten Gruppen erstellt werden, insbesondere sind Personalvertretungen und Datenschutz- sowie Informationssicherheitsbeauftragter rechtzeitig zu beteiligen. Bei Änderung einer Benutzerordnung ist darauf zu achten, dass die Betroffenen wieder im Vorfeld beteiligt werden. Die geänderte Benutzerordnung muss allen Benutzern bekannt gegeben werden.

Die Aufgabenbeschreibung muss alle für die Informationssicherheit relevanten Aufgaben und Verpflichtungen enthalten. Dazu gehört u. a. die Verpflichtung auf die hausinternen Leitlinien zur Informationssicherheit.

Werden IT-, ICS- oder IoT-Systeme oder Dienste in einer Weise benutzt, die den Interessen der Behörde bzw. des Unternehmens widersprechen, muss jeder, der davon Kenntnis erhält, dies seinen Vorgesetzten mitteilen.

Gemeinsam mit den Basismaßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich Sensibilisierung und Schulung.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Sensibilisierung und Schulung".

ORP.3.M4 Konzeption eines Sensibilisierungs- und Schulungsprogramms zur Informationssicherheit

Die Mitarbeiter sind die wesentlichen Erfolgsfaktoren, um Informationssicherheit in einer Institution zu etablieren und aufrechtzuerhalten. Sie sind es, die technische Schutzsysteme nutzen oder administrieren, die Richtlinien und Vorgaben mehr oder weniger sorgfältig beachten und die aus Unkenntnis oder Vorsatz sicherheitsrelevante Fehler machen können. Deshalb sollte ein zielgruppenorientiertes Sensibilisierungs- und Schulungsprogramm erstellt und regelmäßig überprüft und aktualisiert werden.

Die im Rahmen eines Sicherheitskonzeptes realisierten technischen und organisatorischen Maßnahmen wirken sich in vielfältiger Weise auf die einzelnen Mitarbeiter aus. So könnten sie zu regelmäßigen Passwortwechseln gezwungen sein, bestimmte Bereiche der Institution ohne Genehmigung nicht betreten dürfen, ihre Mitarbeiterausweise gut sichtbar tragen oder regelmäßig Sicherheitsschulungen besuchen müssen.

Ziel jeder Institution sollte es daher sein, dass alle Mitarbeiter den Wert und die Notwendigkeit einer angemessenen Informationssicherheit zur Erfüllung ihrer Aufgaben und den Fortbestand der Institution erkennen, akzeptieren und aktiv unterstützen. Sie sollten die bestehenden Regelungen und Maßnahmen beachten und durch ihr Verhalten dazu beitragen, die Informationssicherheit aufrechtzuerhalten und weiterzuentwickeln. Sie sollen sicherheitskritische Situationen möglichst frühzeitig erkennen können und darauf richtig reagieren.

Dies setzt eine systematische Sensibilisierung der Mitarbeiter voraus, die durch einen kontinuierlichen Prozess in der Institution zu verankern ist. Aufbauend auf der Sensibilisierung sollten die Mitarbeiter durch ergänzende Schulungen alle erforderlichen Informationen und Fähigkeiten vermittelt bekommen (siehe ORP.3.M3 Einweisung des Personals in den sicheren Umgang mit IT). Sensibilisierungs- und Schulungsprogramme sind somit eng verwandte Themengebiete, denen auf allen Organisationsebenen eine hohe Bedeutung zugemessen werden sollte. Damit das besondere Gewicht von Sensibilisierungsmaßnahmen erkennbar ist und die benötigten Ressourcen zur Planung, Umsetzung und Aufrechterhaltung verfügbar sind, muss das Management die Maßnahmen unterstützen.

Die nachfolgenden Aspekte sind bei Konzeption und Aufbau des Sensibilisierungs- und Schulungsprogrammes hilfreich.

Sensibilisierung für Informationssicherheit bedeutet, dass bei Mitarbeitern die Wahrnehmung von Informationssicherheit geschärft und ihr Sicherheitsbewusstsein entsprechend den Anforderungen der Institution geschult wird.

Zu Beginn der Sensibilisierung sollte ein Ziel definiert und im weiteren Verlauf dieser Maßnahme zielgruppenbezogen verfeinert werden. So können später Inhalte passgenau entwickelt und der Erfolg der Maßnahmen gemessen werden. Bei der Zieldefinition sollte die Frage im Vordergrund stehen, warum Informationssicherheit für die Institution und ihre Mitarbeiter wichtig ist.

Beispiel für eine Zieldefinition:

Durch eine Zielgruppenanalyse können die Sensibilisierungsmaßnahmen an spezielle Anforderungen und unterschiedliche Hintergründe der Mitarbeiter angepasst werden (siehe ORP.3.M5 Analyse der Zielgruppen für Sensibilisierungs- und Schulungsprogramme). Durch Hilfe der Zielgruppenanalyse werden Mitarbeiter mit vergleichbaren Merkmalen in Bezug auf die Informationssicherheit identifiziert, wie z. B. "Administratoren", "Mitarbeiter der Personalabteilung" oder "externe Mitarbeiter". Weiterhin sollten auch die Entwicklungen der Mitarbeiterlaufbahn betrachtet werden, die für die Institution charakteristisch sind, z. B. Abteilungs-, Funktions- oder Standortwechsel.

Die Sensibilisierungsmaßnahmen sind zielgruppengerecht aufzubereiten. Als Ergebnis können z. B. Auswirkungen von Sicherheitsvorfällen für die jeweiligen Mitarbeiter so praxisnah wie möglich beschrieben werden. Weiterhin hat es sich auch als äußerst wirksam erwiesen, Beispiele aus dem privaten Umfeld der Mitarbeiter in Sensibilisierungsprogramme aufzunehmen, wie der Verlust der Digitalfotos aus dem letzten Urlaub oder ein verlorenes Smartphone.

Sensibilisierungskampagnen können alle Themen beinhalten, die begründen, warum Informationssicherheit für die Institution und ihre Mitarbeiter wichtig ist. Hierzu zählen z. B. relevante Gefährdungen oder beispielhafte wie auch reale Sicherheitsvorfälle, an denen richtiges Verhalten trainiert werden kann. Dabei sollte darauf geachtet werden, dass genügend Inhalte einen engen Bezug zur Institution sowie deren Rahmenbedingungen und der angesprochenen Zielgruppe haben. Zusätzlich können Beispiele aus vergleichbaren Institutionen oder aussagekräftigen Publikationen die Inhalte untermauern.

Es sind solche Medien und Methoden auszuwählen, die sich eng an der herrschenden Kultur der Institution orientieren. Ziel ist es, die Mitarbeiter mit vertretbaren Kosten möglichst eindrucksvoll und nachhaltig zu erreichen und für Informationssicherheit zu sensibilisieren. Das heißt, die Wahrnehmungen, Emotionen und Fähigkeiten der Mitarbeiter für Schwachstellen und Vorfälle in ihrer Arbeitsumgebung müssen gestärkt werden, damit sie diese frühzeitig erkennen, bewerten und richtig darauf reagieren. Dabei sollte auf reine Anweisungstexte, ausführliche und detaillierte schriftliche Regelungen sowie auf eine unverständliche Fachsprache zugunsten einer kurzen und prägnanten Kommunikation verzichtet werden (siehe auch ORP.3.1.3 Durchführung von Planspielen zur Informationssicherheit).

Sensibilisierung und Schulung sind eng verwandte Themen, die sich in der Umsetzung ergänzen und aufeinander aufbauen. Sensibilisierung soll die Mitarbeiter zum Handeln motivieren. Die richtigen Verhaltensweisen werden anschließend durch Schulungsmaßnahmen weiter unterstützt. Es ist in der Praxis eine große Herausforderung, Mitarbeiter für Informationssicherheit zu interessieren und das richtige Verhalten aufrechtzuerhalten. Je klarer, begeisterungsfähiger aufgearbeitet und eindrucksvoller das Gesamtkonzept der Maßnahmen ist, umso wirksamer kann der Lehrstoff beim Mitarbeiter verarbeitet und angewandt werden. Deshalb muss der Lehrstoff durch geeignete Maßnahmen gefestigt werden (siehe ORP.3.1.4 Lehrstoffsicherung).

Der Erfolg der festgelegten Sensibilisierungs- und Schulungsziele ist zu messen und auszuwerten. Dafür sollte der Stand der Teilnehmer vor, während und nach der Maßnahme anhand geeigneter Kennzahlen oder Kriterien erfasst werden. So lässt sich verfolgen, ob die Kampagne erfolgreich ist und wie sich die Sensibilisierung entwickelt. Weitere Informationen sind in Maßnahme ORP.3.M8 Messung und Auswertung des Lernerfolgs dargestellt.

Die Informationssicherheit in einer Institution ist permanenten Veränderungen unterworfen. IT-Systeme, Prozesse, Leistungsspektren, Wettbewerbssituationen wandeln sich und damit einhergehend auch Gefährdungslagen, Risikobewertungen und erforderliche Sicherheitsmaßnahmen. Zusätzlich müssen die Ergebnisse der bisherigen Sensibilisierungsmaßnahmen betrachtet werden, insbesondere notwendige Veränderungen aufgrund der Messung und Auswertung des Lernerfolgs.

Diese Veränderungen müssen sorgfältig analysiert und das Sensibilisierungs- und Schulungsprogramm regelmäßig aktualisiert werden.

ORP.3.M5 Analyse der Zielgruppen für Sensibilisierungs- und Schulungsprogramme

Wird für eine Institution ein Sensibilisierungs- und Schulungsprogramm erstellt, sollten im Konzept die jeweiligen Zielgruppen definiert werden (siehe ORP.3.M4 Konzeption eines Schulungs- und Sensibilisierungsprogrammes zur Informationssicherheit). Dazu sollte eine detaillierte Zielgruppenanalyse durchgeführt werden, sodass Maßnahmen auf spezielle Anforderungen und unterschiedliche Hintergründe fokussiert werden können.

Es können beispielsweise Mitarbeiter mit vergleichbaren fachlichen Hintergründen, Kenntnissen oder Aufgaben zu einer Zielgruppe zusammengefasst werden. Ein praktikabler Ansatz ist auch die Zielgruppen aus den organisatorischen Einheiten abzuleiten. In der Regel kann hier davon ausgegangen werden, dass Mitarbeiter mit vergleichbarer Technik und ähnlichen Vorgaben arbeiten.

Ein weiteres Kriterium sind Ereignisse, die innerhalb einer Mitarbeiterlaufbahn eintreten. Hierzu zählen z. B. Neueinstellung, Aufgaben- oder Abteilungswechsel, Standortwechsel, Technikwechsel, Änderungen in der bestehenden Organisation oder der Weggang aus der Institution.

Beispiele möglicher Zielgruppen und deren Merkmale:

Managementebene

Die Mitglieder der Managementebene haben eine Vorbildfunktion für die Mitarbeiter. Oft haben sie wenig Zeit, sodass die Sensibilisierungs- und Schulungsmaßnahmen strukturiert und prägnant sein müssen. Die Motivation der Managementebene für die Informationssicherheit kann durch geeignete persönlichen Zielvereinbarungen erreicht werden.

Mitarbeiter

Das Verhalten dieser Zielgruppe im Arbeitsalltag hat die stärksten direkten Auswirkungen auf die Informationssicherheit. Hier ist zu berücksichtigen, dass der Wissensstand und die Rahmenbedingungen innerhalb der Zielgruppe sehr unterschiedlich sein können. Beispielsweise haben Software-Entwickler eine andere IT-Ausstattung und andere Aufgaben und Kenntnisse als Mitarbeiter der Personalverwaltung. Ebenso ist davon auszugehen, dass die persönlichen Ausrichtungen dieser beiden Zielgruppen recht verschieden sind. Die beiden Gruppen benötigen unterschiedliche Schulungsinhalte zur Informationssicherheit.

Administratoren

Administratoren und Support-Mitarbeiter müssen tief gehende Fachkenntnisse der von ihnen betreuten IT-Systeme und Anwendungen haben, sodass sie auch in der Lage sind, Sicherheitsprobleme zu erkennen und zu beheben sowie diesen vorzubeugen.

Personalabteilung (Vorzimmer, Poststelle, Pressebereich)

Mitarbeiter dieser Abteilung haben einen hohen Informationsbedarf über Datenschutzanforderungen. Weiterhin sind die Mitarbeiter der Personalabteilung wesentlicher Treiber für die Beschreibung der Aufgabengebiete je Mitarbeiter, dem Nachvollziehen der Vertreterregelung sowie der Veröffentlichung zentraler Zuständigkeitsbereiche der Kollegen innerhalb der Institution.

Externe Projektmitarbeiter

In vielen Fällen haben auch Externe, die eng mit oder sogar in der Institution tätig sind, Zugriff auf interne Informationen, Anwendungen oder Systeme.

Diese Zielgruppe muss die Informationssicherheitsziele und -regeln der Institution ebenso unterstützen und darauf verpflichtet werden, wie interne Mitarbeiter. Dies erfordert entsprechende Schulungsmaßnahmen, z. B. in Form von Einweisungen mit dokumentierter Kenntnisnahme. Diese Maßnahmen sollte die externe Institution entsprechend den mit der eigenen Institution vereinbarten Anforderungen durchführen.

Neueinstellungen

Diese Zielgruppe hatte bisher keine Berührung mit der organisationsinternen Informationssicherheit. Daher müssen grundsätzlich im Rahmen der Erstinformation die Inhalte der Informationssicherheit wirksam vermittelt und Mitarbeiter darauf verpflichtet werden. Hier haben sich Vorgehensweisen bewährt, die diesen Schritt in den Willkommensprozess einbeziehen.

ORP.3.M6 Planung und Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit

Ein Schulungsprogramm zur Informationssicherheit sollte den Mitarbeitern alle Informationen und Fähigkeiten vermitteln, die erforderlich sind, um in der Institution geltende Sicherheitsregelungen und -maßnahmen umsetzen zu können.

Nachdem die Ziele der Informationssicherheitsschulungen für die Institution festgelegt, sowie relevante Zielgruppen und deren spezifischer Schulungsbedarf identifiziert wurden (siehe ORP.3.M5 Analyse der Zielgruppen für Sensibilisierungs und Schulungsprogramme), müssen die konkreten Schulungsmodule und -inhalte geplant und entsprechend umgesetzt werden, indem die Zielgruppen gemäß dieser Planung geschult werden.

Hierzu sollten folgende Aspekte betrachtet werden:

- In welcher Tiefe und mit welcher Methodik soll welche Zielgruppe geschult werden?
- Welche Mitarbeiter gehören in welche Zielgruppe?
- Welche Ressourcen sind für eine Zielgruppe erforderlich, z. B. Trainerkapazität, Räumlichkeiten, benötigte IT-Infrastruktur, Organisation etc.?
- Welche speziellen Arbeitsumgebungen mit ihren Anforderungen an die Informationssicherheit und welche zugeordneten Maßnahmen müssen berücksichtigt werden, z. B. Prozesse, Verfahren, Aufgaben und Rollen inklusive möglicher Veränderungen?

Mögliche Schulungsinhalte

Im Folgenden werden beispielhaft eine Struktur und wichtige Inhalte von Schulungsmodulen vorgestellt, die entsprechend den dargestellten Aspekten noch rollen- und ressourcenbezogen aufbereitet werden müssen. Für viele Bereiche stehen Schulungsangebote von entsprechenden Anbietern zur Verfügung, falls eine interne Planung und Durchführung in der Institution nicht möglich ist.

Die Module unterscheiden sich zunächst nur nach Themen. Jedes Modul kann in angepasster inhaltlicher Tiefe durchgeführt werden. Dies ist abhängig davon, für welche Arbeitsumgebung oder welchen Abschnitt einer Mitarbeiterlaufbahn das Modul bestimmt ist.

Die Schulungsinhalte sollten auf Basis der in Maßnahme ORP.3.M4 Konzeption eines Schulungs- und Sensibilisierungsprogrammes zur Informationssicherheit erarbeiteten Analyse festgelegt sowie regelmäßig überprüft und angepasst werden, um eine größtmögliche Wirksamkeit der Schulungsmaßnahmen zu erzielen. Zusätzlich sollen alle für den jeweiligen Informationsverbund relevanten Bausteine des IT-Grundschutz-Kompendiums daraufhin überprüft werden, ob die erforderlichen Maßnahmen nicht nur angeordnet, sondern auch geschult wurden.

Ebenfalls exemplarisch wurden hier die Schulungsmodule den Zielgruppen zugeordnet. Dabei wird mit "X" gekennzeichnet, dass das jeweilige Modul für die entsprechende Rolle empfohlen wird. Mit einem "O" werden die optionalen Schulungsmodule gekennzeichnet, bei denen von Fall zu Fall entschieden werden sollte, ob die Inhalte für die entsprechende Rolle benötigt werden.

Modul 1: Grundlagen der Informationssicherheit

Modul 2: Informationssicherheit am Arbeitsplatz

Modul 3: Gesetze und Regularien

Modul 4: Sicherheitskonzept der Organisation

Modul 5: Risikomanagement

Modul 6: Informationssicherheitsmanagement

Modul 7: IT-Systeme

Modul 8: Operativer Bereich

Modul 9: Technische Realisierung von Sicherheitsmaßnahmen

Modul 10: Notfallvorsorge/Notfallplanung

Modul 11: Neue Entwicklungen im IT-Bereich

Modul 12: Betriebswirtschaftliche Seite der Informationssicherheit

Modul 13: Infrastruktur-Sicherheit

Modul → Funktion ↓	1	2	3	4	5	6	7	8	9	10	11	12	13
Vorgesetzte	X	X	X	X							O	X	
Sicherheitsmanagement	X	X	X	X	X	X	X	X	X	X	X	X	X
Datenschutzbeauftragter	X	X	X	X							X	O	
Infrastrukturverantwortliche	X	X	X	X	X	O				X			X
Benutzer	X	X											
Administratoren	X	X		X	X		X	X	X	X	X		O

Tabelle: Vorgeschlagene Schulungsmodule je Funktion

In diesem Beispiel dienen die beiden Module 1 und 2 als Basisschulung für alle Mitarbeiter und sind eng mit Sensibilisierungsmaßnahmen abzustimmen. Alle anderen Module zeigen auf, welche Vertiefungsgebiete je nach Fachaufgabe außerdem vermittelt werden sollten.

Je nach Art der Institution kann es sinnvoll sein, weitere Zielgruppen und die zugehörigen Schulungsziele zu definieren (siehe ORP.3.M5 Analyse der Zielgruppen für Sensibilisierungs und Schulungsprogramme). Wichtig ist auch die Einbindung der Mitarbeiter, die in erster Linie wenig oder nichts mit Informationstechnik zu tun haben, wie z. B. der Sicherheits- und Reinigungsdienst.

Modul 1: Grundlagen der Informationssicherheit

Institutionen sind stark von einer ausreichend verfügbaren und gegen Angriffe geschützten IT und Infrastruktur abhängig. Daher ist die wichtigste Aufgabe von Sensibilisierung und Schulung, den Mitarbeitern den Wert von Informationssicherheit für die Institution und entsprechende Grundlageninformationen zu vermitteln.

Unter anderem sollten in diesem Modul folgende Themen behandelt werden:

- Motivation
  - Fallbeispiele aus der Praxis für Gefährdungen und Risiken
  - Auswirkungen von Angriffen, inklusive Social Engineering
- Informationen als Werte einer Institution und ihr Schutzbedarf
- Begriffserläuterungen:
  - Informationssicherheit
  - Vertraulichkeit, Integrität, Verfügbarkeit
  - Security, Safety, Datenschutz und ihre Abgrenzung zur Informationssicherheit
- Informationssicherheit in der eigenen Institution
  - Aufgaben und Ziele der Institution
  - Sicherheitsanforderungen und Risiken in der Institution
  - Informationssicherheitsstrategie und -konzept der Institution im Überblick
  - Aufgaben und Verpflichtungen der einzelnen Mitarbeiter
- Wesentliche Sicherheitsregeln für Mitarbeiter
  - Überblick über interne Sicherheitsregelungen
  - Umgang mit sensiblen Informationen (inklusive Passwörtern)
  - Nutzung von E-Mail und Internet
  - Schutz vor Schadprogrammen und Datensicherung
  - Umgang mit mobilen Endgeräten
  - Arbeiten in fremden oder öffentlichen Umgebungen

Modul 2: Informationssicherheit am Arbeitsplatz

Mitarbeiter können durch die Beachtung einfacher Vorsichtsmaßregeln dazu beitragen, Schäden zu vermeiden. Das Modul zur Umsetzung von Informationssicherheit am Arbeitsplatz sollte unter anderem die folgenden Themenschwerpunkte umfassen:

- Sensibilisierung von Mitarbeitern
- Vermeidung von typischen Fehler von Anwendern
  - leichtsinniger Umgang mit Passwörtern
  - Verzicht auf Verschlüsselung
  - mangelnder Schutz von Informationen
  - mangelndes Misstrauen
  - Diebstahl von mobilen Geräten (wie Laptops und Smartphones)
- Vorbeugung gegen Social Engineering
- Organisation und Sicherheit
  - Die Sicherheitsvorgaben der Institution und deren Bedeutung für den Arbeitsalltag
  - Verantwortlichkeiten und Meldewege in der Institution (mit persönlicher Vorstellung der Informationssicherheitsbeauftragten)
- Zutritts-, Zugangs- und Zugriffsschutz
- Bedeutung der Datensicherung und gegebenenfalls deren Durchführung
- E-Mail- und Internet-Sicherheit
- Schutz vor Schadprogrammen
- Sicherheitsaspekte relevanter IT-Systeme und Anwendungen
- Rechtliche Aspekte
- Verhalten bei Sicherheitsvorfällen
  - Erkennung von Sicherheitsvorfällen
  - Meldewege und Ansprechpartner
  - Verhaltensregeln im Verdachtsfall

Die hier angegebenen Themen stellen eine Auswahl dar. Das Schulungsmodul "Informationssicherheit am Arbeitsplatz" muss stets an die individuellen Gegebenheiten der Institution angepasst sein.

Modul 3: Anforderungen, Gesetze und Regularien

Dieses Schulungsmodul sollte den rechtlichen Anforderungsrahmen, in dem Informationssicherheit innerhalb der Institution zu betrachten ist, für die Mitarbeiter umreißen.

Hierzu zählen Sicherheitsanforderungen, die sich aus den folgenden Punkten ergeben können:

- Verträge (z. B. mit Kunden, Lieferanten, Outsourcing-Partnern, Kreditgebern)
- regulatorische Anforderungen, einschlägige Gesetze, Vorschriften, Informationssicherheitsstandards und -richtlinien, etc.
- sonstigen Anforderungen der Institution (z. B. bewusste Marktdifferenzierung, Produktstrategie, Sicherheitsimage etc.)

Es ist wichtig, Mitarbeiter nicht nur auf die Einhaltung relevanter Anforderungen zu verpflichten, sondern ihnen diese auch nahe zu bringen sowie Hintergründe und Auswirkungen zu erläutern.

Relevante Anforderungen können je nach Branche und Ländern, in denen eine Institution tätig ist, sehr unterschiedlich sein. Eine wichtige Komponente stellen die Standards und Richtlinien zur Informationssicherheit und ihre konkrete Umsetzung in der Institution dar, da hier erfahrungsgemäß schon eine Reihe der übrigen Anforderungen verarbeitet wurde.

Beispielhafte Themen sind:

- Datenschutz in der Institution
  - Rolle und Aufgabe des Datenschutzbeauftragten
  - Datenschutzgesetz
  - Organisationspflichten
  - Umgang mit personenbezogenen Daten durch Mitarbeiter, z. B. Zusammenhang mit Protokoll-Dateien
- Arbeitsschutz
  - Rolle des Arbeitsschutzbeauftragten
  - Regelungen zu Bildschirmarbeitsplätzen
- Rechtliche oder regulatorische Vorgaben mit Bezug zur Informationssicherheit, soweit sie für die Institution relevant sind, wie z. B. PCI DSS, Basel III, etc.
- Gesetze und Normen zur technischen Infrastruktur
  - Brandschutz, Klimatisierung, Verkabelung, Blitzschutz, etc.
- Juristische Haftungsrisiken und IT-Nutzung
  - Nutzung oder Angebot von TK- oder Internetdiensten
  - Haftung des Unternehmens nach außen (z. B. KonTraG, Schäden durch Schadsoftware)
  - Haftung bei der Privatnutzung von IT-Komponenten
  - Rechtsrahmen bei der Mitarbeiterüberwachung
- Sonstige rechtliche Rahmenbedingungen
  - Ausfuhrbestimmungen für IT-Produkte, z. B. bei Verschlüsselung
  - digitale Signaturen und ihre rechtliche Stellung
  - Lizenz- und Urheberrecht für Software
- Umgang mit Angriffen auf interne IT
  - Strafbarkeit im Bereich Hacking
  - Gesetzlich zulässige Abwehrmaßnahmen
  - Verfolgung von Hacker-Straftaten

Modul 4: Sicherheitskonzept der Institution

Dieses Schulungsmodul vertieft die im Modul 2 behandelten Themen. Darüber hinaus soll es die System- und Aufgabenverantwortlichen in die Lage versetzen, an der permanenten Verbesserung und Weiterentwicklung des Sicherheitskonzeptes aufgrund technischer, organisatorischer oder rechtlicher Änderungen mitzuwirken.

Folgende Inhalte gehören unter anderem zu diesem Themengebiet:

- detaillierte Kenntnis der Anforderungen und Risiken, die als Basis für das Sicherheitskonzept dienen
- spezifische Risiken und Sicherheitsmaßnahmen des Sicherheitskonzeptes aus den Bereichen Management, Organisation, Infrastruktur, IT-Betrieb und Mitarbeiter
- Anpassung dieser Sicherheitsmaßnahmen an neue technische, organisatorische und rechtliche Gegebenheiten
- Revision und Aufrechterhaltung des Sicherheitskonzeptes

Modul 5: Risikomanagement

Dieses Schulungsmodul zeigt Verantwortlichen, wie sie Risiken der Informationssicherheit systematisch analysieren, bewerten und behandeln können.

Beispielhafte Themen sind:

- Definitionen und Beispiele zu den Begriffen: Gefährdung, Bedrohung, Schwachstelle, Risiko, Sicherheitsziel
- Typische Gefährdungen und Bedrohungen:
    - Höhere Gewalt: Feuer, Wasser, Explosion, Sturm, Erdbeben, Blitzschlag, Streik, Demonstration, etc.
    - Organisatorische Mängel: fehlende oder unzureichende Regelungen, ungeeignete Rechtevergabe, unkontrollierter Einsatz von IT-Systemen, Umgang mit sensiblen Informationen / Datenträgern etc.
    - Menschliche Fehlhandlungen: Irrtum, Nachlässigkeit, Neugier, Unwissenheit, etc.
    - Technisches Versagen: Stromausfall, Ausfall der Klimaanlage, Überspannung, Ausfall von Schaltelementen oder Schaltkreisen, Störungen in der Mechanik oder Elektronik, etc.
    - Vorsätzliche Handlungen: Schadprogramme, Diebstahl, Sabotage, Spionage, Manipulation, Vandalismus, Hacking und Cracking inklusive Gegenüberstellung von Angreifertypen und Motivationen, z. B. bei Innentätern oder bei Angreifern von außen
- Risikomanagement
    - Begriffe zum Risikomanagement: Risikoanalyse, -bewertung, -behandlung, -akzeptanz, Restrisiko
    - Erstellung einer Gefährdungsübersicht
    - Ermittlung zusätzlicher Gefährdungen
    - Gefährdungsbewertung
    - Identifizierung und Bewertung der Risiken
    - Risikobehandlung (Reduktion, Vermeidung, Übernahme, Transfer)
    - Umgang mit Restrisiken

Modul 6: Sicherheitsmanagement

Dieses Schulungsmodul umfasst für die Verantwortlichen wichtige Grundlagen zur Umsetzung der Informationssicherheit in der Institution. Folgende Inhalte gehören unter anderem zu diesem Themengebiet:

- Sicherheitsmanagement
  - Ziel und Aufgaben
  - Prozess (Informationssicherheitsmanagementsystem, ISMS) und Strategie (Leitlinie)
  - Bereitstellung von Ressourcen
  - Organisation und Verantwortlichkeiten
  - Standards wie ISO/IEC 2700x, IT-Grundschutz, ITIL, CobiT etc.
  - Durchführen von Reviews, Audits, Managementbewertungen
  - Planung und Umsetzung von Verbesserungsmaßnahmen
  - Einbindung der Mitarbeiter
- Sicherheitskonzept
  - Ziele und Inhalte eines Sicherheitskonzeptes
  - Aufbau eines Sicherheitskonzeptes
  - Verpflichtung von Mitarbeitern, System- und Aufgabenverantwortlichen zur Umsetzung des Sicherheitskonzeptes
- System- und anwendungsspezifische Sicherheitsrichtlinien
- Berechtigungsmanagement
  - Berechtigungskonzepte, Gestaltung der Rechtevergabe
  - Zugriffsrechte auf Systemressourcen, Zuweisung und zeitliche Begrenzung
  - Authentisierung (z. B. Stärken und Auswahl von Mechanismen)
  - Remote Zugriff (z. B. bei Telearbeit)

- Sensibilisierung und Training zur Informationssicherheit
  - Ausarbeitung passender Programme entsprechend den Rahmenbedingungen der Institution
- Evaluierung und Zertifizierung im Bereich Informationssicherheit
  - Produkt-/System-Zertifizierung (z. B. nach ITSEC, Common Criteria usw.)
  - Zertifizierung des Sicherheitsmanagements (z. B. nach IT-Grundschutz)
  - Experten-Zertifikate (z. B. TISP, CISA, CISSP, IT-Sicherheitskoordinator, Security+ usw.)
  - Experten-Zertifikate (z. B. TISP, CISA, CISSP, IT-Sicherheitskoordinator, Security+ usw.)
- Spezielle Probleme in der Informationssicherheit
  - Kommunikation mit Management und Fachabteilung
  - Kosten- und Akzeptanzprobleme

Modul 7: IT-Systeme

Dieses Schulungsmodul beschreibt die Steuerungsinstrumente, die in den verschiedenen Phasen des Lebenszyklus von IT-Systemen gewährleisten, dass die Sicherheitsnormen eingehalten werden.

Folgende Inhalte gehören unter anderem zu diesem Themengebiet:

- Sicherheitsmaßnahmen in den Lebenszyklus-Phasen
  - Planung
  - Beschaffung/Entwicklung
  - Test und Evaluierung
  - Implementierung bzw. Installation
  - produktiver Betrieb
  - Aussonderung
  - Notfallvorsorge
- Sicherheitsplanung für den Systembetrieb
  - Feststellung des Einsatzzweckes und -nutzens eines bestimmten IT-Systems
  - Festlegung der Schutzmaßnahmen für dieses System
  - Bestimmung der für den Systembetrieb Verantwortlichen
  - Installation und Konfiguration der in jeder Phase des Lebenszyklus erforderlichen Sicherheitsmechanismen
- Festlegung von Konfigurations-, Patch- und Änderungsmanagement in Abhängigkeit von den Sicherheitszielen
- Festlegung der Freigabekriterien für den operativen Betrieb
- Tests und Freigabe der Sicherheitsmechanismen

Modul 8: Operativer Bereich

Dieses Schulungsmodul beschreibt die Prozeduren und Maßnahmen, die operationelle Systeme und Anwendungen schützen sollen.

Folgende Inhalte gehören unter anderem zu diesem Themengebiet:

- Infrastruktur-Maßnahmen
  - Zugangskontrollen, Werkschutz, Alarmanlagen
  - Haustechnik, Energie- und Wasserversorgung
  - Brandschutzeinrichtungen
  - Klimaanlagen
- Organisatorische Maßnahmen
  - Dokumentation von Systemen und Konfgurationen, Applikationen, Soft- und Hardware-Bestand
  - Regelmäßige Kontrolle von Protokolldateien
  - Regelungen für die Datensicherung
  - Regelungen für den Datenträgeraustausch
  - Lizenzverwaltung und Versionskontrolle von Standardsoftware
- Maßnahmen im Bereich Personal
  - Auswahl, Einarbeitung und Schulung von Mitarbeitern
  - Geregelte Verfahrensweise beim Weggang von Mitarbeitern
  - Funktionen und Verantwortlichkeiten
  - Funktionstrennung und funktionsbezogene Rechtevergabe
  - Vertretungsregelungen
  - Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
- Maßnahmen im Bereich Hardware und Software
  - Grundlagen Betriebssystem-Sicherheit
  - Sichere Konfiguration von Hardware und Software
  - Schutz vor Schadprogrammen
  - Nutzung der in der Hardware bzw. den Anwendungsprogrammen vorhandenen Sicherheitsfunktionen
  - Implementierung zusätzlicher Sicherheitsfunktionen
  - Rechteverwaltung
  - Protokollierung
- Maßnahmen im Bereich Kommunikation
  - - Sichere Konfiguration von TK-Anlagen und Netzdiensten
    - E-Mail- und Internet-Sicherheit
    - Absicherung externer Remote-Zugriffe
    - Virtual Private Networks (VPN)
    - Sichere Nutzung mobiler IT-Systeme und drahtloser Kommunikation
    - Information über Sicherheitslücken (z. B. über CERTs) und Umgang mit Sicherheitsvorfällen

Modul 9: Technische Realisierung von Sicherheitsmaßnahmen

Dieses Schulungsmodul vermittelt Kenntnisse über die Möglichkeiten der technischen Realisierung der in den Modulen 6 bis 8 abstrakt beschriebenen Steuerungs- und Kontrollinstrumente.

Folgende Inhalte gehören unter anderem zu diesem Themengebiet:

- Basiswissen Kryptographie
  - Problemabgrenzung Vertraulichkeit, Integrität, und Authentizität
  - Grundbegriffe wie Klartext, Chiffrat und Schlüssel
  - Symmetrische, asymmetrische und hybride Verschlüsselung
  - Public Key Infrastrukturen
  - Digitale Signaturen
  - Aufzählung "guter" und "schlechter" bekannter Algorithmen
- Identifizierung und Authentisierung, z. B.
  - Begriffsdefinition (Wissen, Besitz, Eigenschaft)
  - Authentisierung durch Wissen: Passwörter, Einmal-Passwörter, Challenge-Response-Verfahren, digitale Signaturen
  - Authentisierung durch Besitz: Token, Chipkarten, etc.
  - Biometrische Verfahren: Fingerabdruckerkennung, Handvenenerkennung, Iriserkennung, Gesichtserkennung, etc.
  - Zwei- bzw. Multi-Faktor-Authentisierung
  - Single Sign-On
  - Berechtigungsmanagement
- Protokollierung und Monitoring, z. B.
  - Technische Möglichkeiten des "Transaction Logging"
  - Intrusion Detection, Response und Prevention Systeme (IDS, IRS, IPS), Unterschiede zwischen aktiven und passiven Systemen
  - Zwangsprotokollierung aller Administratoraktivitäten
  - Datenschutzaspekte
- Überblick über Administrationswerkzeuge
  - Werkzeuge, mit denen Sicherheitsvorgaben realisiert und kontrolliert werden können
  - Zusatzprodukte zur Ergänzung bzw. Verbesserung der Sicherheitsfunktionen von Betriebssystemen ("gehärtete Betriebssysteme")
  - Netzmanagement-Software
  - Remote-Management-Software
- Firewalls (Sicherheitsgateways)
  - Internet-Technik (OSI-Modell, TCP/IP)
  - Realisierungsformen (statische Paketfilter, Stateful Inspection, Application Level Gateways)
  - Content Security
  - Hochverfügbare Firewalls
- Schutz der Vertraulichkeit: Kryptografische Verfahren und Produkte, Zugriffsschutz z. B. durch Festplattenverschlüsselung, Kryptografie auf den verschiedenen Schichten des OSI-Modells
  - Protokolle für Schicht 1 und 2 (ISDN-Verschlüsselung, ECP und CHAP, WLAN, Bluetooth)
  - Protokolle für Schicht 3 (IPsec, IKE, SINA)
  - Protokolle für Schicht 4 und höher (SSL/TLS, S/MIME)
- Schutz der Verfügbarkeit
  - Organisatorische Maßnahmen zur Erhöhung der Verfügbarkeit (SLAs, Change Management, Vermeidung von SPOF)
  - Datensicherung, Datenwiederherstellung
  - Speichertechnologien
  - Netzkonfigurationen zur Erhöhung der Verfügbarkeit
  - Infrastrukturelle Maßnahmen zur Erhöhung der Verfügbarkeit
  - Verfügbarkeit auf der Client, Server und Anwendungsebene (Server-Standby, Failover)
  - Methoden zur Replikation von Daten
  - Wiederanlauf- und Geschäftsfortführungsmaßnahmen
- Technische Möglichkeiten zum Schutz von TK-Anlagen
  - Schutz vor Abhören
  - Schutz der Datenleitungen z. B. durch alarmüberwachte und plombierte Leitungsschächte, gesicherte Verteiler (Knoten), Verschlüsselung der Nachrichten, etc.
  - Sicherung von Wartungs-, Fernwartungs-, und Administratorenzugängen
  - Protokollierung jedes Systemzugangs, Löschungsschutz der Protokolldateien
- Erkennen von Schwachstellen des eigenen Systems mittels Penetrationstests
- Hacker-Methoden, Web-Seiten-Hacking, Schutz vor: Sniffer, Scanner, Password Cracker, etc.

Modul 10: Notfallmanagement

Dieses Schulungsmodul soll die Grundlagen zur Etablierung und Aufrechterhaltung eines Notfallmanagements in der Institution vermitteln. Thematisch stellt es einen Aufbaukurs zum Modul 5 "Risikomanagement" dar. Die Schulungsinhalte können gemäß der Struktur des BSI-Standards 100-4 aufgebaut werden.

Folgende Inhalte sollten vorgesehen und entsprechend den Inhalten des BSI-Standards 100-4 weiter detailliert werden:

- Einführung: Ziel, Aufgaben, Begriffe, Abgrenzung von Business Continuity und IT Service Continuity, Standards
- Der Prozess im Überblick
- Initiierung des Prozesses
- Konzeption
- Umsetzung des Notfallvorsorgekonzepts
- Notfallbewältigung und Krisenmanagement
- Tests und Übungen

Modul 11: Neue Entwicklungen im IT-Bereich

Dieses Schulungsmodul soll IT-Systembetreiber über Innovationen auf ihrem Gebiet informieren. Um stets auf dem aktuellen Stand zu sein, sollte dieses Seminar in regelmäßigen Abständen von etwa zwei Jahren wieder besucht werden. Alternativ können der angesprochenen Zielgruppe auch die Ressourcen bereitgestellt werden, um sich aus verfügbaren Informationsquellen entsprechend selbstständig zu informieren.

Folgende Inhalte gehören unter anderem zu diesem Themengebiet:

- Hardware-Architekturen, Schnittstellen, Bussysteme, Peripherie
- Speicher-/Archivierungstechnologien und -systeme
- Hochverfügbarkeitslösungen
- Client- / Server-Betriebssysteme
- Software-Architekturen
- Terminal Server, N-Tier, Host versus Client/Server
- Datenbanken
- Cloud Computing
- Mobile Computing
- Data Warehouse, SharePoint, etc.
- Netztechnologie
- Informationssicherheit, insbesondere neue Bedrohungen und Schwachstellen zu allen angesprochenen Themen

Modul 12: Betriebswirtschaftliche Seite der Informationssicherheit

Dieses Schulungsmodul ist speziell für das Management und Entscheidungsträger gedacht, um Informationssicherheit übergreifend in die Planung der Institution zu integrieren.

Folgende Inhalte gehören unter anderem zu diesem Themengebiet:

- Betriebswirtschaftliche Vorteile der Informationssicherheit
  - Risikominimierung
  - Beschleunigung der Bearbeitung
  - Reduzierung des Aufwands
  - Umsatzerhöhung
  - Erschließen neuer Geschäftsfelder
  - sonstiger Nutzen
- Kalkulation der Investitionen für Informationssicherheit
  - Erstellung einer Kostenübersicht
  - Abgrenzung gegenüber Betriebs- und Fortschreibungskosten
  - Verdeckte Kosten
- Investitionsrechnung in der Informationssicherheit
  - Investitionsrechnung
  - Argumentation gegenüber dem Management
- Verzahnung von Sicherheitsmaßnahmen im Unternehmen
  - Berücksichtigung der Geschäftsprozesse und der Geschäftsvorfälle bei den Sicherheitsmaßnahmen
  - Einfluss- und Verantwortungsbereiche, typische Stolpersteine
  - Informationssicherheit bei der IT-Beschaffung und in IT-Projekten
- Erfolgsfaktoren der Informationssicherheit
  - Wie gelingt ein Projekt zur Informationssicherheit?
  - Klärung der Erwartungshaltung
  - Konzeption von Sicherheitslösungen
  - Erstellen eines Konzepts
  - Gliedern in Teilprojekte
  - Umsetzen der Teilprojekte
  - Modul- und Funktionstests
  - Akzeptanz- und Integrationstests
  - Inbetriebnahme
- Häufige Fehler bei der Umsetzung von Informationssicherheit
  -
    - Fehler bei der Projektleitung
    - andere typische Fehler

Modul 13: Infrastruktursicherheit

Dieses Modul befasst sich mit dem Schutz der Informationstechnik mit Hilfe von baulichen und technischen Maßnahmen. Diese Maßnahme schließt die prozessuale Aktualisierung der Inhalte bei Veränderungen in Infrastrukturen und Rahmenbedingungen ein.

Wichtige Punkte dabei sind unter anderem:

- Objektschutz
  - Absicherung des Standortes: Umgebung, Umfriedung, Freilandschutz, Nachbarschaftsgefahren und Zonenbildung
  - Bautechnik: Einbruchschutz, Brandschutz, Klimaschutz, Schutz gegen Wasser, etc.
  - Technische Überwachung
  - Geräteschutz
- Zutrittskontrolle
  - Pförtnerdienst
  - Verschluss von Räumen
  - Technische Zutrittskontrolle
- Stromversorgung
  - Überspannungsschutz
  - Unterbrechungsfreie Stromversorgung
  - Trassen/Verkabelung

Weitere Module

Je nach Art und Ausprägung der Institution kann es sinnvoll sein, zielgruppenspezifische weitere Module vorzusehen. Wenn die Institution industrielle Steuerungssysteme einsetzt, ist es beispielsweise sinnvoll, hierzu ein Modul anzubieten.

ORP.3.M7 Schulung zur Vorgehensweise nach IT-Grundschutz

Sicherheitsverantwortliche müssen die IT-Grundschutz-Methodik sehr gut kennen, um sie erfolgreich anwenden zu können. Das Vorgehen in der Institution muss sich an der jeweils aktuellen Ausprägung des Standards und der Ausrichtung des ISMS in der Institution orientieren. Es gibt verschiedene Möglichkeiten, um sich in die Vorgehensweise nach IT-Grundschutz einzuarbeiten:

- Selbststudium
- Web-Kurs des BSI zum Einstieg in die IT-Grundschutz-Vorgehensweise
- Durcharbeiten der BSI-Beispielunterlagen des fiktiven Unternehmens RECPLAST
- Externe Schulungsanbieter von IT-Grundschutz-Schulungen
  Hinweis: Auf den BSI-Webseiten findet sich eine Liste von Schulungsanbietern zum Thema IT-Grundschutz. Das BSI hat dabei Schulungsqualität und Schulungsinhalte nicht bewertet.
- Erarbeitung eigener IT-Grundschutz-Schulungen

Wenn eine neue IT-Grundschutz-Schulung geplant wird oder eine extern angebotene Schulung zu beurteilen ist, sollten die folgenden Inhalte einbezogen werden:

- Sensibilisierung für Informationssicherheit
- Was ist ein Informationssicherheitsmanagementsystem (ISMS)? Wie wird ein funktionierender Sicherheitsprozess etabliert?
- Überblick über das IT-Grundschutzkonzept (Philosophie, Anwendungsgebiet, Struktur)
- Erstellung einer Leitlinie zur Informationssicherheit
  - Definition von Informationssicherheitszielen
  - Definition des Informationsverbundes
- Informationssicherheitsmanagement
  - Organisationsstrukturen (Darstellung geeigneter Organisationsstrukturen für das Informationssicherheitsmanagement)
  - Rollen (Informationssicherheitsbeauftragter, Sicherheitsmanagement-Team, etc.)
  - Verantwortlichkeiten
- Sicherheitskonzept: typischer Aufbau und Inhalte
- Auswahl einer geeigneten IT-Grundschutz-Vorgehensweise:
  - Basis-Absicherung
  - Kern-Absicherung
  - Standard-Absicherung
- Strukturanalyse
  - Gruppenbildung
  - Erfassung der Anwendungen und der zugehörigen Informationen
  - Erstellung eines Netzplans
  - Erhebung der IT-, ICS- und IoT-Systeme
  - Erfassung der Räume
- Schutzbedarfsfeststellung
  - Vorgehensweise
  - Definition der Schutzbedarfskategorien inklusive individueller Anpassung der Bewertungstabellen
  - Schadensszenarien
  - Schutzbedarfsfeststellung für Geschäftsprozesse, Anwendungen, IT-, ICS- und IoT-Systeme, Kommunikationsverbindungen und Räume
- Modellierung nach IT-Grundschutz
  - Überblick über die IT-Grundschutz-Bausteine
  - Schichtenmodell
    - Bausteine der Prozess-Schichten
    - Bausteine der System-Schichten
- IT-Grundschutz-Check
  - Darstellung der Vorgehensweise
  - Umsetzungsstatus
- Risikoanalyse basierend auf IT-Grundschutz
- Erfüllung der Sicherheitsanforderungen
  - Sichtung aller noch nicht erfüllten Anforderungen
  - Konsolidierung der Anforderungen
  - Kosten und Aufwandsabschätzungen (Budgetierung)
  - Realisierung von Maßnahmen zur Erfüllung der Anforderungen (Umsetzungsreihenfolge, Verantwortliche, Realisierungsplan)
- IT-Grundschutz-Profile als Schablone
- Hilfsmittel zur Arbeit mit dem IT-Grundschutz-Kompendium
  Das BSI stellt verschiedene Hilfsmittel zur Verfügung, die die praktische Arbeit mit dem IT-Grundschutz-Kompendium erleichtern. Die Folgenden sollten den Anwendern vorgestellt werden:
  - Leitfaden als Motivation für Informationssicherheit
  - Webkurs als Einstieg in die IT-Grundschutz-Vorgehensweisen
  - Tabellen und Formblätter als Hilfsmittel bei der Umsetzung
  - Musterrichtlinien und Profile als Beispielanwendungen
  - Tool-Unterstützung bei der Erstellung, Verwaltung und Fortschreibung von Sicherheitskonzepten auf der Basis von IT-Grundschutz. Diverse Hersteller bieten hierfür geeignete IT-Grundschutz-Tools an.
- Kurzvorstellung der ISO 27001
  - Die Standardfamilie ISO 2700x
  - Aufbau des Standards ISO 27001
  - Zuordnung der Normkapitel von ISO 27001 zu den BSI-Standards sowie der Themen im An-

In einer umfassenden IT-Grundschutz-Schulung sollten die Teilnehmer die dargestellte Vorgehensweise anhand von Beispielen üben.

ORP.3.M8 Messung und Auswertung des Lernerfolgs [Personalabteilung]

Die Lernerfolge im Bereich Informationssicherheit sollten zielgruppenbezogen gemessen und ausgewertet werden, um festzustellen, inwieweit die in den Sensibilisierungs- und Schulungsprogrammen beschriebenen Ziele erreicht sind (vergleiche ORP.3.M4 Konzeption eines Schulungs- und Sensibilisierungsprogrammes zur Informationssicherheit). Dadurch ist es möglich, ein detailliertes Gesamtbild zu erhalten und punktuelle Korrekturmaßnahmen zu ergreifen, falls einzelne Ziele nicht erreicht wurden.

Die Personalabteilung verfügt oft über gute Erfahrungen in der Auswertung von Schulungsmaßnahmen. Daher ist es empfehlenswert, sich an dieser Vorgehensweise zu orientieren und sich dazu mit der Personalabteilung abzustimmen.

Um den Lernerfolg zu testen, sollten sowohl quantitative als auch qualitative Aspekte der Sensibilisierungs- und Schulungsprogramme berücksichtigt werden. Die Ergebnisse sollten bei der Verbesserung des Sensibilisierungs- und Schulungsangebots geeignet einfließen.

Die folgenden Möglichkeiten können dafür genutzt werden:

Dokumentation durchgeführter Sensibilisierungs- oder Schulungsmaßnahmen

Die Dokumentation aller Maßnahmen inklusive einer Kurzbeschreibung der Inhalte und der Durchführungszyklen geben einen ersten Überblick über den Umfang und die betroffenen Zielgruppen der durchgeführten Aktivitäten.

Dokumentation der Teilnehmerzahlen an Sensibilisierungs- oder Schulungsmaßnahmen

Die Dokumentation der Teilnehmerzahlen von Schulungen oder die Anzahl der von Sensibilisierungsmaßnahmen erreichten Mitarbeiter pro Abteilung, Bereich, Standort, etc. liefern einen Hinweis auf die erzielte Durchdringung der Maßnahmen in der Institution.

Anzahl der Anfragen an Ansprechpartner in Sicherheitsfragen (siehe ORP.3.M2 Ansprechpartner zu Sicherheitsfragen)

Wenn nach Schulungs- oder Sensibilisierungsmaßnahmen die Anzahl der Kontakte zu den Ansprechpartnern in Sicherheitsfragen steigt, kann das als Indiz für eine stärkere Sensibilität der Mitarbeiter gewertet werden, aber auch als Folge des gestiegenen Bekanntheitsgrades der Einrichtung.

Schulungsbewertungen

Einen ersten qualitativen Überblick über die Schulungserfolge geben standardisierte Schulungsbewertungsbögen, wie sie üblicherweise am Ende einer Veranstaltung durch die Teilnehmer ausgefüllt werden. Neben Fragen zum Ablauf, der Veranstaltungsorganisation oder der Vorgehensweise des Referenten können hier Fragen zur Nutzenbewertung durch die Teilnehmer eingearbeitet werden.

Test zum Schulungsabschluss

Während oder nach einer Schulungsveranstaltung durchgeführte Wissenstests sind erprobte Methoden zur Lernerfolgskontrolle. Angepasst auf die jeweiligen Veranstaltungsinhalte können dabei Fragen nach erlerntem Wissen, aber auch Fragen zur Einschätzung beschriebener Situationen die Grundlage bilden.

Wissenstest in zeitlichem Abstand

Um den Verlauf von Lernkurven nach Schulungsveranstaltungen zu ermitteln, können nach dem Ende einer Schulung zu festgelegten Zeitpunkten weitere Tests durchgeführt werden. Da hier ein direkter Bezug zur Veranstaltung fehlt, kann es schwierig sein, die Teilnehmer dazu zu motivieren, Wissensfragen zu beantworten. Um dem entgegenzuwirken, kann dieser Test auch in Quiz-Form durchgeführt werden, z. B. mit Preisen für die Teilnehmer. Weit verbreitet ist auch das Vorgehen, jährlich ein Mindestmaß an grundlegendem Wissen nachzuweisen. Dazu empfehlen sich WBT-Module (Web Based Traning), also Intranet-basierte Schulungsmodule, die von den Mitarbeitern zu einer selbstbestimmten Zeit bearbeitet werden können.

Mitarbeiterbefragungen

Durch Mitarbeiterinterviews mit standardisierten Fragebögen können Informationen darüber gesammelt werden, ob auch nicht-schulische Sensibilisierungsmaßnahmen wirksam sind.

Anzahl von Regelverstößen

Eine weitere Variante zu bewerten, ob eine Maßnahme erfolgreich war, ist es, die Anzahl von Regelverstößen vor und nach den Sensibilisierungsmaßnahmen zu zählen. Dazu können Verantwortliche auch bewusst und kontrolliert Sicherheitslücken platzieren und dann beobachten, wie Mitarbeiter damit umgehen. Hierzu eignen sich beispielsweise:

- Fremdpersonen ohne Mitarbeiterausweis, die unbegleitet in der Institution herumlaufen
- USB-Sticks, die an verschiedenen Stellen in der Institution ausliegen
- E-Mails, die mit Anhang oder Links auf unbekannte Webseiten, aber mit vertraut klingenden Absenderadressen an die Mitarbeiter versendet werden
- Türschließfunktionen, die blockiert werden

Wichtig ist hierbei, die Ergebnisse nie als Fehlverhalten einzelner Mitarbeiter zu deuten, sondern als Ergebnisse von Gruppen. Ein solches Vorgehen ist zudem sorgfältig in der Institution abzustimmen (etwa unter Einbeziehung von Führungsebene und Personalvertretung).

Social-Penetration-Tests / Social-Engineering-Audits

Um einen Lernerfolg im Rahmen der Social-Engineering-Vorbeugung zu prüfen, können Social-Penetration-Tests bzw. Social-Engineering-Audits durchgeführt werden. Hierbei wird in der Rolle eines externen Angreifers versucht, Fehlverhalten von Mitarbeitern auszunutzen und Informationen zu erlangen, mit deren Hilfe der Tester zu den vorgesehenen Angriffszielen kommt.

Diese Art von Audits sind jedoch immer umstritten, da Mitarbeiter, die ohne ihr Wissen als Angriffsziel ausgewählt wurden, die Auswertung nach einem erfolgreichen Angriff als Vertrauensbruch oder Bloßstellung ansehen könnten. Auf der anderen Seite liefern solche Audits gute Einblicke, inwieweit Informationssicherheit wirklich gelebt wird. Daher ist der Einsatz dieser Methode im Einzelfall zu prüfen und gemeinsam mit der Personalvertretung und dem Management abzuwägen.

Praktische Übungen

Als Alternative zu den beschriebenen Social-Penetration-Tests können auch praktische Übungen eingesetzt werden. Hier sind unterschiedliche Varianten möglich, die einen Überblick über das Sensibilisierungs- und Schulungsniveau geben. Im Nachgang zu Schulungen können Übungssequenzen aufgebaut werden, in denen Situationen spielerisch dargestellt sind, zum Beispiel ein Social-Engineering-Angriff. Die Aufgabe für freiwillige Teilnehmer aus der Gruppe würde darin bestehen, auf diesen Angriff zu reagieren. Eine anonyme Bewertung der Übung durch den Seminarleiter gibt Aufschluss über den Lernerfolg vorangegangener Maßnahmen.

Tools und Spiele

Lernspiele oder -tools jeglicher Art bieten in den meisten Fällen ebenfalls die Möglichkeit, Spielergebnisse oder Ergebnisentwicklungen auszuwerten.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

ORP.3.M9 Spezielle Schulung von exponierten Personen und Institutionen (CIA)

Gibt es in der Institution besonders exponierte Personen wie Funktions- oder Geheimnisträger, oder ist die Institution bzw. einzelne Bereiche selbst ein attraktives Ziel (z. B. für mögliche IT-Angriffe oder Industriespionage), so sollten diesbezüglich vertiefende Schulungen in Hinblick auf mögliche Gefährdungen und geeignete Verhaltensweisen sowie Vorsichtsmaßnahmen durchgeführt werden.

Hierzu gehören beispielsweise präzise Vorgaben zum Umgang mit sensiblen Informationen oder Verhaltenstrainings für konkrete Situationen.

Wenn in der Institution hochschutzbedürftige oder geheimschutzrelevante Informationen verarbeitet werden, sollte überlegt werden, auch hierzu spezielle Schulungen anzubieten. Beispielsweise könnte das Schulungsprogramm (siehe ORP.3.M6 Planung und Durchführung von Schulungen zur Informationssicherheit) um ein weiteres Modul zum Geheimschutz erweitert werden.

Modul: Geheimschutz

Mitarbeiter, die mit Aufgaben im Umfeld des materiellen und IT-Geheimschutz befasst sind, sollten grundlegende Kenntnisse und Fähigkeiten für die Ausübung von Tätigkeiten im Bereich des materiellen und IT-Geheimschutzes haben. Das Modul zum Umgang mit geheimschutzrelevanten Informationen am Arbeitsplatz sollte unter anderem die folgenden Themenschwerpunkte umfassen:

- Grundlagen des personellen und materiellen Geheimschutzes
- Struktur und Inhalt der Verschlusssachenanweisung (VSA)
- aktuelle und vertiefende Darstellung der
- organisatorischen Maßnahmen (z. B. Geheimschutzdokumentation)
- materiell-technischen Maßnahmen (z. B. technische Leitlinien, Lauschabwehr)
- IT-spezifische Maßnahmen (z. B. IT-Sicherheitsprodukte und Betriebsumgebungen, Zulassung/Zertifizierung/Freigabe, Abstrahlsicherheit)
- Anwendungsbeispiel zur Verarbeitung von geheimschutzrelevanten Informationen im Informationsverbund

3 Weiterführende Informationen

3.1 Wissenswertes

Je nach Branche, eingesetzter Technik oder anderen Rahmenbedingungen können sich für einen Informationsverbund weitere (benutzerdefinierte) Anforderungen ergeben. Zu diesen können beispielsweise die folgenden Maßnahmen gehören.

Zu den wichtigsten Grundpfeilern der Informationssicherheit in einer Institution gehören deren Mitarbeiter. Selbst die aufwendigsten technischen Sicherheitsvorkehrungen sind ohne das richtige Verhalten der Mitarbeiter wertlos. Ein Bewusstsein dafür, was Informationssicherheit für die Institution und deren Geschäftsprozesse bedeutet und der richtige Umgang der Mitarbeiter mit den zu schützenden Werten und Informationen der Institution sind dafür wesentlich.

Die für die Institution ausgewählten Sicherheitsmaßnahmen sollten sich daher immer an den Mitarbeitern orientieren. Dabei sollte deren Wissen und Umgang mit Informationen und IT einbezogen werden. Zur Beurteilung, wie sich Mitarbeiter aus Sicherheitssicht verhalten, können die Faktoren analysiert werden, die zu diesem Verhalten beitragen. Darauf aufbauend kann untersucht werden, wo die personelle und organisatorische Sicherheit noch verbessert werden kann, beispielsweise durch Sensibilisierung und Schulung zur Informationssicherheit.

Folgende Aspekte sollten berücksichtigt werden:

Sicherheitskultur

Der Begriff Sicherheitskultur umfasst die sicherheitsbezogenen Einstellungen, Werte und grundlegenden Überzeugungen einer Institution und aller ihrer Mitarbeiter. Zur Sicherheitskultur gehört auch, wie offen der Umgang mit Fragen zur Informationssicherheit in der Institution gelebt wird. So ist für die effektive und effiziente Behandlung von Sicherheitsvorfällen eine vertrauensvolle und offene Kommunikationskultur wichtig, damit Sicherheitsvorfälle auch umgehend weitergemeldet und lösungsorientiert angegangen werden.

- Wie ist der Umgang in der Behörde oder dem Unternehmen mit geschäftsrelevanten Informationen und mit Risiken generell? Ist die Institution eher risiko-orientiert oder eher risiko-vermeidend? Werden Informationen eher freizügig oder nur restriktiv weitergegeben?
- Wie sind die Anforderungen an Genauigkeit und Präzision? Sind kleinere Fehler beispielsweise in Texten tragbar, weil diese ohnehin noch mehrere Abstimmprozesse durchlaufen müssen? Kann ein Eingabefehler bereits zu folgenschweren Schäden führen?
- Wie sind die Ansprüche an Verfügbarkeit? Gibt es eine Vielzahl enger Termine? Können Bearbeitungszeiten für Anfragen und Geschäftsprozesse flexibel festgelegt werden? Sind kleinere Terminüberschreitungen oder -änderungen im Allgemeinen tragbar oder führen sie zu harten Konsequenzen?

Stark beeinflusst wird die Sicherheitskultur einer Institution davon, in welcher Branche diese tätig ist. In Hochsicherheitsbereichen wird naturgemäß weniger offen mit Informationen umgegangen als in Forschungseinrichtungen.

Wissen und Können

- Wie gut kennen sich die Mitarbeiter mit IT aus? Ist IT- und Internet-Nutzung eher eine Notwendigkeit, um Geschäftsprozesse effektiver gestalten zu können, oder sind Leben und Arbeiten ohne IT und Internet nicht mehr vorstellbar?
- Welche Erfahrungen und Kenntnisse haben die Mitarbeiter bzgl. Informationssicherheit und Datenschutz? Wie ausgebildet sind deren Fähigkeiten auf dem Gebiet der IT-basierten Sicherheitsmaßnahmen wie z.B. Verschlüsselung? Wie ist das Wissen in den verschiedenen Bereichen der Institution verteilt?
- Wie ist der gelebte Umgang der Mitarbeiter mit Fragen der Informationssicherheit und des Datenschutzes? Wie sehen die Mitarbeiter den Bedarf, Informationen vor Veränderungen oder unbefugter Weitergabe zu schützen?
- Können Mitarbeiter aktiv ihre Ideen und Vorstellungen zur Informationssicherheit in den Sicherheitsprozess einbringen?

Sicherheitsrichtlinien

- Passen die Sicherheitsrichtlinien der Institution zu den Geschäftsprozessen und der internen Sicherheitskultur? Sind sie einfach umzusetzen? Sind sie praxisnah und den aktuellen Umgebungsbedingungen angepasst? Behindern sie Arbeitsläufe? Unterstützen sie erwünschte Verhaltensweisen? Sind Sie allen bekannt?

Anwendungen und IT

- Ermöglichen die vorhandenen IT-, ICS- und IoT-Komponenten einen Umgang mit den geschäftsrelevanten Informationen, der sowohl deren Schutzbedarf als auch den festgelegten Sicherheitsvorgaben entspricht?

Leitungsebene

- Wie steht die Leitungsebene zur Informationssicherheit? Nehmen Vorgesetzte ihre Vorbildfunktion wahr? Gibt es Wünsche der Leitungsebene zur Verbesserung der Sicherheitsprozesse?

Kulturelle Hintergründe

- Auch die kulturellen Hintergründe können den Umgang mit zu schützenden Informationen und mit Sicherheitsvorgaben generell beeinflussen. Daher sollte untersucht werden, ob es regionale und nationale Unterschiede im Umgang mit Informationssicherheit gibt. Vor allem sollte auch ergründet werden, welche unterschiedlichen Herangehensweisen an Informationssicherheit es in den verschiedenen Bereichen der Institution gibt. Auch einzelne Abteilungen oder Außenstellen können bereits eigene Regeln und Verhaltensweisen im Umgang mit geschäftsrelevanten Informationen entwickeln.

Veränderungen

- Alle Arten von weitreichenden Veränderungen für die Beschäftigten können deren Umgang mit Informationen, Geschäftsprozessen, IT und sonstigen Geräten ändern. Dazu gehören beispielsweise Umstrukturierungen, Entlassungen, Wechsel von Aufgaben oder Vorgesetzten.

Sollte sich bei der Analyse herausstellen, dass sich Mitarbeiter anders verhalten als es aus Sicherheitssicht sinnvoll ist, gibt es verschiedene Wege, um hiermit umzugehen. Es sollte versucht werden, das Verhalten der Beschäftigten zu ändern. Andererseits kann es in vielen Fällen einfacher sein, die Sicherheitsvorgaben oder Arbeitsabläufe umzugestalten und sicherer zu machen.

Die Verantwortlichen für Sensibilisierungs- und Schulungsprogramme sollten klären, ob und in welchem Umfang sie eigene Mitarbeiter oder externe Anbieter als Trainer einsetzen wollen. Außerdem muss die Form der Ausbildung festgelegt werden. Sofern ein Programm mehrere Sensibilisierungs- und Schulungsmaßnahmen umfasst, sollte ein Schulungskoordinator ernannt werden. Darüber hinaus sollten verschiedene Angebote von Schulungsanbieter daraufhin verglichen worden, welche inhaltlich, qualitativ und preislich am besten geeignet sind. Die durchgeführten Sensibilisierungs- oder Schulungsmaßnahmen sollten von den Teilnehmern bewertet und diese Erfahrungen regelmäßig intern ausgewertet werden.

Wenn eigene Mitarbeiter als Trainer eingesetzt werden sollen, müssen diese das benötigte Fachwissen haben und dazu fähig sein, dieses Wissen auch zielgruppengerecht zu vermitteln. Neben den erforderlichen Informationssicherheitskenntnissen müssen die Trainer über ausgeprägte didaktische, methodische und kommunikative Fähigkeiten verfügen. Speziell für Sensibilisierungsmaßnahmen sind außerdem ausreichende Kenntnisse über die Institution, deren Sicherheitskultur sowie die Geschäftsprozesse erforderlich. Wichtig ist, dass Trainer die Sprache ihres jeweiligen Zielpublikums beherrschen, also die zu schulenden Informationssicherheitsaspekte in die jeweiligen Arbeits- und Projektzusammenhänge stellen können. Interne Trainer müssen die erforderliche Zeit bekommen, um Sensibilisierungs- und Schulungsmaßnahmen nicht nur durchführen, sondern auch vorbereiten und auswerten zu können.

Aus Kosten- oder Qualifikationsgründen kann es zumindest zu Beginn vorteilhafter sein, die Schulung durch externe Fachkräfte durchführen zu lassen. Schon in der Planungsphase muss geklärt werden, welche finanziellen Ressourcen dafür verfügbar sind. Die externen Trainer sollten sorgfältig anhand von inhaltlichen, qualitativen und preislichen Kriterien ausgewählt und auf ihre Aufgabe vorbereitet werden. Insbesondere müssen ihnen die erforderlichen institutionsinternen Hintergründe vermittelt werden. Interne Referentinnen und Referenten können diese Kurse begleitend nutzen, um sich auf ihren eigenen Einsatz vorzubereiten.

Auch bei externer Durchführung von Sensibilisierungs- oder Schulungsmaßnahmen sind interne Ressourcen erforderlich. Es sollte ein verantwortlicher Schulungskoordinator benannt werden, der

- qualifizierte Schulungsanbieter auswählt,
- Lerninhalte und -methoden vorgibt sowie den Trainern erforderliche Informationen zur Verfügung stellt,
- die interne Schulungsplanung, -vorbereitung und -durchführung koordiniert,
- die Kommunikationsschnittstelle zwischen Trainern und eigenen Mitarbeitern bildet,
- die Teilnehmerbewertungen analysiert und geeignete Verbesserungsmaßnahmen festlegt, gegebenenfalls zusammen mit den Trainern.

Die Schulungskoordination kann der Informationssicherheitsbeauftragter, auch ein Mitarbeiter aus der Personalabteilung oder eine Person aus dem ISMS Team rund um den ISB übernehmen. Der Informationssicherheitsbeauftragte und die Personalabteilung müssen hierbei auf jeden Fall eng zusammenarbeiten.

Erfahrungsgemäß gibt es eine Reihe von externen Anbietern, die geeignete Sensibilisierungs- oder Schulungsmaßnahmen in einer Form anbieten, die den Bedürfnissen der Institution entsprechen oder die mit vertretbarem Aufwand angepasst werden können.

Bei Sensibilisierungs- oder Schulungsmaßnahmen, die in mehreren Zyklen eine größere Zahl von Mitarbeitern erreichen sollen, bietet es sich an, über ein "Train the Trainer"-Konzept nachzudenken. Hierbei werden die initialen Maßnahmen entweder von geeigneten internen Mitarbeitern oder externen Trainern mit dem Ziel durchgeführt, dass die Teilnehmer dieser Maßnahmen später selbst eine Trainerrolle übernehmen. Dies kann für diese Mitarbeiter einen sehr positiven Effekt auf ihre eigene Sensibilisierung und Motivation für Informationssicherheit haben. Darüber hinaus können sie ihre eigenen Erfahrungen in die Trainingsmaßnahmen einbringen. Gerade bei Trainingsthemen, die Aspekte der Kultur und bestimmter Verhaltensweisen innerhalb der Institution beinhalten, kann ein interner Trainer aufgrund seiner tieferen Kenntnis interner Prozesse und Bekanntheit bei den Teilnehmern die Akzeptanz und den Lernerfolg des Trainings erhöhen. Sofern das "Train the Trainer"-Konzept eingesetzt werden soll, müssen die initialen Maßnahmen neben den vorgesehenen Fachinhalten auch Anleitungen zur methodisch-didaktischen Lehrstoffvermittlung beinhalten.

Die durchgeführten Sensibilisierungs- oder Schulungsmaßnahmen sollten von den Teilnehmern abschließend bewertet werden. Diese Erfahrungen sollten regelmäßig intern ausgewertet werden.

Viele Sicherheitsschulungen empfinden Teilnehmer als trocken, was negative Auswirkungen auf den gewünschten Lerneffekt mit sich bringt. Eine gute Möglichkeit, den Lehrstoff aufzulockern, sind Plan- oder Rollenspiele. An solche Spiele erinnern sich die Teilnehmer meist länger und prägnanter als an klassische Folienpräsentationen. Auch tragen sie dazu bei, die Bedrohungen stärker zu verdeutlichen und typische Schwachstellen, aber auch Lösungsmöglichkeiten in der eigenen Arbeitsumgebung aufzuzeigen. Sie ermöglichen es den Teilnehmern, Situationen zu üben, um dann im Ernstfall routinierter zu agieren. Es sollte geprüft werden, ob die restlichen Sensibilisierungs- und Schulungsinhalte durch den Einsatz von Planspielen unterstützt werden können.

Planspiele können aus praktischen Beispielen, z. B. anhand aktueller Vorfälle aus den Medien, selbst zusammengestellt oder bei Schulungsdienstleistern in Auftrag gegeben werden. Dabei sind die Inhalte der Planspiele möglichst an die eigene Institution anzupassen. Dadurch können sich die Mitarbeiter besser mit den aufgezeigten Lösungen identifizieren. Durch die Simulation z. B. von Sicherheitsvorfällen, die geschäftskritische Prozesse beeinträchtigen können, sind die Mitarbeiter im Ernstfall gut vorbereitet.

Genau wie bei Schulungen ist bei diesen Formaten die zielgruppengerechte Planung von Inhalten sehr wichtig. Die Teilnehmer sollen die Relevanz der Rollenspiele erkennen und in ihrem Arbeitsumfeld unmittelbar davon profitieren können.

Bei allen Bemühungen, die Mitarbeiter auf die Bedeutung von Informationssicherheit aufmerksam zu machen, soll eine positive und konstruktive Grundstimmung bewahrt werden. Ständige Angst vor Sicherheitsvorfällen kann einerseits zur Verdrängung von Sicherheitsproblemen und andererseits zu Panikreaktionen verleiten.

Die folgenden Beispiele zeigen, dass Planspiele von sehr einfach zu realisierenden Übungen, die im Rahmen einer Schulung durchgeführt werden können, bis hin zu komplexen Simulationsübungen reichen können. Die Aufgabe der verantwortlichen Planer ist es nun, entsprechend den Erfordernissen der unterschiedlichen Zielgruppen die geeigneten Szenarien zu entwickeln.

Tragen von Mitarbeiterausweise

Durch kurze Rollenspiele können Mitarbeiter sehr gut üben, wie sie sich verhalten sollen, wenn sie innerhalb der Institution organisationsfremde Personen antreffen. Es kann eingeübt werden, wie die Mitarbeiter optimal auf diese Situation reagieren können, beispielsweise indem sie anbieten, die Externen zum Gesprächspartner zu begleiten. Auch der Umgang mit Besuchern, die die Hausregeln kennen, aber verweigern, kann trainiert werden, beispielsweise wenn ein Besucher das Tragen eines Ausweises ablehnt, weil er persönlich mit dem Geschäftsführer bekannt sei.

Social

Im Rahmen von Simulationen können Mitarbeiter üben, wie sie sich bei Social-Engineering-Angriffen verhalten sollen. Dazu werden die ausgewählten Zielgruppen wie z. B. IT-Betreuer und verschiedene Administratorengruppen in einer gemeinsamen Simulation mit vermeintlich harmlosen Anfragen konfrontiert. Erst durch das fachübergreifende Betrachten dieser Anfragen wird deutlich, dass hier ein Angriff vorliegt. Ziel der Simulation ist es, diese Zusammenhänge durch entsprechende Übungen herauszufinden, um im Anschluss in definierter Art und Weise reagieren zu können. Diese Art von Simulation lässt sich in der Praxis sehr gut durch Workshops mit Moderationsmaterialien wie Pinnwand und Moderationskarten durchführen.

Simulationsübungen

Besonders wichtig sind Simulationen, in denen die Behandlung von Sicherheitsvorfällen bis hin zu Notfallsituationen geübt wird. Sie sollen Mitarbeiter in die Lage versetzen, zugeordnete Rollen und Verantwortlichkeiten innerhalb eines Szenarios auch unter erschwerten Bedingungen (Anspannung, Häufung von Anweisungen, unklare oder oft wechselnde Sachlage, Ressourcenmangel, Kommunikationsprobleme etc.) möglichst sicher wahrzunehmen. Das Ziel von Simulationen liegt primär im Training persönlicher Fähigkeiten anhand repräsentativer Szenarien, die dann in möglichst vielen Vorfallsituationen genutzt werden können. Daher sollte eine Simulation von einem erfahrenen Trainer geleitet werden, der nach ihrer Durchführung im Rahmen eines Reviews mit den Teilnehmern ihre Erfahrungen diskutiert und vertieft.

Bei der Konzeption von Sensibilisierungs- und Schulungsprogrammen ist die Lehrstoffsicherung wichtig, da nur dauerhaft präsentes Wissen auch zu den gewünschten Verhaltensänderungen führt. Nach Sensibilisierungs- und Schulungsaktivitäten sind die Teilnehmer in der Regel mit viel neuem Wissen und neuen Fertigkeiten ausgestattet. Wenn sie dieses Wissen im Anschluss an die Veranstaltungen nicht abrufen oder anwenden, besteht die Gefahr, dass sie es wieder ganz oder teilweise vergessen. Damit sich das Bewusstsein für Informationssicherheit bei den Mitarbeitern dauerhaft verbessert, sollten die Inhalte von Sensibilisierungs- und Schulungsmaßnahmen regelmäßig wiederholt bzw. angewendet werden. Dies wird durch die Lehrstoffsicherung unterstützt, die sowohl während der Schulung, am Ende einer Schulung als auch im Zeitraum danach durchgeführt werden sollte.

Die Auswahl von Maßnahmen zur Lehrstoffsicherung ist auf die jeweilige Organisationskultur und -größe abzustimmen.

Beispiele für Maßnahmen zur Lehrstoffsicherung sind:

- schriftliche oder mündliche Tests während der Schulung oder/und zum Abschluss
- Quizfragebögen mit Gewinnmöglichkeiten zu Schulungsinhalten
- Intranet-basierte Befragungen zu den Inhalten der durchgeführten Schulungen
- Nutzung von Teambesprechungen etc. für die Diskussion aktueller Aspekte der Informationssicherheit
- Durchführung von Plan- oder Rollenspielen (siehe ORP.3.M11 Durchführung von Planspielen zur Informationssicherheit)
- regelmäßige Wiederholung von Seminaren
- kurze Hinweise im Intranet
- ergänzende Kurzvorträge, z. B. im Rahmen anderer interner Veranstaltungen

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Sensibilisierung und Schulung" finden sich unter anderem in folgenden Veröffentlichungen:

[27001] ISO/IEC 27001:2013

Information technology-Security techniques-Information security management systems-Requirements, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/SC 27, Oktober 2013

[ISF] The Standard of Good Practice for Information Security:

Information Security Forum (ISF), June 2018

[NIST80053] Security and Privacy Controls for Federal Information Systems and Organizations

NIST Special Publication 800-53, Revision 4, April 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf , zuletzt abgerufen am 30.08.2018

ORP: Organisation und Personal

Umsetzungshinweise zum Baustein ORP.5 Compliance Management (Anforderungsmanagement)

1 Beschreibung

1.1 Einleitung

In jeder Institution gibt es aus den verschiedensten Richtungen gesetzliche, vertragliche, strukturelle und interne Richtlinien und Vorgaben, die beachtet werden müssen. Viele davon haben direkte oder indirekte Auswirkungen auf das Informationssicherheitsmanagement. Die Anforderungen sind je nach Branche, Land und anderen Rahmenbedingungen unterschiedlich. Weiterhin unterliegt beispielsweise eine Behörde anderen externen Regelungen als eine Aktiengesellschaft. Die Leitungsebene der Institution muss die Einhaltung der Anforderungen durch angemessene Überwachungsmaßnahmen (neudeutsch: Compliance) sicherstellen und ein Compliance Management System betreiben.

Ziel des Compliance Managements ist es, jederzeit den Überblick über die verschiedenen Anforderungen an die einzelnen Bereiche der Institution zu haben und geeignete Maßnahmen zu identifizieren und umzusetzen, um Verstöße gegen diese Anforderungen zu vermeiden.

Diese Aufgabe wird typischerweise an einen Mitarbeiter übertragen. Die Rolle wird im Folgenden mit „Compliance Manager “ bezeichnet. In einigen Unternehmen wird z. B. auch die Bezeichnung „Anforderungsmanager “ benutzt. Sofern dies nicht durch andere Regelungen vorgeschrieben ist, müssen hierfür aber keine neuen Stellen geschaffen werden. Die Aufgabe kann beispielsweise vom Sicherheitsmanagement, der Revision, dem Controlling oder dem Justiziariat mit übernommen werden.

Je nach Größe einer Institution kann diese verschiedene Managementprozesse haben, die sich mit unterschiedlichen Aspekten des Risikomanagements beschäftigen, z. B. Sicherheitsmanagement, Datenschutzmanagement, Compliance Management, Controlling. Diese sollten vertrauensvoll zusammenarbeiten, um Synergieeffekte zu nutzen und Konflikte frühzeitig auszuräumen.

1.2 Lebenszyklus

Im Rahmen des Compliance Managements ist eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über den Aufbau geeigneter Organisationsstrukturen bis hin zur regelmäßigen Revision. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Planung und Konzeption

Es sollten Prozesse und Organisationsstrukturen etabliert sein, um den Überblick über die verschiedenen Anforderungen zu gewährleisten (siehe ORP.5.A4 Konzeption und Organisation des Compliance Managements). Neben den externen Regelungen, die die Institution betreffen, müssen auch die internen Richtlinien und Anforderungen definiert und transparent sein. Eine wichtige Grundlage, um alle geschäftsrelevanten Informationen, Geschäftsprozesse und Systeme angemessen abzusichern, ist die Einstufung von deren Schutzbedarf (siehe ORP.5.A10 Klassifizierung von Informationen). In der Folge leiten sich daraus konkrete Sicherheitsvorgaben für diese Objekte ab.

Umsetzung

Die identifizierten Anforderungen werden durch die Managementprozesse der Institution, insbesondere auch durch den Sicherheitsprozess, umgesetzt. Mitarbeiter, aber auch Besucher und externe Dienstleister müssen auf ihre Sorgfaltspflichten und die einzuhaltenden Maßnahmen im Umgang mit Informationen und IT-Systemen hingewiesen werden, bevor sie Zugang oder Zugriff darauf erhalten (siehe ORP.5.A3 Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen).

Betrieb

Die Sicherheitsvorgaben, die die Institution zur Erfüllungen der Anforderungen erstellt hat, müssen dauerhaft eingehalten werden. Dies sollte regelmäßig überprüft werden (siehe ORP.5.A7 Aufrechterhaltung der Informationssicherheit). Sowohl die eigenen Regelungen als auch die rechtlichen Rahmenbedingungen, denen eine Institution unterliegt, können sich ändern. Dies muss im Rahmen des Compliance Managements berücksichtigt werden (siehe ORP.5.A2 Beachtung rechtlicher Rahmenbedingungen).

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Compliance Management (Anforderungsmanagement)" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

ORP.5.M1 Identifikation der rechtlichen Rahmenbedingungen [Institutionsleitung, Leiter Organisation]

Bei der Verarbeitung von Informationen sind eine Vielzahl von gesetzlichen oder vertraglichen Rahmenbedingungen zu beachten. Diese variieren sehr stark in Abhängigkeit von der Art der Institution, der Branche und den Geschäftsprozessen.

Typische Bereiche der Informationsverarbeitung, die besonderen gesetzlichen Regelungen unterliegen, sind:

- Schutz personenbezogener Daten,
- Einsatz von kryptographischen Verfahren,
- Schutz von geistigem Eigentum,
- ordnungsgemäßer Betrieb von IT-Systemen, inklusive Überwachung, Protokollierung und Auswertung,
- Langzeitspeicherung von Daten.

Abhängig von dem Land, in dem die Informationen verarbeitet werden und ihrem speziellen Einsatzzweck können noch eine Vielzahl von weiteren rechtlichen Regelungen existieren. Diese einzeln zu nennen, würde den Rahmen dieses Dokumentes sprengen. In diversen Bereichen des IT-Grundschutzes werden länder- oder branchenspezifische Gesetze angesprochen, wie z. B. zu Kryptographie, Outsourcing oder Archivierung. Dies sind aufgrund der Vielzahl möglicher gesetzlicher Rahmenbedingungen jeweils nur Beispiele ohne Anspruch auf Vollständigkeit oder Aktualität.

Übersicht über rechtliche Rahmenbedingungen

Alle für die Geschäftsprozesse und Informationsverarbeitung, den Betrieb von IT-Systemen und der zugehörigen physischen Infrastruktur zu beachtenden gesetzlichen, vertraglichen und sonstigen Vorgaben müssen identifiziert und dokumentiert werden. Es ist dabei zu beachten, dass gesetzliche Vorschriften sich häufig ebenfalls auf Landes- und Regionalebene unterscheiden. Als Konsequenz müssen unter Umständen für jede Lokation jeweils die dort gültigen Gesetze eingehalten werden. Ebenso ist zu berücksichtigen, dass je nach Art der Geschäftsprozesse und dem Einsatzzweck der IT-Systeme (z. B. Büroumgebung, Prozesssteuerung) verschiedene Vorschriften gelten können.

Insbesondere müssen

- alle angewandten betrieblichen Praktiken und Vorgehensweisen,
- alle im Rahmen der geschäftlichen Tätigkeiten verarbeiteten Informationen,
- alle installierten IT-Systeme (Hardware- und Software) sowie
- die zum Betrieb der Geschäftsprozesse und IT-Systeme notwendige physikalische Infrastruktur

die gültigen gesetzlichen Vorschriften erfüllen. Alle Änderungen gesetzlicher Auflagen müssen erfasst und die für die Institution relevante Änderungen berücksichtigt werden.

Typischerweise gibt es in den verschiedenen Bereichen einer Institution Übersichten über die Anforderungen, die in diesen Bereichen und für deren Geschäftsprozesse relevant sind. Nicht immer sind dies formalisierte Übersichten, sondern oftmals Einzelinformationen in verschiedenen Strukturen und Wissen in den Köpfen von Experten. Durch die Komplexität vieler Geschäftsprozesse und Organisationsstrukturen sowie durch eine zunehmende Vielfalt an Vorgaben aus der internationalen Zusammenarbeit können sich hierbei schnell eine große Anzahl verschiedener Anforderungen ergeben. Deswegen sollte das vorhandene Wissen über die verschiedenen gesetzlichen, vertraglichen und sonstigen Vorgaben zentral zusammengetragen und, wenn nötig, ergänzt werden.

ORP.5.M2 Beachtung rechtlicher Rahmenbedingungen [Institutionsleitung, Leiter Organisation, Vorgesetzte]

Führungskräfte, welche die rechtliche Verantwortung für die Institution vor Ort tragen, müssen für die Identifizierung und Dokumentation der anzuwendenden gesetzlichen Vorschriften sorgen. Idealerweise sollte ein Jurist oder Rechtsexperte beauftragt werden. Falls innerhalb der Institution das erforderliche Wissen oder die nötigen Ressourcen nicht zur Verfügung stehen, sollte externe Rechtsberatung eingeholt werden. Da nicht alle Mitarbeiter sämtliche Gesetze und Regelungen kennen müssen, sollten dabei die für die einzelnen Bereiche der Institution relevanten gesetzlichen und vertraglichen Vorgaben herausgearbeitet werden. Um deren Einhaltung zu überwachen, können in den einzelnen Bereichen Verantwortliche benannt werden. So ist der betriebliche Datenschutzbeauftragte dafür verantwortlich, auf die Einhaltung der gültigen Datenschutzvorschriften sowie für die Erstellung und Einhaltung eines institutionsweit gültigen Regelwerks zum Schutz personenbezogener Daten hinzuwirken. Die IT-Leitung muss dagegen z. B. für die Definition und Dokumentation des Lizenzmanagements sorgen.

Natürlich ist auch jeder einzelne Mitarbeiter und insbesondere das Führungspersonal für die Umsetzung der Regelungen zu rechtlichen Aspekten und für die Überwachung der Einhaltung in seinem Arbeitsumfeld verantwortlich (siehe ORP.5.M3 Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen).

ORP.5.M3 Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen [Personalabteilung, Vorgesetzte]

Mitarbeiter müssen verpflichtet werden, einschlägige Gesetze (z. B. zum Datenschutz), Vorschriften und interne Regelungen einzuhalten. Bereits bei der Einstellung sollten neue Mitarbeiter mit den bestehenden Vorschriften und Regelungen rund um das Thema der Informationssicherheit bekannt gemacht und gleichzeitig zu deren Einhaltung motiviert werden. Dabei ist es sinnvoll, nicht nur die Verpflichtung durchzuführen, sondern auch die erforderlichen Exemplare der Vorschriften und Regelungen auszuhändigen und den Empfang quittieren zu lassen bzw. für die Mitarbeiter an zentraler Stelle zur ständigen Einsichtnahme vorzuhalten. Auf neue Gesetze und Regelungen sowie deren Änderungen sollte geeignet hingewiesen werden, z. B. über das Intranet. Falls erforderlich, muss die Einweisung nach einer Aktualisierung von wesentlichen Vorgaben erneut durchgeführt werden. Um das richtige Verhalten in Bezug auf die einschlägigen Vorgaben nachhaltig zu verankern, ist es sinnvoll, hierzu regelmäßig geeignete Schulungsmaßnahmen anzubieten.

Die Verpflichtung sollte geeignet zentral dokumentiert werden. So ist z.B. eine Ablage von Verpflichtungserklärungen in der Personalakte einer Ablage bei den einzelnen Verantwortlichen, z. B. dem Datenschutzbeauftragten, vorzuziehen.

Alle Mitarbeiter müssen darauf hingewiesen werden, dass alle Arbeitsergebnisse und alle während der Arbeit erhaltenen Informationen ausschließlich zum internen und dienstlichen Gebrauch bestimmt sind. Außerdem sollten die Mitarbeiter dafür sensibilisiert werden, dass sie vor der Weitergabe personenbezogener oder vertraulicher Informationen prüfen, ob diese zulässig ist. Dies gilt ebenso für Daten, die lizenz- oder urheberrechtlich geschützt sind.

Gemeinsam mit den Basismaßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich Compliance Management.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Compliance Management (Anforderungsmanagement)".

ORP.5.M4 Konzeption und Organisation des Compliance Managements [Institutionsleitung]

Typischerweise ergeben sich aus den verschiedenen Tätigkeiten einer Institution eine Vielzahl verschiedener gesetzlicher, vertraglicher und anderer rechtlicher Vorgaben. Die Identifikation dieser Anforderungen und der Umgang mit diesen kann schnell sehr komplex werden. Dafür sollten Verantwortliche benannt und deren Aufgaben im Bereich Compliance Management festgelegt werden. Die entsprechende Rolle wird häufig als "Compliance Manager" bezeichnet. Je nach Art und Größe der Institution kann es sinnvoll sein, einen oder mehrere Compliance Manager zu benennen.

In einigen Unternehmen wird auch die Bezeichnung "Anforderungsmanager" benutzt.Sofern dies nicht durch andere Regelungen vorgeschrieben ist, muss hierfür aber keine neue Stelle geschaffen werden. Die Aufgabe kann beispielsweise vom Sicherheitsmanagement, der Revision, dem Controlling oder dem Justiziariat mit übernommen werden.

Die Benennung eines zentralen Compliance Manager hat den Vorteil, dass dieser einen Überblick über die gesamte Institution hat, wodurch Doppelarbeiten und Konflikte frühzeitig erkannt und vermieden werden können. Mehrere Compliance Manager in den verschiedenen Bereichen einer Institution können andererseits meist besser die Bedürfnisse der von ihnen betreuten Zielgruppe abdecken. Im Folgenden wird der besseren Lesbarkeit wegen immer im Singular auf die Rolle des Compliance Managers Bezug genommen.

Zu den Aufgaben eines Compliance Managers (für die von ihm betreuten Bereiche) gehören:

- Alle für die wesentlichen Geschäftsprozesse und Informationen sowie für den Betrieb von IT-Systemen und der zugehörigen physischen Infrastruktur zu beachtenden gesetzlichen, vertraglichen und sonstigen Vorgaben müssen identifiziert und dokumentiert werden (siehe ORP.5.M1 Identifikation der rechtlichen Rahmenbedingungen).
- Die Anforderungen sind strukturiert zu erfassen und aus den verschiedenen Bereichen zusammenzuführen und zu konsolidieren.
- Um die einzelnen identifizierten Anforderungen zu erfüllen und angemessene Maßnahmen umzusetzen, müssen Verantwortliche benannt werden. Der Compliance Manager sollte regelmäßig überprüfen, ob die ergriffenen Maßnahmen geeignet sind, um die Anforderungen abzudecken.
- Häufig müssen Anforderungen auch zunächst interpretiert und auf die Gegebenheiten der jeweiligen Institution übersetzt werden, da die meisten Gesetze und Vorgaben eher Ziele und Erwartungen formulieren, nicht aber wie deren Umsetzung konkret auszugestalten ist.
- Alle Arten der genannten Anforderungen gehen auch jeweils auf eine bestimmte Zielgruppe zurück, die deren Einhaltung fordert oder prüft. Bei der Identifikation der Anforderungen sollte auch immer die Zielgruppe dokumentiert werden, um deren Bedürfnisse zu erfüllen. Dies erspart später viele Anpassungsarbeiten. Bei gesetzlichen Anforderungen ist es z. B. sinnvoll, festzuhalten, welche Instanz (also z. B. welche Aufsichtsstelle) deren Einhaltung prüft und in welcher Form hierfür die Informationen aufbereitet werden müssen.

In der folgenden Tabelle finden sich hierzu einige Beispiele:

Anforderungen	**Zielgruppe**	**Verantwortlicher Compliance Manager**
Datenschutz-Gesetze	Datenschutz-Aufsicht	Behördlicher oder betrieblicher Datenschutzbeauftragter
Arbeitsrecht	Personalvertretung	Personalreferat
Strafrecht	Strafverfolgungsbehörden	Justiziariat / Hausjurist
Verträge	DienstleisterKunden	EinkaufVertrieb
Sonstige Anforderungen	Kooperationspartner	Fachabteilung

Tabelle: Zuordnung von Anforderungen zu Zielgruppen und Compliance Manager

Zusammenarbeit mit Sicherheitsmanagement

Die Informationssicherheit ist direkt oder indirekt ein zu beachtender Aspekt in fast allen Anforderungsbereichen. Dabei ist der Informationssicherheitsbeauftragte nur in wenigen Fällen der Compliance Manager. Compliance Manager und Informationssicherheitsbeauftragter müssen daher regelmäßig zusammenarbeiten, um einerseits die Sicherheitsanforderungen aus den verschiedenen Bereichen ins Compliance Management zu integrieren und andererseits die als sicherheitsrelevant identifizierten Anforderungen in Sicherheitsmaßnahmen zu überführen und deren Umsetzung zu kontrollieren.

Sicherheitsanforderungen ergeben sich in erster Linie durch die Auslegung allgemeiner Rechtsvorschriften, teilweise aus Spezialgesetzen sowie aus tätigkeits- oder branchenbezogenen Vorschriften, die die Sicherheit bestimmter Systeme, Dienstleistungen oder Tätigkeiten regeln. Dazu kommen zivilrechtliche Pflichten, deren (schuldhafte) Verletzung zu Haftung des Verantwortlichen führen kann. Beispiele sind

- Datenschutzgesetze
- KWG, KonTraG, MaRisk der BaFin
- Urheberrechtsgesetz
- TKG, TMG
- ITSiG
- Verträge, Allgemeine Geschäftsbedingungen, etc.
- Lizenzmanagement

Die als sicherheitsrelevant identifizierten Anforderungen sollten bei der Planung und Konzeption von Geschäftsprozessen, Anwendungen und IT-Systemen oder bei der Beschaffung neuer Komponenten einfließen.

ORP.5.M5 Ausnahmegenehmigungen [Informationssicherheitsbeauftragter (ISB), Vorgesetzte]

In Einzelfällen kann es sinnvoll und notwendig sein, Ausnahmen von den in einer Sicherheitsrichtlinie getroffenen Regelungen zuzulassen. Ausnahmen sollten zwar möglichst vermieden werden, es ist aber auf jeden Fall besser, eine Ausnahme zuzulassen, als unnachgiebig auf Vorgaben zu bestehen, die im konkreten Einzelfall nicht einzuhalten sind. Sollten sich Ausnahmen häufen, ist dies ein Zeichen dafür, dass die vorhandenen Sicherheitsvorgaben überdacht und eventuell angepasst werden müssen.

Ausnahmen müssen aber in jedem Fall durch eine autorisierte Stelle genehmigt werden. Bei dem Genehmigungsverfahren sind sowohl Fachverantwortliche als die "Eigentümer" von Informationen und Anwendungen, als auch das Sicherheitsmanagement zu beteiligen. Für alle Ausnahmefälle muss gründlich überprüft werden, ob diese essentielle Sicherheitsvorgaben nicht untergraben. Dafür ist eine Risikobewertung vorzunehmen. Ausnahmen dürfen nur genehmigt werden, wenn dass ermittelte Risiko als tragbar eingestuft wurde.

Ausnahmegenehmigungen sollten zeitlich klar befristet werden. Es muss regelmäßig überprüft werden (spätestens alle 12 Monate), ob die Ausnahmegenehmigungen noch erforderlich sind und ob zeitlich befristete Ausnahmegenehmigungen wieder aufgehoben oder nach Ablauf verlängert wurden.

Anschließend muss eine schriftliche Begründung verfasst werden, die von den Verantwortlichen zu unterzeichnen ist.

Für die Erteilung von Ausnahmegenehmigungen sollte ein dokumentiertes Verfahren existieren. Es sollte mindestens folgendes dokumentiert werden:

- Begründung, warum eine Abweichung von den Sicherheitsvorgaben erforderlich ist und welche Regelung betroffen ist,
- Beschreibung der Ausgestaltung der Ausnahmegenehmigungen sowie Darstellung der Auswirkungen und Abgrenzung des betroffenen Bereichs, inklusive der Risikobewertung,
- Zeitpunkt der Einrichtung,
- Antragsteller und Genehmigender,
- Zeitraum der Befristungen.

Über genehmigte Abweichungen von den geltenden Sicherheitsvorgaben sind alle betroffenen Mitarbeiter zu informieren.

ORP.5.M6 Einweisung des Personals in den sicheren Umgang mit IT [Personalabteilung, Vorgesetzte]

Viele Sicherheitsprobleme entstehen durch fehlerhafte Benutzung bzw. Konfiguration der IT. Um solchen Problemen vorzubeugen, sind alle Mitarbeiter und alle externen IT-Benutzer in den sicheren Umgang mit der IT der Institution einzuweisen. Hierzu müssen alle Mitarbeiter entsprechend sensibilisiert und geschult werden (siehe auch ORP.3 Sensibilisierung und Schulung zur Informationssicherheit).

Allen Mitarbeitern muss deutlich gemacht werden, welche Rechte und Pflichten sie bei der IT-Nutzung haben. Ihnen sollten spezifische Richtlinien an die Hand gegeben werden, was sie im Umgang mit der IT beachten müssen. In einer solchen Richtlinie ist zu beschreiben, welche Randbedingungen es beim Einsatz der betrachteten IT-Systeme gibt, welche Sicherheitsmaßnahmen zu ergreifen sind und welche Meldewege oder Ansprechpartner es bei Verlust, Sicherheitsvorfällen oder Unklarheiten gibt. Diese Richtlinien sollten verbindlich, verständlich, aktuell und verfügbar sein. Um die Verbindlichkeit zu dokumentieren, sollten sie von der Behörden- bzw. Unternehmensleitung oder zumindest vom IT-Verantwortlichen unterzeichnet sein. Es empfiehlt sich auch, sie kurz und verständlich zu formulieren, sodass sie beispielsweise als Poster, Merkzettel, Flyer, Karteikarte oder Ähnliches verteilt werden können. Zusätzlich sollten sie im Intranet abrufbar sein.

Benutzerrichtlinien sollten grundsätzlich nur Regelungen enthalten, die auch umgesetzt werden können, und so positiv wie möglich formuliert werden. Beispielsweise könnte eine Benutzerrichtlinie statt

"Benutzer dürfen keine Software selbständig installieren."

so lauten:

"Alle IT-Systeme werden in einer Standardkonfiguration ausgeliefert, die auf Ihre spezifischen Arbeitsbedingungen angepasst wurde und Ihnen maximale Sicherheit bietet. Bei Problemfällen können wir Ihnen durch eine Neuinstallation der Standardkonfiguration eine schnelle Problemlösung garantieren. Bitte verändern Sie daher die Einstellungen möglichst nicht. Wenn Sie zusätzliche Hard- oder Software benötigen, wenden Sie sich bitte an den Benutzerservice."

Weitere Beispiele für Benutzerrichtlinien finden sich unter den Hilfsmitteln zum IT-Grundschutz.

Eine Benutzerrichtlinie für die allgemeine IT-Nutzung sollte mindestens die folgenden Punkte umfassen:

- Hinweis, dass IT-Systeme oder IT-Komponenten nur mit ausdrücklicher Erlaubnis benutzt werden dürfen
- Hinweis, dass nur diejenigen Mitarbeiter Informationen auf IT-Systemen ändern dürfen, die dazu autorisiert sind
- Umgang mit Passwörtern
- Nutzungsverbot nicht freigegebener Software
- Hinweis, dass dienstliche IT-Systeme nur für dienstliche Zwecke eingesetzt werden dürfen, beziehungsweise eine präzise Beschreibung möglicher Ausnahmen von dieser Regel, falls es sie gibt,
- Hinweise zur sicheren Verwahrung und Aufstellung von IT-Systemen und Datenträgern
- Hinweise zur sicheren mobilen Nutzung von IT
- Schutz vor Computer-Viren und anderer Schadsoftware
- Durchführung von Datensicherungen bzw. der zentralen Ablage von Daten
- Nutzung von Internet-Diensten
- Hinweis auf Verantwortliche und Ansprechpartner zu Themen die IT und Informationssicherheit betreffend
- Neben solchen Richtlinien müssen klare Aussagen darüber vorliegen, welche Benutzer auf welche Informationen zugreifen dürfen, an wen diese weitergegeben werden dürfen und welche Maßnahmen bei einem Verstoß gegen diese Richtlinien unternommen werden.

Wenn ein Benutzer seinen Arbeitsplatz verlässt, sollte er sich davon überzeugen, dass jedes Arbeitsmittel (Dokumente, Datenträger, etc.) sicher verwahrt ist. Alle IT-Systeme sollten durch Passwörter gegen unbefugten Zugriff geschützt sein. Bei unbeaufsichtigten IT-Systemen ist der Computer mindestens zu sperren.

Die Grundkonfiguration aller IT-Systeme sollte möglichst eingeschränkt sein. In der Standardkonfiguration von Arbeitsplatzrechnern sollten nur die Dienste vorhanden sein, die von allen Benutzern einer Gruppe benötigt werden. Weitere Programme oder Funktionen dürfen nur dann aufgespielt bzw. freigeschaltet werden, wenn die Benutzer in deren Handhabung eingewiesen und für eventuelle Sicherheitsprobleme sensibilisiert wurden.

Jede Benutzerordnung sollte in Zusammenarbeit mit Vertretern aller beteiligten Gruppen erstellt werden, insbesondere sind Personalvertretungen und Datenschutz- sowie Informationssicherheitsbeauftragte rechtzeitig zu beteiligen. Bei jeder Änderung einer Benutzerordnung ist darauf zu achten, dass die Betroffenen wieder im Vorfeld beteiligt werden. Die geänderte Benutzerordnung muss allen Benutzern bekannt gegeben werden.

Die Aufgabenbeschreibung sollte alle für die Informationssicherheit relevanten Aufgaben und Verpflichtungen enthalten. Dazu gehört u. a. die Verpflichtung auf die hausinternen Leitlinien zur Informationssicherheit.

Werden IT-Systeme oder Dienste in einer Weise benutzt, die den Interessen der Behörde bzw. des Unternehmens widersprechen, sollte jeder, der davon Kenntnis erhält, dies seinen Vorgesetzten mitteilen.

Beispiele für Benutzerrichtlinien finden sich unter den Hilfsmitteln zum IT-Grundschutz [GSH].

ORP.5.M7 Aufrechterhaltung der Informationssicherheit [Informationssicherheitsbeauftragter (ISB)]

Im Sicherheitsprozess geht es nicht nur darum, das angestrebte Sicherheitsniveau zu erreichen, sondern dieses auch dauerhaft zu gewährleisten. Um das bestehende Sicherheitsniveau aufrechtzuerhalten und fortlaufend zu verbessern, sollten alle Sicherheitsmaßnahmen regelmäßig überprüft werden.

Sowohl die korrekte Umsetzung als auch die Umsetzbarkeit eines Sicherheitskonzepts müssen regelmäßig überprüft werden. Dabei ist zu unterscheiden zwischen der Prüfung, ob bestimmte Maßnahmen geeignet und effizient sind, um die gesteckten Sicherheitsziele zu erreichen (Vollständigkeits- bzw. Aktualisierungsprüfung), und der Kontrolle, inwieweit Sicherheitsmaßnahmen in den einzelnen Bereichen umgesetzt wurden (Revision der Informationssicherheit).

Die im Sicherheitskonzept geplanten Sicherheitsmaßnahmen müssen gemäß des Realisierungsplans umgesetzt werden. Der Umsetzungsstatus muss dokumentiert werden. Zieltermine und Ressourceneinsatz müssen überwacht und gesteuert werden. Die Leitungsebene ist dazu regelmäßig zu informieren.

Diese Überprüfungen sollten zu festgelegten Zeitpunkten (mindestens jährlich) durchgeführt werden und können auch zwischendurch erfolgen. Insbesondere Erkenntnisse aus sicherheitsrelevanten Zwischenfällen, Veränderungen im technischen oder technisch-organisatorischen Umfeld sowie Änderungen von Sicherheitsanforderungen Bedrohungen erfordern eine Anpassung der bestehenden Sicherheitsmaßnahmen. Die in den einzelnen Überprüfungen ermittelten Ergebnisse sollten dokumentiert werden. Es muss zudem festgelegt sein, wie mit den Überprüfungsergebnissen zu verfahren ist, da die Informationssicherheit nur dann wirksam aufrechterhalten werden kann, wenn aufgrund der Überprüfungsergebnisse auch die erforderlichen Korrekturmaßnahmen ergriffen werden.

Es sollten auch gelegentlich unangekündigte Überprüfungen durchgeführt werden, da angekündigte Kontrollen häufig ein verzerrtes Bild des Untersuchungsgegenstands ergeben.

Kontrollen sollten vor allen Dingen darauf ausgerichtet sein, Mängel abzustellen. Für die Akzeptanz ist es wichtig, dass dies allen Beteiligten als Ziel der Kontrollen erkennbar ist und dass die Kontrollen nicht den Charakter von Schulmeisterei haben. Es ist daher sinnvoll, während einer Kontrolle mit den Beteiligten über mögliche Problemlösungen zu sprechen und entsprechende Abhilfen vorzubereiten.

Es sollte in der Behörde oder im Unternehmen festgelegt werden, wie die Tätigkeiten im Zusammenhang mit diesen Überprüfungen zu koordinieren sind. Dazu ist zu regeln, welche Sicherheitsmaßnahmen wann und von wem zu überprüfen sind, auch damit Doppelarbeit vermieden wird und keine Bereiche innerhalb einer Institution ungeprüft verbleiben.

Die vorhandenen Sicherheitsmaßnahmen sollten mindestens einmal im Jahr überprüft werden. Darüber hinaus sind sie immer dann zu prüfen, wenn

- neue Geschäftsprozesse, Anwendungen oder IT-Komponenten aufgebaut werden,
- größere Änderungen der Infrastruktur vorgenommen werden (z. B. Umzug),
- größere organisatorischen Änderungen anstehen (z. B. Outsourcing),
- die Gefährdungslage sich wesentlich ändert,
- wenn gravierende Schwachstellen oder Schadensfälle bekannt werden.

Einhaltung des Sicherheitskonzeptes (Sicherheitsrevision)

Hierbei muss geprüft werden, ob Sicherheitsmaßnahmen tatsächlich so umgesetzt sind und eingehalten werden wie im Sicherheitskonzept vorgegeben. Hierbei ist auch zu untersuchen, ob technische Maßnahmen korrekt implementiert und konfiguriert wurden und ob alle vorgesehenen Detektionsmaßnahmen (z. B. Auswertung von Protokolldateien) tatsächlich durchgeführt werden.

Dabei kann sich zeigen, dass Sicherheitsmaßnahmen nicht umgesetzt worden sind oder dass sie in der Praxis nicht greifen. In beiden Fällen sollten die Ursachen für die Abweichungen ermittelt werden. Als mögliche Korrekturmaßnahmen kommen - je nach Ursache - in Frage:

- organisatorische Maßnahmen sind anzupassen,
- personelle Maßnahmen, z. B. Schulungs- und Sensibilisierungsmaßnahmen, sind zu ergreifen oder disziplinarische Maßnahmen einzuleiten,
- infrastrukturelle Maßnahmen, z. B. bauliche Veränderungen, sind zu initiieren,
- technische Maßnahmen, z. B. Änderungen an Hardware und Software oder Kommunikationsverbindungen und Netzen, sind vorzunehmen,
- Entscheidungen des verantwortlichen Vorgesetzten (bis hin zur Leitungsebene) sind einzuholen.

Auf jeden Fall sollte für jede Abweichung eine Maßnahmenbehandlung vorgeschlagen werden. Außerdem sollten auch hier der Zeitpunkt und die Zuständigkeiten für die Umsetzung der Korrekturmaßnahme festgelegt werden.

Kontrollen sollen helfen, Fehlerquellen abzustellen. Es ist für die Akzeptanz von Kontrollen extrem wichtig, dass dabei keine Personen bloßgestellt werden oder als "Schuldige" identifiziert werden. Wenn die Mitarbeiter dies befürchten müssen, besteht die Gefahr, dass sie nicht offen über ihnen bekannte Schwachstellen und Sicherheitslücken berichten, sondern versuchen, bestehende Probleme zu vertuschen.

Im Vorfeld sollten aber auch die Reaktionen auf Verletzung der Sicherheitsvorgaben festgelegt werden. Es müssen angemessene Maßnahmen ergriffen werden, die dazu beitragen, dass sich Sicherheitsvorfälle nicht wiederholen. Dazu könnte beispielsweise die Einschränkung von Zugriffsrechten gehören.

Falls unzulässige Aktivitäten von Mitarbeitern entdeckt werden, sollte der jeweilige Vorgesetzte informiert werden, damit angemessene Konsequenzen angestoßen werden können.

Kontinuierliche Verbesserung des Sicherheitskonzeptes (Vollständigkeits- bzw. Aktualisierungsprüfung)

Das Sicherheitskonzept muss regelmäßig aktualisiert, verbessert und an neue Rahmenbedingungen angepasst werden. Es muss regelmäßig geprüft werden, ob die ausgewählten Sicherheitsmaßnahmen noch geeignet sind, die Sicherheitsziele zu erreichen. Dabei kann direkt untersucht werden, ob die eingesetzten Sicherheitsmaßnahmen effizient sind oder ob die Sicherheitsziele mit anderen Maßnahmen ressourcenschonender erreicht werden könnten.

Deshalb ist es wichtig, externe Wissensquellen, wie Standards oder Fachpublikationen, im Hinblick auf neue technische und regulatorische Entwicklungen auszuwerten. Auch Kontakte zu Gremien und Interessengruppen, die sich mit Sicherheitsaspekten beschäftigen, helfen dem IS-Management-Team, das vorhandene Wissen über sicherheitsrelevante Methoden und Lösungen zu erweitern und zu aktualisieren. Außerdem werden dabei auch wertvolle Kontakte zu anderen Informationssicherheitsbeauftragten geknüpft, um Lösungen anderer Institutionen kennenzulernen und Praxiserfahrungen auszutauschen. Es entstehen dadurch auch Wege, über die frühzeitig Warnungen über aufkommende Sicherheitsprobleme ausgetauscht werden können. Das IS-Management-Team sollte einen Überblick über thematisch passende Gremien und Interessengruppen haben und festlegen, wo sich aktive Mitarbeit anbietet und wo nur die Ergebnisse regelmäßig beobachtet und ausgewertet werden sollten.

Durchführung der Prüfungen

Entsprechend dem Prüfungszweck sind Umfang und Tiefe der Überprüfungen festzulegen. Als Grundlage für alle Überprüfungen dient das Sicherheitskonzept und die vorhandene Dokumentation des Sicherheitsprozesses.

Eine Überprüfung muss von Personen mit geeigneten Qualifikationen durchgeführt werden. Diese dürfen idealerweise jedoch nicht an der Erstellung der Konzepte beteiligt gewesen sein, um Betriebsblindheit und Konflikte zu vermeiden. Die Auditoren müssen möglichst unabhängig und neutral sein.

Jede Überprüfung ist sorgfältig zu planen. Alle relevanten Feststellungen und Ergebnisse sind in einem Bericht festzuhalten. Dieser sollte neben einer Auswertung auch Korrekturvorschläge enthalten. Der Bericht sollte dem Leiter des überprüften Bereiches sowie dem IS-Management-Team übergeben werden, die auf dieser Basis die weiteren Schritte konzipieren müssen. Schwerwiegende Probleme sollten direkt der Leitungsebene kommuniziert werden, damit weitreichende Entscheidungen zeitnah getroffen werden können.

Werden bei der Prüfung spezielle Audit- oder Diagnosewerkzeuge eingesetzt, muss ebenso wie bei der Ergebnisdokumentation sichergestellt sein, dass nur autorisierte Personen darauf Zugriff haben. Diagnose- und Prüftools sowie die Prüfergebnisse müssen daher besonders geschützt werden.

Wenn Externe an Prüfungen beteiligt sind, muss sichergestellt werden, dass keine Informationen der Institution missbräuchlich verwenden (z. B. durch entsprechende Vertraulichkeitsvereinbarungen) und dass sie nur auf die benötigten Informationen zugreifen können (z. B. durch Zugriffsrechte oder Vier-Augen-Kontrolle). Sollten sie Prüftools einsetzen, muss deren Nutzung genau geregelt werden.

Korrekturmaßnahmen

Erkannte Fehler und Schwachstellen müssen zeitnah abgestellt werden. Der identifizierte Optimierungsbedarf bei Effizienz und Effektivität von Sicherheitsmaßnahmen muss umgesetzt werden.

Aufgrund der Überprüfungsergebnisse sind Entscheidungen über das weitere Vorgehen zu treffen. Insbesondere sind alle erforderlichen Korrekturmaßnahmen in einem Umsetzungsplan festzuhalten. Die Verantwortlichen für die Umsetzung der Korrekturmaßnahmen sind zu benennen und mit den notwendigen Ressourcen auszustatten. Dabei ist in der Regel die Einbindung der Leitungsebene erforderlich.

ORP.5.M8 Regelmäßige Überprüfungen des Compliance Managements

Ebenso wie die Prozesse des Sicherheitsmanagements sollte auch das Compliance Management und die sich aus diesem ergebenden Anforderungen und Maßnahmen regelmäßig auf Effizienz und Effektivität überprüft werden (siehe auch DER.1.3 Audits und Revisionen). Es sollte regelmäßig geprüft werden, ob die Organisationsstruktur und die Prozesse des Compliance Managements noch angemessen sind.

In diesem Rahmen sollte auch überprüft werden, ob die in den verschiedenen Bereichen der Institution vorhandenen Geschäftsprozesse einerseits den rechtlichen Vorgaben und andererseits den Sicherheitsanforderungen genügen.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

ORP.5.M9 Schutz gegen nachträgliche Veränderungen von Informationen [Benutzer, Informationssicherheitsbeauftragter (ISB)] (I)

Dateien, die an Dritte weitergegeben werden, können von diesen im Allgemeinen auch weiterbearbeitet werden. Dies ist nicht immer im Sinne des Erstellers. Daher sollten Daten gegen nachträgliche Veränderungen, auszugsweise Weitergabe oder Verarbeitung geschützt werden.

Häufig steht man vor dem Problem, dass Informationen über das Internet oder andere Netze Dritten zwar zur Verfügung gestellt, aber nicht hundertfach ausgedruckt oder nahtlos in andere Werke integriert werden sollen.

Hierzu gibt es verschiedene Lösungen, die teilweise auch miteinander kombiniert werden können. Beispiele hierfür sind:

- Die Verwendung von digitalen Signaturen, um unbemerkte Änderungen an Dateien zu verhindern (siehe auch CON.1 Kryptokonzept).
- Das Hinzufügen von Urheberrechts-Vermerken zu Informationen, wie Broschüren oder Dateien auf Webseiten. Diese können wie folgt lauten: "Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der Bestimmungen des Urheberrechtsgesetzes ohne Zustimmung des Autors ist unzulässig und strafbar." sowie "Copyright (©) 7/2016 by BSI".
- Die Verwendung von Dateiformaten, die nachträgliche Änderungen bzw. auszugsweise Weiterverarbeitung erschweren. Hierfür kann z. B. Postscript genutzt werden oder die Sicherheitseigenschaften von Anwendungsprogrammen, z. B. bei PDF-Dateien.

Viele Anwendungsprogramme bieten Sicherheitsmechanismen an, um den weiteren Umgang mit den erstellten Dateien einzuschränken. Im Folgenden werden einige solcher Sicherheitsmechanismen am Beispiel von PDF-Dateien vorgestellt. Da die Sicherheitsmechanismen der verschiedenen Anwendungsprogramme sehr unterschiedlich ausgeprägt sind und teilweise sogar von Version zu Version variieren, ist es wichtig, die Mitarbeiter darüber zu informieren, wie diese zu benutzen sind und welche Schritte vor der Weitergabe von elektronischen Dokumenten zu beachten sind. Es ist häufig sinnvoll, einen Mitarbeiter (plus Vertreter) gründlich hierzu auszubilden. Dieser sollte dann alle weiterzugebenden Dokumente entsprechend der Sicherheitsvorgaben bearbeiten oder als Ansprechpartner zur Verfügung stehen.

Schutz von PDF-Dokumenten

PDF-Dokumente können bei der Erstellung mit Zugriffsbeschränkungen versehen werden. So kann z. B. das Öffnen, Drucken oder Kopieren von PDF-Dateien eingeschränkt werden.

- Häufig sollen in einem Dokument vor dessen Veröffentlichung einzelne Passagen unkenntlich gemacht werden. Eine beliebte, aber extrem fehlerträchtige Methode ist es, Textpassagen elektronisch zu "schwärzen".
  Die so übermalten Informationen sind allerdings in vielen Fällen einfach auslesbar. Daher ist dies unbedingt zu unterlassen.

- Durch die Verwendung von kryptographischen Verfahren können PDF-Dokumente signiert oder so verschlüsselt werden, dass nur bestimmte Anwender diese benutzen können.
- Es können PDF-Sicherheitsrichtlinien erstellt werden. Diese kann jeder Benutzer für sich erstellen oder es können von der Institution vorgegebene Sicherheitsrichtlinien verwendet werden, hierfür ist ein Adobe Policy Server erforderlich.
- Dateischutz
  Mit Adobe Acrobat, also der verbreitetsten Anwendung, mit der PDF-Dateien erstellt und nachbearbeitet werden können, ist die Vergabe von zwei Arten von Passwörtern möglich. Die einen werden zum Öffnen des Dokuments, die anderen zum Ändern der Sicherheitsattribute benötigt. Bei der Vergabe eines Passwortes wird zunächst danach gefragt, zu welchen Programmversionen die Schutzfunktion kompatibel sein soll. Bis zur Version "Adobe 5.0 und höher" ist dabei nur eine 40-Bit-Verschlüsselung mit RC4 möglich, ab "Adobe 5.0 und höher" ist eine 128-Bit-Verschlüsselung mit RC4 und ab "Adobe 7.0 und höher" ist eine 128-Bit-Verschlüsselung mit vorgesehen. Es sollte darauf geachtet werden, mindestens mit 128 Bit zu verschlüsseln, da der Dokumentenschutz sonst einfach ausgehebelt werden kann.
  Über die Sicherheitsattribute können unter anderem folgende Funktionen eingeschränkt werden:
  - Öffnen des Dokuments
  - Drucken
  - Ändern des Dokuments
  - Kopieren von Texten, Bildern oder anderen Inhalte
  - Zugriff auf Metadaten eines Dokuments
  - Notizen und Formularfelder hinzufügen oder ändern

  So können sehr einfach die Rechte beschränkt werden, so dass niemand mit Cut and Paste die Inhalte einer Veröffentlichung übernehmen kann. Wenn im Extremfall sogar das Ausdrucken verhindert wird, kann die Datei nur online gelesen werden.

Es sollte genau überlegt werden, welche Metadaten die Datei enthalten soll. Hier kann es beispielsweise erwünscht sein, einer Datei eine Vielzahl von Metadaten mitzugeben, damit dieses über Suchmaschinen gefunden werden kann. Es kann aber auch sinnvoll sein, keine Metadaten weiterzugeben, beispielsweise sollte der Name des Autors entfernt werden, wenn ein Dokument anonymisiert weitergegeben werden soll.

Leider bietet dies nur einen rudimentären Schutz, da PDF-Dateien (abhängig von der Programmversion, mit der sie erstellt wurden) auch mit Programmen geöffnet werden können, die diese Sicherheitsattribute ignorieren. Solange z. B. Drucken erlaubt wird, kann das Dokument sogar jederzeit wieder in eine PDF-Datei ohne jegliche Einschränkungen verwandelt werden.

Es muss also beachtet werden, dass je nach verwendetem Anwendungsprogramm, verwendeter Version und eingestellten Optionen mit den zur Verfügung gestellten Programmeigenschaften kein ausreichender Schutz erzielt werden kann. Je nach Schutzbedarf müssen Dateien daher mit kryptographischen Verfahren signiert werden (siehe auch CON.1 Kryptokonzept).

ORP.5.M10 Klassifizierung von Informationen (CIA)

Grundsätzlich sollten Mitarbeiter natürlich sorgfältig mit allen Informationen umgehen. Darüber hinaus gibt es aber in vielen Bereichen Daten, die einen höheren Schutzbedarf haben oder besonderen Restriktionen unterliegen, z. B. personenbezogene, finanzrelevante, vertrauliche oder Copyright-geschützte Daten. Für diese gelten je nach ihrer Kategorisierung unterschiedliche Beschränkungen im Umgang mit ihnen. Daher ist es wichtig, alle Mitarbeiter auf die für diese Daten geltenden Restriktionen hinzuweisen (siehe auch ORP.5.A3 Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen). Die Daten sollten möglichst entsprechend gekennzeichnet werden, z. B. indem die Kategorie bei Dokumenten in der Kopf- oder Fußzeile genannt wird.

Der Schutzbedarf von Daten wirkt sich natürlich unmittelbar auf alle Medien aus, auf denen diese gespeichert oder verarbeitet werden. Daten mit besonderem Schutzbedarf können in den unterschiedlichsten Bereichen anfallen, z. B. bei Fax oder E-Mail. Es sollte also in allen Bereichen Regelungen geben, in denen auch festgelegt ist, wer solche Daten lesen, bearbeiten bzw. weitergeben darf. Dazu gehört, falls erforderlich, auch die regelmäßige Überprüfung auf Korrektheit und Vollständigkeit der Daten.

Viele Informationen, aber auch Anwendungen, unterliegen Copyright-Vermerken oder Weitergaberestriktionen ("Nur für den internen Gebrauch"). Alle Mitarbeiter müssen darauf hingewiesen werden, dass weder Dokumente, noch Dateien oder Software ohne Berücksichtigung eventueller Copyright-Vermerke oder Lizenzbedingungen kopiert werden dürfen.

Ein besonderes Augenmerk muss auch auf alle Informationen gelegt werden, die die Grundlage für die Aufgabenerfüllung bilden. Dazu gehören alle geschäftsrelevanten Daten, also z. B. diejenigen Daten, bei deren Verlust die Institution handlungsunfähig wird, die die wirtschaftlichen Beziehungen zusammenarbeitender Unternehmen beeinträchtigen können oder aus deren Kenntnis ein Dritter (z. B. Konkurrenzunternehmen) finanzielle Vorteile ziehen kann. Jede Behörde und jedes Unternehmen sollte eine Übersicht darüber haben, welche Daten als geschäftskritisch einzustufen sind. Neben den allgemeinen Sorgfaltspflichten können auch hier für diese Daten bei der Speicherung, Verarbeitung, Weitergabe und Vernichtung besondere Vorschriften und Regelungen gelten. Diese geschäftskritischen Informationen müssen vor Verlust, Manipulation und Verfälschung geschützt werden. Längerfristig gespeicherte oder archivierte Daten müssen regelmäßig auf ihre Lesbarkeit getestet werden. Nicht mehr benötigte Informationen müssen zuverlässig gelöscht werden (siehe auch CON.7 Löschen und Vernichten).

ORP.5.M11 Erhebung der rechtlichen Rahmenbedingungen für kryptografische Verfahren und Produkte [IT-Betrieb, Verantwortliche der einzelnen Anwendungen] (CI)

Bevor eine Entscheidung getroffen werden kann, welche kryptographischen Verfahren und Produkte eingesetzt werden sollen, müssen eine Reihe von Einflussfaktoren ermittelt werden. Dazu können die Systemadministratoren und die Verantwortlichen der einzelnen IT-Systeme bzw. IT-Anwendungen befragt werden. Die Ergebnisse müssen nachvollziehbar z. B. in einem Kryptokonzept dokumentiert werden (siehe auch CON.1 Kryptokonzept).

Für sämtliche festgelegten Speicherorte und Übertragungsstrecken sind folgende Einflussfaktoren zu ermitteln:

- Sicherheitsaspekte, z. B. zu erreichender Schutzbedarf und Angreiferpotential
- Technische Aspekte, z.B. IT-Systemumfeld, Datenvolumen, Performance
- Personelle und organisatorische Aspekte, z. B. Benutzerfreundlichkeit, Schulungsbedarf, zusätzlicher Personalbedarf
- Wirtschaftliche Aspekte, z. B. einmalige Investitionen, laufende Kosten, Personalkosten, Lizenzgebühren
- Einsatz von Key-Recovery-Mechanismen
- maximale Lebensdauer der kryptographischen Verfahren
- gesetzliche Rahmenbedingungen beim Einsatz kryptographischer Produkte

Beim Einsatz kryptographischer Produkte sind diverse gesetzliche Rahmenbedingungen zu beachten. In einigen Ländern dürfen beispielsweise kryptographische Verfahren nicht ohne Genehmigung eingesetzt werden. Daher muss untersucht werden,

- ob innerhalb der zum Einsatzgebiet gehörenden Länder Einschränkungen beim Einsatz kryptographischer Produkte zu beachten sind (innerhalb Deutschland gibt es keinerlei Einschränkungen) und
- ob für infrage kommende Produkte Exportbeschränkungen beachtet werden müssen.

Werden mobile IT-Systeme oder Komponenten auf Auslandsreisen eingesetzt, muss vor jedem Grenzübertritt geklärt werden, welche länderspezifischen Regelungen zu beachten sind (siehe auch CON.8 Sicherheit auf Auslandsreisen).

Es gibt allerdings nicht nur Maximalanforderungen, sondern auch Minimalanforderungen an die verwendeten kryptographischen Algorithmen oder Verfahren. So müssen z. B. bei der Übermittlung von personenbezogenen Daten Verschlüsselungsverfahren mit ausreichender Schlüssellänge eingesetzt werden.

3 Weiterführende Informationen

3.1 Wissenswertes

Derzeit liegen keine über das bereits beschriebene Maß hinausgehenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne entgegen (grundschutz@bsi.bund.de).

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Compliance Management (Anforderungsmanagement)" finden sich unter anderem in folgenden Veröffentlichungen:

[19600] ISO 19600:2014

Compliance management systems - Guidelines, International Organization for Standardization (Hrsg.), ISO/TC 309, Dezember 2014

[27001] ISO/IEC 27001:2013

Information technology-Security techniques-Information security management systems-Requirements, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/SC 27, Oktober 2013

[GSKHM] Hilfsmittel zur Nutzung der IT-Grundschutz-Kataloge

Bundesamt für Sicherheit in der Informationstechnik (BSI), https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Kataloge/Hilfsmittel/Bausteine/bausteine_node.html, zuletzt abgerufen am 05.10.2018

[ISFSY] The Standard of Good Practice for Information Security

Area SY System Management, Information Security Forum (ISF), June 2018

Bundesamt
für Sicherheit in der
Informationstechnik

Umsetzungshinweise für die Bausteinschicht CON

Umsetzungshinweise zum Baustein CON.3 Datensicherungskonzept

1 Beschreibung

1.1 Einleitung

Unternehmen und Behörden speichern immer mehr Daten und sind gleichzeitig immer stärker auf sie angewiesen. Gehen Daten dann verloren, z. B. durch defekte Hardware oder Malware, können gravierende Schäden entstehen. Durch regelmäßige Datensicherungen lassen sich solche Auswirkungen jedoch minimieren: Eine Datensicherung soll gewährleisten, dass durch einen redundanten Datenbestand der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen.

1.2 Lebenszyklus

Planung und Konzeption

Um eine effektive Datensicherung einzurichten, müssen zuerst mögliche Einflussfaktoren identifiziert (siehe CON.3.M1 *Erhebung der Einflussfaktoren der Datensicherung*) und danach eine geeignete Verfahrensweise festgelegt werden (siehe CON.3.M2 *Festlegung der Verfahrensweise für die Datensicherung*). Darauf aufbauend müssen die Verantwortlichen ein Minimaldatensicherungskonzept (siehe CON.3.M4 *Erstellung eines Minimaldatensicherungskonzeptes*) und ein Datensicherungskonzept (siehe CON.3.M6 *Entwicklung eines Datensicherungskonzepts*) entwickeln.

Beschaffung

Datensicherungen werden meistens mithilfe von Backup-Programmen durchgeführt. Allerdings sind nicht alle Programme für jede Institution geeignet. Deswegen muss die Sicherungssoftware sorgfältig ausgesucht werden (siehe CON.3.M7 *Beschaffung eines geeigneten Datensicherungssystems*).

Umsetzung

Alle Mitarbeiter müssen über die Datensicherungen informiert werden und sollten wissen, welche Aufgaben sie selbst dabei zu erfüllen haben (siehe CON.3.M10 *Verpflichtung der Mitarbeiter zur Datensicherung*). Ebenso sollte eine Sicherungskopie der eingesetzten Software erstellt werden (siehe CON.3.M11 *Sicherungskopie der eingesetzten Software*).

Alle Datensicherungen sind geeignet zu dokumentieren (siehe CON.3.M6 *Entwicklung eines Datensicherungskonzepts*).

Betrieb

Die im Datensicherungskonzept vorgegebenen Schritte und Verfahrensweise müssen regelmäßig durchgeführt werden (siehe CON.3.M5 *Regelmäßige Datensicherung*).

Datensicherungen enthalten meistens sehr viele schützenswerte Information über die Institution. Deshalb muss dafür gesorgt werden, dass die Backup-Datenträger geschützt aufbewahrt sind (siehe CON.3.M12 *Geeignete Aufbewahrung der Backup-Datenträger*).

Notfallvorsorge

Datensicherungen müssen im Notfall auch funktionieren, d. h. die gesicherten Daten müssen sich problemlos und schnell wieder einspielen lassen. Um das sicherzustellen, müssen regelmäßige Tests durchgeführt werden (siehe CON.3.A8 *Funktionstests und Überprüfung der Wiederherstellbarkeit*).

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Datensicherungskonzept" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

CON.3.M1 Erhebung der Einflussfaktoren der Datensicherung [Fachverantwortliche, IT-Betrieb]

Für jedes IT-System, eventuell sogar für einzelne IT-Anwendungen mit besonderer Bedeutung, müssen die nachfolgenden Einflussfaktoren ermittelt werden. Dazu können die Systemadministratoren und die Verantwortlichen der einzelnen IT-Anwendungen befragt werden. Die Ergebnisse sind nachvollziehbar zu dokumentieren. Im einzelnen muss ermittelt werden:

- Spezifikation der zu sichernden Daten: Ermittelt werden sollte der Datenbestand des IT-Systems (der IT-Anwendung), der für die Fachaufgaben erforderlich ist. Dazu gehören die Anwendungs- und Betriebssoftware, die Systemdaten (z. B. Initialisierungsdateien, Makrodefinitionen, Konfigurationsdaten, Textbausteine, Passwortdateien, Zugriffsrechtedateien), die Anwendungsdaten selbst und Protokolldaten (z.B. Login-Protokollierung, Protokolle über Sicherheitsverletzungen, Datenübertragungsprotokolle).
- Verfügbarkeitsanforderungen der IT-Anwendungen an die Daten: Für die im ersten Schritt spezifizierten Daten müssen nun die Verfügbarkeitsanforderungen festgelegt werden. Ein erprobtes Maß dazu ist die Angabe der maximal tolerierbaren Ausfallzeit. Sie gibt an, über welchen Zeitraum die Fachaufgabe ohne diese Daten weitergeführt werden kann, ohne dass auf Datensicherungsbestände zurückgegriffen werden muss.
- Rekonstruktionsaufwand der Daten ohne Datensicherung: Um ein unter wirtschaftlichen Gesichtspunkten angemessenes Datensicherungskonzept zu entwickeln (siehe CON.3.M6 Entwicklung eines Datensicherungskonzepts), ist es notwendig zu wissen, ob und mit welchem Aufwand zerstörte Datenbestände rekonstruiert werden können, wenn eine Datensicherung nicht verfügbar ist. Untersucht werden sollte, aus welchen Quellen die Daten rekonstruiert werden können und wie lange das dauern würde. Beispiele hierfür sind die Aktenlage, Ausdrucke, Befragungen und Erhebungen.
- Datenvolumen: Für die Auswahl des Speichermediums ist ein entscheidender Faktor das gespeicherte und zu sichernde Datenvolumen.
- Änderungsvolumen: Um die Häufigkeit der Datensicherung und das adäquate Sicherungsverfahren bestimmen zu können, muss bekannt sein, wie viele Daten sich in einem bestimmten Zeitabschnitt ändern. Notwendig sind Angaben, ob bestehende Dateien inhaltlich geändert oder ob neue Dateien erzeugt werden.
- Änderungszeitpunkte der Daten: Es gibt IT-Anwendungen, bei denen sich Datenänderungen nur zu bestimmten Terminen ergeben, wie zum Beispiel der Abrechnungslauf zur Lohnbuchhaltung zum Monatsende. In solchen Fällen ist eine Datensicherung unverzüglich nach einem solchen Termin sinnvoll. Daher sollte für die zu sichernden Daten angegeben werden, ob sie sich täglich, wöchentlich oder zu bestimmten Terminen ändern.
- Fristen: Für die Daten ist zu klären, ob bestimmte Fristen einzuhalten sind. Hierbei kann es sich um Aufbewahrungsfristen oder auch um Löschfristen im Zusammenhang mit personenbezogenen Daten handeln. Diese Fristen sind bei der Datensicherung zu berücksichtigen.
- Vertraulichkeitsbedarf der Daten: Der Vertraulichkeitsbedarf einer Datei überträgt sich bei einer Datensicherung auf die Sicherungskopie.
- Integritätsbedarf der Daten: Für Datensicherungen muss sichergestellt sein, dass die Daten integer gespeichert wurden und während der Aufbewahrungszeit nicht verändert werden. Das ist um so wichtiger, je höher der Integritätsbedarf der Nutzdaten ist. Daher ist für die Datensicherungen anzugeben, wie hoch der Integritätsbedarf ist.
- Kenntnisse und Fähigkeiten der IT-Benutzer: Um entscheiden zu können, wer die Datensicherung durchführt, der IT-Benutzer selbst oder speziell beauftragte Mitarbeiter bzw. die Systemadministratoren, ist ausschlaggebend, über welche Kenntnisse und Fähigkeiten der IT-Benutzer verfügt und welche Werkzeuge ihm zur Verfügung gestellt werden können. Falls die zeitliche Belastung bei der Durchführung einer Datensicherung für IT-Benutzer zu hoch ist, sollte dies angegeben werden.

CON.3.M2 Festlegung der Verfahrensweise für die Datensicherung [Fachverantwortliche, IT-Betrieb]

Wie eine Datensicherung durchzuführen ist, wird hauptsächlich von den in CON.3.M1 *Erhebung der Einflussfaktoren der Datensicherung* erhobenen Einflussfaktoren bestimmt. Für jedes IT-System und für jede Datenart muss die Verfahrensweise der Datensicherung festgelegt werden. Bei Bedarf ist sogar noch eine Unterscheidung für einzelne IT-Anwendungen des jeweiligen IT-Systems vorzunehmen.

Folgende Punkte sind bei der Festlegung einer Verfahrensweise für die Datensicherung zu betrachten:

- Art der Datensicherung,
- Häufigkeit und Zeitpunkt der Datensicherung,
- Anzahl der Generationen,
- Vorgehensweise und Speichermedium,
- Verantwortlichkeit für die Datensicherung,
- Aufbewahrungsort,
- Anforderungen an das Datensicherungsarchiv,
- Transportmodalitäten und
- Aufbewahrungsmodalität.

In der nachfolgenden Tabelle werden die Abhängigkeiten zwischen den genannten Punkten und den Einflussfaktoren (siehe CON.3.M1 *Erhebung der Einflussfaktoren der Datensicherung*) dargestellt und anschließend erläutert:

	Art der Datensicherung	Häufigkeit und Zeitpunkte der Datens.	Anzahl der Generationen	Vorgehensweise und Speichermedium	Verantwortlichkeit für Datens.	Aufbewahrungsort	Anforderungen an DS-Archiv	Transportmodalitäten	Aufbewahrungsmodalität
Verfügbarkeitsanforderungen	X	(X)	X	X	X	X	X	X	
Rekonstruktionsaufwand ohne Datens.		(X)	X						
Datenvolumen	X		X	X		X	X	X	
Änderungsvolumen	X	X	X	X					
Änderungszeitpunkte der Daten	(X)	X						(X)	
Fristen				X			X		X
Vertraulichkeitsbedarf der Daten				(X)	X		X	X	X

	Art der Datensicherung	Häufigkeit und Zeitpunkte der Datens.	Anzahl der Generationen	Vorgehensweise und Speichermedium	Verantwortlichkeit für Datens.	Aufbewahrungsort	Anforderungen an DS-Archiv	Transportmodalitäten	Aufbewahrungsmodalität
Integritätsbedarf der Daten			(X)	(X)	X		X	X	X
Kenntnisse der IT-Benutzer	X			X	X				

Tabelle: Datensicherung

Art der Datensicherung

Folgende Datensicherungsarten gibt es:

- Volldatensicherung: Bei der Volldatensicherung werden sämtliche zu sichernden Dateien zu einem bestimmten Zeitpunkt auf einen zusätzlichen Datenträger gespeichert. Es wird dabei nicht berücksichtigt, ob die Dateien sich seit der letzten Datensicherung geändert haben oder nicht. Daher benötigt eine Volldatensicherung viel Speicher. Der Vorteil ist, dass die Daten vollständig für den Sicherungszeitpunkt vorliegen und die Restaurierung von Dateien einfach und schnell möglich ist, da nur die betroffenen Dateien aus der letzten Volldatensicherung extrahiert werden müssen. Werden Volldatensicherungen selten durchgeführt, so kann sich durch umfangreiche nachträgliche Änderungen innerhalb einer Datei ein hoher Nacherfassungsaufwand ergeben.
- Inkrementelle Datensicherung: Bei der inkrementellen Datensicherung werden im Gegensatz zur Volldatensicherung nur die Dateien gesichert, die sich gegenüber der letzten Datensicherung (Volldatensicherung oder inkrementelle Sicherung) geändert haben. Das spart Speicherplatz und verkürzt die erforderliche Zeit für die Datensicherung. Die inkrementelle Datensicherung basiert immer auf einer Volldatensicherung. In periodischen Zeitabständen werden Volldatensicherungen erzeugt, in der Zeit dazwischen werden eine oder mehrere inkrementelle Datensicherungen vollzogen. Bei der Restaurierung wird die letzte Volldatensicherung als Grundlage genommen, die um die in der Zwischenzeit geänderten Dateien aus den inkrementellen Sicherungen ergänzt wird.
- Differenzielle Datensicherung: Bei der differenziellen Datensicherung werden jedes Mal die Dateien gesichert, die sich gegenüber der letzten Volldatensicherung geändert haben. Eine differenzielle Datensicherung benötigt mehr Speicherplatz als eine inkrementelle, Dateien lassen sich aber einfacher und schneller restaurieren. Für die Restaurierung der Daten reicht die letzte Volldatensicherung sowie die aktuellste differenzielle, nicht wie bei der inkrementellen, wo unter Umständen mehrere Datensicherungen nacheinander eingelesen werden müssen.
- Spiegelung: Bei einer Datenspiegelung wird permanent eine exakte Kopie der Daten in einem anderen Verzeichnis oder Medium erstellt. Dies geschieht in der Regel transparent für den Benutzer, beispielsweise durch ein RAID-System. Eine Spiegelung alleine ersetzt keine Datensicherung, da Inkonsistenzen, Dateifehler oder Löschungen von Dateien sich sofort auf die gespiegelte Version auswirkt. Werden beispielsweise die originalen Datenbestände durch Ransomware verschlüsselt, wirkt sich dies direkt auf die gespiegelte Kopie aus.

Eine spezielle Form der genannten Datensicherungsstrategien ist die Image-Datensicherung. Hier werden nicht die einzelnen Dateien eines Festplattenstapels gesichert, sondern die physikalischen Sektoren der Festplatte. Es handelt sich dabei um eine Vollsicherung, die sehr schnell auf eine gleichartige Festplatte restauriert werden kann.

Eine weitere Form ist das Hierarchische Speicher-Management (HSM). Hierbei geht es in erster Linie darum, vorhandenen Speicher möglichst wirtschaftlich zu nutzen. Dateien werden abhängig von der Häufigkeit, mit der auf sie zugegriffen wird, auf schnellen Online-Speichern (Festplatten) gehalten, auf Nearline-Speicher (automatische Datenträger-Wechselsysteme) ausgelagert oder auf Offline-Speichern (Magnetbänder) archiviert. Gleichzeitig bieten diese HSM-Systeme auch automatische Datensicherungsroutinen kombiniert aus inkrementeller Datensicherung und Volldatensicherung.

Eine redundante Datenspeicherung bieten RAID-Systeme an (Redundant Array of Inexpensive Disks). Das RAID-Konzept beschreibt die Verbindung von mehreren Festplatten unter dem Kommando eines sogenannten Array-Controllers. Es gibt verschiedene RAID-Level, wovon RAID-Level 1 die Datenspiegelung beschreibt. RAID-Systeme ersetzen jedoch keine Datensicherung! Sie helfen nicht bei Diebstahl oder Brand, daher müssen auch die auf RAID-Systemen gespeicherten Daten auf zusätzliche Medien gesichert werden und diese Medien auch in anderen Brandabschnitten untergebracht werden.

Für die Entscheidung, welche Datensicherungsstrategie angewendet werden soll, sind die folgenden Einflussfaktoren (siehe CON.3.M1 *Erhebung der Einflussfaktoren der Datensicherung*) zu berücksichtigen, um eine für die Anforderungen geeignete und gleichzeitig wirtschaftliche Form zu finden:

- Verfügbarkeitsanforderungen: Sind die Verfügbarkeitsanforderungen sehr hoch, so ist eine Datenspiegelung in Erwägung zu ziehen. Sind die Verfügbarkeitsanforderungen hoch, so sollte einer Volldatensicherung statt einer inkrementellen Datensicherung durchgeführt werden.
- Datenvolumen und Änderungsvolumen: Entspricht das Änderungsvolumen annähernd dem Datenvolumen (z. B. bei der Nutzung einer Datenbank), so verringert sich die Speicherplatzersparnis der inkrementellen Datensicherung so stark, dass eine Vollsicherung erwogen werden kann. Ist jedoch das Änderungsvolumen erheblich kleiner als das Datenvolumen, so spart die inkrementelle Datensicherung Speicherplatz.
- Änderungszeitpunkte der Daten: Einen geringen Einfluss auf die Datensicherungsstrategie können die Änderungszeitpunkte der Daten haben. Gibt es Zeitpunkte, an denen anwendungsbezogen der Komplettdatenbestand gesichert werden muss (z. B. nach buchhalterischen Wochen-, Monats- oder Jahresabschlüsse), so kommt zu diesen Zeitpunkten nur eine Vollsicherung infrage.
- Kenntnisse der IT-Benutzer: Eine Datenspiegelung setzt entsprechende Kenntnisse des Systemadministrators voraus, erfordert jedoch vom Benutzer keinerlei Kenntnisse. Eine Volldatensicherung lässt sich auch von einem IT-Benutzer mit geringen Systemkenntnissen durchführen. Demgegenüber erfordert eine inkrementelle Datensicherung schon mehr Systemkenntnisse und Erfahrungen im Umgang mit Datensicherungen.

Häufigkeit und Zeitpunkte der Datensicherung

Tritt ein Datenverlust ein, sind alle Daten bis zur letzten Sicherung verloren. Je aktueller die letzte Datensicherung ist, desto weniger Datenverlust muss die Institution verkraften. Gleichzeitig muss beachtet werden, dass der Zeitpunkt der Datensicherung nicht nur periodisch (z.B. täglich, wöchentlich, werktags) gewählt werden kann, sondern dass auch ereignisabhängige Datensicherungen (z. B. nach x Transaktionen, nach Ausführung eines bestimmten Programms, nach Systemänderungen) notwendig sein können.

Bei der Auswahl der Häufigkeit und der Zeitpunkte der Datensicherung sind folgende Einflussfaktoren (siehe CON.3.M1 *Erhebung der Einflussfaktoren der Datensicherung*) zu beachten:

- Verfügbarkeitsanforderungen, Wiederherstellungsaufwand ohne Datensicherung und Änderungsvolumen: Der zeitliche Abstand der Datensicherungen ist so zu wählen, dass die Restaurierungs- und Nacherfassungszeit (Rekonstruktionsaufwand der geänderten Daten, für die keine Datensicherung vorhanden ist) der in diesem Zeitraum geänderten Daten (Änderungsvolumen) kleiner als die maximal tolerierbare Ausfallzeit ist.
- Änderungszeitpunkte der Daten: Gibt es Zeitpunkte, an denen sich die Daten in großem Umfang ändern (z. B. Programmlauf für Gehaltszahlung oder Versionswechsel der Software) oder an denen der Komplettdatenbestand vorliegen muss, so bietet es sich an, unmittelbar danach eine Volldatensicherung durchzuführen. Dazu sind neben den periodischen die ereignisabhängigen Datensicherungszeitpunkte festzulegen.

Anzahl der Generationen

Einerseits werden Datensicherungen in kurzen Zeitabständen wiederholt, um eine Kopie eines möglichst aktuellen Datenbestandes verfügbar zu haben, andererseits muss die Datensicherung gewährleisten, dass gesicherte Daten möglichst lange aufbewahrt werden. Eine Volldatensicherung wird als Generation bezeichnet. Die Anzahl der aufzubewahrenden Generationen und der zeitliche Abstand, der zwischen den Generationen liegen muss, sollte festgelegt werden. Diese Anforderungen lassen sich an folgenden Beispielen erläutern:

- Wird eine Datei absichtlich oder unabsichtlich gelöscht, so ist diese Datei in allen späteren Datensicherungen nicht mehr verfügbar. Stellt sich heraus, dass diese gelöschte Datei dennoch benötigt wird, so muss zur Wiederherstellung auf eine ältere Datensicherung zurückgegriffen werden, die zeitlich vor dem Löschen erstellt wurde. Ist eine solche Generation nicht mehr vorhanden, so muss die Datei neu erfasst werden.
- Tritt ein Integritätsverlust in einer Datei auf, z. B. durch Malware, ist es wahrscheinlich, dass dies nicht direkt, sondern erst zeitlich versetzt bemerkt wird. Um die Integrität der Datei wiederherstellen zu können, muss dann auf eine Generation zurückgegriffen werden, die vor dem Integritätsverlust erstellt wurde.
- Es kann nicht ausgeschlossen werden, dass eine Datensicherung fehlerhaft oder unvollständig erstellt wurde. Deswegen ist es oft hilfreich, wenn auf eine weitere Generation zurückgegriffen werden kann.

Um diese Vorteile des Generationenprinzips aufrechterhalten zu können, muss jedoch eine Randbedingung eingehalten werden: der zeitliche Abstand der Generationen darf ein Mindestmaß nicht unterschreiten. Beispiel: In einem automatisierten Datensicherungsverfahren kommt es zu wiederholten Abbrüchen des Datensicherungslaufs. Hierdurch würden nacheinander sämtliche Generationen überschrieben werden. Verhindert werden kann dies, indem vor Überschreiben einer Generation das Mindestalter überprüft und nur dann überschrieben wird, wenn dieses Alter überschritten ist.

Charakterisieren lässt sich ein Generationsprinzip durch zwei Größen: das Mindestalter der ältesten Generation und die Anzahl der verfügbaren Generationen. Dabei gilt:

- je höher das Mindestalter der ältesten Generation ist, je größer ist die Wahrscheinlichkeit, dass zu einer Datei mit Integritätsverlust (eine gelöschte Datei, die im Nachhinein als notwendig erkannt wird, ist ebenfalls darunter zu fassen) noch eine Vorläuferversion vorhanden ist,
- je größer die Anzahl der verfügbaren Generationen ist, umso aktueller ist die angeforderte Vorläuferversion.

Die Anzahl der Generationen hängt jedoch direkt mit den Kosten der Datensicherung zusammen, weil Datenträger in ausreichender Zahl vorhanden sein müssen. Da für jede Generation ein eigener Datenträger benutzt werden sollte, muss die Anzahl der Generationen auf ein wirtschaftlich sinnvolles Maß beschränkt werden.

Für die Wahl der Parameter des Generationsprinzips ergeben sich folgende Einflüsse (siehe CON.3.M1 *Erhebung der Einflussfaktoren der Datensicherung*):

- Verfügbarkeitsanforderungen und Integritätsbedarf der Daten: Je höher die Verfügbarkeitsanforderungen oder der Integritätsbedarf der Daten ist, umso mehr Generationen müssen vorhanden sein, um im Fall des Integritätsverlustes die Wiederherstellungszeit zu minimieren.
- Wenn der Verlust einer Datei oder eine Integritätsverletzung möglicherweise erst sehr spät bemerkt werden kann, sind zusätzliche Quartals- oder Jahressicherungsdatenbestände empfehlenswert.

- Wiederherstellungsaufwand ohne Datensicherung: Sind die Daten zwar umfangreich, aber auch ohne Datensicherung rekonstruierbar, so kann das als eine weitere Pseudo-Generation ins Kalkül gezogen werden.

- Datenvolumen: Je höher das Datenvolumen ist, desto mehr Speicherplatz wird gebraucht und desto höher sind auch die Kosten einer Generation. Ein hohes Datenvolumen kann deshalb die Anzahl der Generationen aus wirtschaftlichen Gründen beschränken.

- Änderungsvolumen: Je höher das Änderungsvolumen ist, umso kürzer sollten die Zeitabstände zwischen den Generationen sein, um eine möglichst zeitnahe Version der betreffenden Datei zu haben und den Wiederherstellungsaufwand gering zu halten.

Vorgehensweise und Speichermedium

Nachdem die Art der Datensicherung, die Häufigkeit und das Generationenprinzip festgelegt wurden, ist nun die Vorgehensweise und das angemessene Speichermedium auszuwählen.

Um das Datenvolumen auf dem Speichermedium zu minimieren, können Datenkompressionsalgorithmen angewandt werden. Teilweise kann das Datenvolumen damit sehr stark reduziert werden. Es ist dabei jedoch sicherzustellen, dass die gewählten Parameter und Algorithmen dokumentiert und für die Wiederherstellung der Daten (Dekompression) vorgehalten werden.

Für die **Vorgehensweise** gibt es zwei Parameter, die festgelegt werden müssen: den Automatisierungsgrad und die Zentralisierung (Speicherort).

Beim Automatisierungsgrad ist zwischen manuell und automatisch zu unterscheiden:

- Manuelle Datensicherung bedeutet, dass die Datensicherung händisch angestoßen wird. Vorteilhaft kann sein, dass der Ausführende individuell den Termin der Datensicherung dem Arbeitsablauf anpassen kann. Nachteil ist, dass die Datensicherung von der Motivation und Disziplin des Mitarbeiters abhängt. Durch Krankheit oder sonstige Abwesenheitsgründe können so eventuell Datensicherungen ausfallen.
- Automatische Datensicherungen werden programmgesteuert zu bestimmten Terminen angestoßen. Vorteilhaft ist, dass die Datensicherung zuverlässig durchgeführt wird, sofern der Terminplan vollständig und aktuell ist. Nachteilig kann sein, dass der Terminplan aktuellen Änderungen angepasst werden muss oder wichtige Änderungen nicht unmittelbar gesichert werden.

Bezüglich der Zentralisierung sind zentral und dezentral durchgeführte Datensicherungen zu unterscheiden:

- Zentrale Datensicherungen zeichnen sich dadurch aus, dass der Speicherort und die Datensicherung am zentralen IT-System durchgeführt werden. Diese Verfahrensweise hat den Vorteil, dass nur ein Mitarbeiter intensiv geschult werden muss und die Benutzer von dieser Arbeit entlastet werden. Vorteilhaft ist weiterhin, dass durch das höhere zentrale Datenaufkommen kostengünstigere Speichermedien verwendet werden können. Nachteilig ist, dass eventuell vertrauliche Daten übertragen und von nicht Befugten eingesehen werden könnten.
- Dezentrale Datensicherungen werden von den Benutzern selbst durchgeführt, ohne dass die Daten auf ein zentrales IT-System übertragen werden müssen. Vorteilhaft ist, dass der Benutzer die Kontrolle über die Daten und die Backup-Datenträger behält, insbesondere wenn es sich um vertrauliche Daten handelt. Nachteilig ist, dass die konsequente Datensicherung damit von der Zuverlässigkeit der Benutzer abhängt und dass dezentrale Lösungen den Benutzern Zeitaufwand abfordern.

Nach der Entscheidung, ob die Datensicherung manuell oder automatisch, zentral oder dezentral durchgeführt wird, muss nun der geeignete Datenträger bzw. das geeignete Speichermedium für die Datensicherung gefunden werden. Dazu können folgende Parameter betrachtet werden:

- Datenträger-Anforderungszeit: Wie lang darf es dauern, bis ein Backup-Datenträger für eine Wiederherstellung bereitstehen muss? Roboter-Systeme können das innerhalb von Minuten, ausgelagerte Bänder müssen unter Umständen erst aufwendig transportiert und aufgelegt werden.
- Zugriffszeit, Transferrate: Wie lang eine Datensicherung dauert und wie schnell sich Daten wiederherstellen lassen, hängt von der mittleren Zugriffszeit des Datenträgers und von der Transferrate ab. Festplatten erlauben einen Zugriff auf bestimmte Dateien im Millisekunden-Bereich, ein Magnetband muss erst zur entsprechenden Stelle gespult werden und bei einem Cloud-Speicher hängt die Transferrate direkt von der Internet-Anbindung ab.
- Speicherkapazität: Das Speichermedium muss über ausreichende Speicherkapazitäten verfügen. Dabei müssen auch zukünftige Datenmengen mit eingeplant werden.
- Kosten: Die Kosten für die Datensicherung müssen in einem angemessenen Verhältnis zum Sicherungszweck stehen. Hierbei ist auch die Lebensdauer der Datenträger zu berücksichtigen.

Die folgenden Einflussgrößen (siehe CON.3.M1 *Erhebung der Einflussfaktoren der Datensicherung*) müssen dabei beachtet werden:

- Verfügbarkeitsanforderungen: Je höher die Verfügbarkeitsanforderungen sind, desto schneller muss auf die Datenträger als Speichermedium der Datensicherung zugegriffen werden können und desto schneller müssen die benötigten Daten vom Datenträger wieder einspielbar sein.
- Es muss sichergestellt sein, dass die Speichermedien auch bei Ausfall eines Lesegerätes zur Wiederherstellung genutzt werden können. Die Kompatibilität und Funktion eines Ersatzgerätes sind zu gewährleisten.
- Daten- und Änderungsvolumen: Mit zunehmenden Datenvolumen werden oft preisgünstige Speichermedien benutzt.
- Fristen: Müssen Löschfristen eingehalten werden (z. B. bei personenbezogenen Daten), muss das ausgewählte Speichermedium die Löschung ermöglichen. Speichermedien, die nicht oder nur mit großem Aufwand löschbar sind (z. B. WORM), sollten in diesem Fall vermieden werden.
- Vertraulichkeitsbedarf und Integritätsbedarf der Daten: Ist der Vertraulichkeits- oder Integritätsbedarf der zu sichernden Daten hoch, so überträgt sich dieser Schutzbedarf auch auf die zur Datensicherung eingesetzten Datenträger. Ist eine Verschlüsselung der Datensicherung nicht möglich, kann über die Auswahl von Datenträgern nachgedacht werden, die aufgrund ihrer kompakten Bauart in Datensicherungsschränken oder Tresoren untergebracht werden können.
- Kenntnisse der IT-Benutzer: Die Kenntnisse und datenverarbeitungsspezifischen Fähigkeiten der IT-Benutzer entscheiden darüber, ob eine Verfahrensweise gewählt werden kann, in der der Benutzer selbst manuell für die Datensicherung tätig wird, ob andere ausgebildete Personen die Datensicherung dezentral durchführen oder ob eine automatisierte Datensicherung praktikabler ist.

Verantwortlichkeit für die Datensicherung

Für die Entscheidung, wer für die Datensicherung verantwortlich ist, kommen drei Personengruppen infrage: Zunächst kann es der Benutzer selbst sein (typischerweise bei dezentralen und nicht vernetzten IT-Systemen), der Systemverwalter oder ein für die Datensicherung speziell ausgebildeter Administrator. Wird die Datensicherung nicht vom Benutzer durchgeführt, sind die Verantwortlichen auf Verschwiegenheit bezüglich der Dateninhalte zu verpflichten. Eventuell sollten die Daten auch verschlüsselt werden.

Darüber hinaus sind die Entscheidungsträger zu benennen, die eine Wiederherstellung veranlassen können. Zu klären ist weiterhin, wer berechtigt ist, auf Datensicherungsträger zuzugreifen, insbesondere wenn sie in Datensicherungsarchiven ausgelagert sind. Es muss sichergestellt sein, dass nur Berechtigte Zutritt erhalten. Abschließend ist zu definieren, wer berechtigt ist, eine Wiederherstellung des Gesamtdatenbestandes oder ausgewählter, einzelner Dateien operativ durchzuführen.

Bei der Festlegung der Verantwortlichkeit ist insbesondere der Vertraulichkeits-, Integritätsbedarf der Daten und die Vertrauenswürdigkeit der zuständigen Mitarbeiter zu betrachten. Es muss sichergestellt werden, dass der Verantwortliche erreichbar ist und ein Vertreter benannt und eingearbeitet wird.

Als Einflussfaktor (siehe CON.3.M1 *Erhebung der Einflussfaktoren der Datensicherung*) ist zu beachten:

- Kenntnisse der IT-Benutzer: Die Kenntnisse und datenverarbeitungsspezifischen Fähigkeiten der IT-Benutzer entscheiden darüber, ob die Datensicherung eigenverantwortlich je IT-Benutzer durchgeführt werden sollte. Sind die Kenntnisse der IT-Benutzer nicht ausreichend, ist die Verantwortung dem Systemadministrator oder einer speziell ausgebildeten Person zu übertragen.

Aufbewahrungsort

Grundsätzlich sollten Datensicherungsmedien und Originaldatenträger in unterschiedlichen Brandabschnitten aufbewahrt werden (siehe CON.3.M12 *Geeignete Aufbewahrung der Backup-Datenträger*). Je weiter entfernt jedoch die Datenträger lagern, desto länger können die Transportwege und damit die Transportzeiten sein, und desto länger dauert die Wiederherstellung. Als Einflussfaktoren (siehe CON.3.M1 *Erhebung der Einflussfaktoren der Datensicherung*) sind daher zu betrachten:

- Verfügbarkeitsanforderungen: Je höher die Verfügbarkeitsanforderungen sind, umso schneller müssen die Datenträger der Datensicherung verfügbar sein. Werden die Datenträger extern ausgelagert, so ist bei sehr hohen Verfügbarkeitsanforderungen zu erwägen, Kopien der Datensicherung zusätzlich in unmittelbarer Nähe vorzuhalten.
- Vertraulichkeits- und Integritätsbedarf der Daten: Je höher dieser Bedarf ist, umso besser muss verhindert werden, dass an den Datenträgern manipuliert werden kann. Die notwendige Zutrittskontrolle lässt sich durch entsprechende infrastrukturelle und organisatorische Maßnahmen erreichen.
- Datenvolumen: Mit steigendem Datenvolumen ist die Sicherheit des Aufbewahrungsortes zunehmend wichtig.

Anforderungen an das Datensicherungsarchiv

Datensicherungen besitzen einen mindestens ebenso hohen Schutzbedarf bezüglich Vertraulichkeit und Integrität wie die gesicherten Daten selbst. Bei der Aufbewahrung in einem zentralen Datensicherungsarchiv sind daher entsprechend wirksame Sicherheitsmaßnahmen notwendig, z. B. eine Zutrittskontrolle.

Zusätzlich muss durch organisatorische und personelle Maßnahmen (Datenträgerverwaltung) sichergestellt werden, dass der schnelle und gezielte Zugriff auf benötigte Datenträger möglich ist. Hierzu ist der Baustein OPS.1.2.2 *Archivierung* zu beachten.

Folgende Einflussfaktoren (siehe CON.3.M1 *Erhebung der Einflussfaktoren der Datensicherung*) müssen beachtet werden:

- Verfügbarkeitsanforderungen: Je höher die Verfügbarkeitsanforderungen sind, umso schneller muss der gezielte Zugriff auf benötigte Datenträger möglich sein. Wenn eine manuelle Bestandsführung den Verfügbarkeitsanforderungen nicht genügt, können automatisierte Zugriffsverfahren eingesetzt werden.
- Datenvolumen: Das Datenvolumen bestimmt letztendlich die Art und die Anzahl der aufzubewahrenden Datenträger bzw. die Größe des Online-Speichers. Für entsprechend große Datenvolumen ist eine ausreichende Aufbewahrungskapazität im Datenträgerarchiv vorzusehen.
- Fristen: Sind Löschungsfristen einzuhalten, muss die Organisation des Datensicherungsarchivs sicherstellen, dass die Daten zu den vorgegebenen Zeitpunkten gelöscht werden. Der Vorgang ist zu dokumentieren.
- Vertraulichkeits- und Integritätsbedarf der Daten: Je höher dieser Bedarf ist, umso sorgfältiger muss verhindert werden, dass an den Datenträgern manipuliert werden kann. Die notwendige Zutrittskontrolle lässt sich durch entsprechende infrastrukturelle und organisatorische Maßnahmen erreichen.

Transportmodalitäten

Während einer Datensicherung werden Daten transportiert. Sei es, dass sie über ein Netz oder eine Leitung übertragen werden, sei es, dass Datenträger zum Datenträgerarchiv transportiert werden. Dabei gilt es folgendes zu beachten:

- Verfügbarkeitsanforderungen: Je höher die Verfügbarkeitsanforderungen sind, desto schneller müssen die Daten zur Wiederherstellung verfügbar sein. Das ist bei der Auswahl des Datenübertragungsmediums bzw. bei Auswahl des Datenträger-Transportweges zu berücksichtigen.
- Datenvolumen: Wenn zur Wiederherstellung die Daten über ein Netz übertragen werden, muss die Übertragungskapazität des Netzes beachtet werden. Es muss gewährleistet sein, dass das Datenvolumen innerhalb der erforderlichen Zeit (Verfügbarkeitsanforderung) übertragen werden kann.
- Änderungszeitpunkte der Daten: Werden Datensicherungen über ein Netz durchgeführt (insbesondere zu ausgewählten Terminen), kann aufgrund des zu übertragenden Datenvolumens ein Kapazitätsengpass entstehen. Daher ist zum Zeitpunkt der Datensicherung eine ausreichende Datenübertragungskapazität sicherzustellen.
- Vertraulichkeits- und Integritätsbedarf der Daten: Je höher dieser Bedarf ist, umso sorgfältiger muss verhindert werden, dass die Daten auf dem Transport abgehört, unbefugt kopiert oder manipuliert werden. Bei Datenübertragungen ist schließlich eine Verschlüsselung oder ein kryptografischer Manipulationsschutz zu bedenken. Beim physischen Transport sind sichere Behältnisse und Wege zu benutzen und eventuell auch Nutzen und Aufwand einer Verschlüsselung abzuwägen.

Aufbewahrungsmodalität

Im Rahmen des Datensicherungskonzeptes (siehe CON.3.M6 *Entwicklung eines Datensicherungskonzepts*) sollte mit betrachtet werden, ob für bestimmte Daten Aufbewahrungs- oder Löschfristen einzuhalten sind.

- Fristen: Falls Aufbewahrungsfristen einzuhalten sind, sollten die Daten archiviert werden (siehe OPS.1.2.2 Archivierung). Falls Löschfristen einzuhalten sind, müssen der organisatorische Ablauf festgelegt und die technischen Voraussetzungen geschaffen werden, damit die Daten zu den vorgegebenen Zeitpunkten gelöscht werden können.

CON.3.M3 Ermittlung von rechtlichen Einflussfaktoren auf die Datensicherung

Für die Datensicherung müssen eine Reihe von rechtlichen Einflussfaktoren beachtet werden, z. B. Datenschutzgesetze. So bestehen für die Aufbewahrung bestimmter Informationen verschiedene rechtliche Vorgaben. Werden diese nicht eingehalten, kann das zivil- oder strafrechtliche Konsequenzen haben. Daher sollten sich die Verantwortlichen informieren, welche rechtlichen Vorgaben zu beachten sind.

Hieraus ergeben sich Anforderungen, die im Datensicherungskonzept berücksichtigt werden müssen.

CON.3.M4 Erstellung eines Minimaldatensicherungskonzeptes

Für eine Institution ist festzulegen, welche Minimalforderungen zur Datensicherung eingehalten werden müssen. Sie dient als Grundlage für ein Datensicherungskonzept und gilt generell für alle IT-Systeme und besonders auch für neue IT-Systeme, für die noch kein Datensicherungskonzept erarbeitet wurde.

Ein Minimaldatensicherungskonzept kann wie folgt aussehen:

- Software: Es ist sämtliche erworbene oder selbst erstellte Software einmalig mittels einer Vollsicherung zu sichern.
- Systemdaten: Alle Systemdaten sind mindestens einmal monatlich mit einer Generation zu sichern.
- Anwendungsdaten: Alle Anwendungsdaten sind mindestens wöchentlich mittels einer Vollsicherung im Drei-Generationen-Prinzip zu sichern.
- Protokolldaten: Sämtliche Protokolldaten sind mindestens einmal monatlich mittels einer Vollsicherung im Drei-Generationen-Prinzip zu sichern.
- Durchführung: Eingesetzt Hard- und Software, verwendete Parameter, Vorgehensweise der Datensicherung bzw. Wiederherstellung.

CON.3.M5 Regelmäßige Datensicherung [IT-Betrieb]

Nach den Vorarbeiten und der Grundkonzeption müssen mit der gewählten Vorgehensweise regelmäßige Datensicherungen durchgeführt werden.

Es müssen mindestens die Daten regelmäßig gesichert werden, die nicht aus anderen Informationen abgeleitet werden können. Dokumentationen, Programm- und Programmablaufbeschreibungen sind vorzuhalten.

Empfehlenswert ist die Erstellung eines Datensicherungskonzepts (siehe CON.3.M6 *Entwicklung eines Datensicherungskonzepts*).

Abhängig von der Menge und Wichtigkeit der laufend neu gespeicherten Daten und vom möglichen Schaden bei Verlust dieser Daten ist folgendes festzulegen:

- ZeitintervallBeispiele: täglich, wöchentlich, monatlich
- ZeitpunktBeispiele: nachts, freitags abends
- Anzahl der aufzubewahrenden GenerationenBeispiel: Bei täglicher Komplettsicherung werden die letzten sieben Sicherungen aufbewahrt, außerdem die Freitag-Abend-Sicherungen der letzten zwei Monate.
- Umfang der zu sichernden DatenAm einfachsten ist es, Partitionen bzw. Verzeichnisse festzulegen, die bei der regelmäßigen Datensicherung berücksichtigt werden. Eine geeignete Differenzierung kann die Übersichtlichkeit vergrößern sowie Aufwand und Kosten sparen helfen.Beispiel: selbst erstellte Dateien und individuelle Konfigurationsdateien
- Speichermedien (abhängig von der Datenmenge)Beispiele: DVDs, USB-Speicher oder Festplatten
- Vorherige Löschung der Datenträger vor Wiederverwendung (z. B. bei Festplatten)
- Zuständigkeit für die Durchführung (Administrator, Benutzer)
- Zuständigkeit für die Überwachung der Sicherung, insbesondere bei automatischer Durchführung (Fehlermeldungen, verbleibender Platz auf den Speichermedien)
- Dokumentation der erstellten Sicherungen (Datum, Art der Durchführung der Sicherung sowie gewählte Parameter, Beschriftung der Datenträger)

Wegen des großen Aufwands können Komplettsicherungen in der Regel höchstens einmal täglich durchgeführt werden. Die seit der letzten Sicherung erstellten Daten können nicht wieder eingespielt werden. Daher und zur Senkung der Kosten sollten zwischen den Komplettsicherungen regelmäßig differenzielle oder inkrementelle Sicherungen durchgeführt werden. Hinweise zu den verschiedenen Arten von Datensicherungen finden sich in CON.3.M2 *Festlegung der Verfahrensweise für die Datensicherung*.

Eine differenzielle oder inkrementelle Sicherung kann häufiger erfolgen, zum Beispiel sofort nach Erstellung wichtiger Dateien oder mehrmals täglich. Die Vereinbarkeit mit dem laufenden Betrieb ist sicherzustellen.

Für eingesetzte Software ist separat zu entscheiden, ob sie von der regelmäßigen Datensicherung erfasst werden muss. Dies hängt beispielsweise davon ab, wie aufwändig eine Neuinstallation und das Einspielen von Patches und Updates ist. Unter Umständen ist es ausreichend, Sicherungskopien von den Originaldatenträgern anzufertigen (siehe CON.3.M11 *Sicherungskopie der eingesetzten Software*).

Alle Benutzer sollten über die Regelungen zur Datensicherung informiert sein (siehe CON.3.M10 *Verpflichtung der Mitarbeiter zur Datensicherung*).

Falls bei vernetzten Rechnern nur die Server-Platten gesichert werden, ist sicherzustellen, dass die zu sichernden Daten regelmäßig von den Benutzern oder automatisch dorthin überspielt werden. Bei größeren Änderungen an IT-Systemen oder im Informationsverbund muss der Datensicherungsprozess entsprechend angepasst werden.

Vertrauliche Daten sollten vor der Sicherung möglichst verschlüsselt werden, wobei darauf zu achten ist, dass eine Entschlüsselung auch nach einem längeren Zeitraum möglich sein muss (siehe CON.3.M13 *Einsatz kryptografischer Verfahren bei der Datensicherung*).

Der Ausdruck von Daten auf Papier ist keine angemessene Art der Datensicherung.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Datensicherungskonzept".

CON.3.M6 Entwicklung eines Datensicherungskonzepts [Fachverantwortliche, Leiter IT]

Die Verfahrensweise der Datensicherung wird von einer großen Zahl von Einflussfaktoren bestimmt: Das IT-System, das Datenvolumen, die Änderungsfrequenz der Daten und die Verfügbarkeitsanforderungen sind einige dieser Faktoren. Im Datensicherungskonzept gilt es, eine Lösung zu finden, die diese Faktoren berücksichtigt und gleichzeitig unter Kostengesichtspunkten wirtschaftlich vertretbar ist.

Die technischen Möglichkeiten, Datensicherungen durchzuführen, sind vielfältig. Jedoch wird die Auswahl immer von den genannten Faktoren bestimmt. Daher gilt es zunächst, die Einflussgrößen der IT-Systeme und der damit realisierten IT-Anwendungen zu bestimmen und nachvollziehbar zu dokumentieren (siehe CON.3.M1 *Erhebung der Einflussfaktoren der Datensicherung)*. Anschließend muss die geeignete Verfahrensweise entwickelt und dokumentiert werden (siehe CON.3.M2 *Festlegung der Verfahrensweise für die Datensicherung*). Zum Abschluss muss durch die Institutionsleitung die Durchführung angeordnet werden. Auch muss das Datensicherungskonzept regelmäßige Funktionstest für Datensicherung vorsehen (siehe CON.3.M9 *Funktionstests und Überprüfung der Wiederherstellbarkeit*)

Die Ergebnisse sollten aktualisierbar und erweiterbar in einem Datensicherungskonzept niedergelegt werden. Ein möglicher Aufbau eines Datensicherungskonzepts ist im nachfolgenden Inhaltsverzeichnis beispielhaft aufgezeigt:

Inhaltsverzeichnis Datensicherungskonzept

1. Definitionen

- Anwendungsdaten, Systemdaten, Software, Protokolldaten
- Vollsicherung, inkrementelle Datensicherung

2. Gefährdungslage (zur Motivation)

- Abhängigkeit der Institution vom Datenbestand
- Typische Gefährdungen wie ungeschulte Benutzer, gemeinsam genutzte Datenbestände, Computer-Viren, Hacker, Stromausfall, Festplattenfehler
- Institutionsrelevante Schadensursachen
- Schadensfälle im eigenen Haus

3. Einflussfaktoren je IT-System

- Spezifikation der zu sichernden Daten
- Verfügbarkeitsanforderungen der IT-Anwendungen an die Daten
- Rekonstruktionsaufwand der Daten ohne Datensicherung
- Datenvolumen
- Änderungsvolumen
- Änderungszeitpunkte der Daten
- Fristen
- Vertraulichkeitsbedarf der Daten
- Integritätsbedarf der Daten
- Kenntnisse und datenverarbeitungsspezifische Fähigkeiten der IT-Benutzer

4. Datensicherungsplan je IT-System

4.1 Festlegungen je Datenart und 4.2 Festlegung der Vorgehensweise bei der Datenwiederherstellung

- Art der Datensicherung
- Häufigkeit und Zeitpunkt der Datensicherung
- Anzahl der Generationen
- Datensicherungsmedium
- Verantwortlichkeit für die Datensicherung
- Aufbewahrungsort der Backup-Datenträger
- Anforderungen an das Datensicherungsarchiv
- Transportmodalitäten
- Wiederherstellungszeiten bei vorhandener Datensicherung
- Randbedingungen für das Datensicherungsarchiv
    - Vertragsgestaltung (bei externen Archiven)
    - Refresh-Zyklen der Datensicherung
    - Bestandsverzeichnis
    - Löschen von Datensicherungen
    - Vernichtung von unbrauchbaren Datenträgern
    - Vorhalten von arbeitsfähigen Lesegeräten

5. Minimaldatensicherungskonzept

6. Verpflichtung der Mitarbeiter zur Datensicherung

7. Sporadische Restaurierungsübungen

Einzelne Punkte dieses Datensicherungskonzepts werden in den Maßnahmen CON.3.M1 *Erhebung der Einflussfaktoren der Datensicherung*, CON.3.M2 *Festlegung der Verfahrensweise für die Datensicherung*, CON.3.M8 *Funktionstests und Überprüfung der Wiederherstellbarkeit* und CON.3.M10 *Verpflichtung der Mitarbeiter zur Datensicherung* näher ausgeführt.

CON.3.M7 Beschaffung eines geeigneten Datensicherungssystems [IT-Betrieb, Leiter IT]

Bei der Beschaffung eines Datensicherungssystems sollte nicht allein auf seine Leistungsfähigkeit geachtet werden, sondern auch auf die Bedienbarkeit und insbesondere auf seine Toleranz gegenüber Benutzerfehlern.

Die Sicherungssoftware sollte folgende Anforderungen erfüllen:

- Die Datensicherungssoftware sollte ein falsches oder ein beschädigtes Medium im Sicherungslaufwerk erkennen können.
- Sie sollte mit der vorhandenen Hardware problemlos zusammenarbeiten.
- Es sollte möglich sein, Sicherungen automatisch zu vorwählbaren Zeiten bzw. in einstellbaren Intervallen durchführen zu lassen, ohne dass hierzu manuelle Eingriffe (außer dem eventuell notwendigen Bereitstellen von Sicherungsdatenträgern) erforderlich wären.
- Es sollte möglich sein, einen oder mehrere ausgewählte Benutzer automatisch über das Sicherungsergebnis und eventuelle Fehlermeldungen per E-Mail oder ähnliche Mechanismen zu informieren. Die Durchführung von Datensicherungen inklusive des Sicherungsergebnisses und möglicher Fehlermeldungen sollten in einer Protokolldatei abgespeichert werden.
- Die Sicherungssoftware sollte die Sicherung des Backup-Mediums durch ein Passwort oder noch besser durch Verschlüsselung unterstützen. Weiterhin sollte sie in der Lage sein, die gesicherten Daten in komprimierter Form abzuspeichern.
- Durch Vorgabe geeigneter Include- und Exclude-Listen bei der Datei- und Verzeichnisauswahl sollte genau spezifiziert werden können, welche Daten zu sichern sind und welche nicht. Es sollte möglich sein, diese Listen zu Sicherungsprofilen zusammenzufassen, abzuspeichern und für spätere Sicherungsläufe wieder zu benutzen.
- Es sollte möglich sein, die zu sichernden Daten abhängig vom Erstellungsdatum bzw. ihrer letzten Modifikation auszuwählen.
- Die Sicherungssoftware sollte logische und physische Vollkopien sowie inkrementelle Kopien (Änderungssicherungen) erzeugen können.
- Die zu sichernden Daten sollten auch auf Netzlaufwerken oder in Online-Datenspeichern abgespeichert werden können.
- Die Sicherungssoftware sollte in der Lage sein, nach der Sicherung einen automatischen Vergleich der gesicherten Daten mit dem Original durchzuführen und nach der Wiederherstellung von Daten einen entsprechenden Vergleich zwischen den rekonstruierten Daten und dem Inhalt des Sicherungsdatenträgers durchzuführen.
- Bei der Wiederherstellung von Dateien sollte es möglich sein auszuwählen, ob die Dateien am ursprünglichen Ort oder auf einer anderen Platte bzw. in einem anderen Verzeichnis wiederhergestellt werden. Ebenso sollte es möglich sein, das Verhalten der Software für den Fall zu steuern, dass am Zielort schon eine Datei gleichen Namens vorhanden ist. Dabei sollte man wählen können, ob diese Datei immer, nie oder nur in dem Fall, dass sie älter als die zu rekonstruierende Datei ist, überschrieben wird, oder dass in diesem Fall eine explizite Anfrage erfolgt.

Falls mit dem eingesetzten Programm die Datensicherung durch Passwort geschützt werden kann, sollte diese Option genutzt werden. Das Passwort ist dann gesichert zu hinterlegen.

Bei den meisten Betriebssystemen werden Programme für Datensicherungen mitgeliefert. Nicht alle erfüllen allerdings die Ansprüche an Produkte für professionelle und komfortable Datensicherungen. Sind jedoch keine anderen Produkte verfügbar, so sollten die systemzugehörigen Programme verwendet werden.

CON.3.M8 Funktionstests und Überprüfung der Wiederherstellbarkeit [IT-Betrieb]

Wenn ein Datenbestand nicht wieder hergestellt werden kann, kann dies viele Ursachen haben. Es können technische Defekte vorliegen, falsche Parameter oder schlicht überalterte Medien. Auch wenn Regeln nicht eingehalten oder die Datenträger nicht richtig verwaltet werden, kann dies zu irreparablen Fehlern führen.

Um dem vorzubeugen und Fehler frühzeitig zu entdecken, muss regelmäßig geprüft werden, ob sich die gesicherten Daten problemlos und in angemessener Zeit zurückspielen lassen. Sollten Defekte oder andere Probleme auftreten, müssen diese so schnell wie möglich repariert werden.

Ebenso sollten die Verantwortlichen regelmäßig testen, ob die Datensicherung auch wie gewünscht funktioniert. Falls möglich, sollten die Programme so eingestellt werden, dass bei einem Fehler (z. B. volles Datensicherungsmedium) der zuständige Mitarbeiter automatisch informiert wird.

Weiterhin muss nach einem Patch oder Update für das Datensicherungsprogramm überprüft werden, ob die Software noch korrekt funktioniert und z. B. keine Einstellungsparameter überschrieben wurden.

CON.3.M9 Voraussetzungen für die Online-Datensicherung [IT-Betrieb, Leiter IT]

Die Erstellung einer Datensicherung mithilfe eines Online-Speicher-Dienstes wird in der Regel über eine entsprechende Anwendung auf dem Client eines Benutzers oder auf einem Server der Institution initiiert. Auch möglich ist z. B. ein hybrides Modell durch eine Appliance: Hier werden die Daten lokal auf der Appliance und zusätzlich in einem Online-Speicher-Dienst vorgehalten. In allen Fällen werden die zu sichernden Daten über das Internet von einem Rechner innerhalb der Institution auf einen Server des Online-Speicher-Anbieters übertragen.

Je nach Anbieter kann der Umgang mit den übertragenen Daten dabei variieren. Ein Großteil der Anbieter unterstützt beispielsweise die Speicherung und Wiederherstellung unterschiedlicher Versionen einer zu übertragenden Datei. Bietet der Online-Speicher-Anbieter hingegen keine Versionierung von Dateien an, wird die ältere Datei ohne zusätzliche Rückfrage überschrieben und ist damit nicht mehr für eine Rücksicherung verfügbar. In diesem Fall erfüllt der Online-Speicher jedoch nicht die Anforderungen, die an eine Datensicherung im Unternehmens- oder Behördenumfeld gestellt werden. Institutionen sollten daher insbesondere auf die vorhandene Versionierung der Daten achten, um dem unerwünschten Löschen älterer Datenversionen vorzubeugen.

Grundsätzlich sollten immer die Fragen im Vordergrund stehen, welchen Schutzbedarf die gesicherten Daten haben, welchen gesetzlichen Verpflichtungen hinsichtlich der geschäftsrelevanten Daten eine Institution unterliegt und wie es sich auswirkt, wenn Daten verloren gehen oder durch Unbefugte verändert werden.

Viele Anbieter von Online-Speicher-Diensten sind sich durchaus bewusst, dass Institutionen großen Wert auf die Verfügbarkeit ihrer Daten legen und halten die Daten ihrer Kunden redundant vor. Institutionen sollten darauf achten, dass der Anbieter die Daten an unterschiedlichen Standorten bzw. in räumlich voneinander getrennten Rechenzentren speichert. Kommt es zu Problemen in einem Rechenzentrum, stehen die Daten in diesem Fall dennoch weiterhin in einem anderen Rechenzentrum zur Verfügung.

Unternehmen und Behörden sollten nicht nur Wert auf die sichere Speicherung ihrer Daten legen, sondern darüber hinaus auch die Umsetzung der Zugriffsmöglichkeiten auf die angelegten Benutzerkonten hinterfragen. Im Unternehmens- und Behördenumfeld sind gezielte Angriffe vorstellbar, deren Absicht darin liegt, eine Sperrung des Benutzerkontos herbeizuführen und auf diesem Weg den Zugriff auf das Backup der Daten zu verhindern. Eine solche Denial-of-Service-Attacke bedient sich dabei in der Regel unterschiedlicher Schwachstellen wie beispielsweise einer Kombination aus der automatischen Sperrung eines Benutzerkontos bei fehlgeschlagenen Anmeldeversuchen und einer nicht validierten E-Mail-Adresse. Als Schutzmaßnahme kann das Time-Out-Prinzip einem solchen gezielten Denial-of-Service-Angriff entgegenwirken. Dabei wird das Benutzerkonto nicht vollständig gesperrt, sondern lediglich ein erneuter Anmeldeversuch für einen vorgegebenen Zeitraum unterbunden.

Nicht nur Vollständigkeit und Verfügbarkeit ihrer gesicherten Daten interessieren Institutionen, vielmehr legen sie, unter anderem zur Vermeidung rechtlicher Konsequenzen oder eines Imageverlustes, auch großen Wert auf deren Vertraulichkeit und Integrität. Institutionen sollten daher Verschlüsselungsverfahren einsetzen, um das Sicherheitsniveau bei der Übermittlung und der Datenspeicherung bei externen Dienstleistern zu erhöhen.

Viele Anbieter von Online-Speicher-Lösungen werben mit der erhöhten Sicherheit durch Verschlüsselung. Hier muss jedoch genauer analysiert werden, wie die Verschlüsselung konkret umgesetzt ist. In der Regel erfolgt nämlich lediglich die eigentliche Übertragung der Daten verschlüsselt, etwa über den Aufbau einer https-Verbindung (Hyper Text Transfer Protocol Secure). Vor und nach dem Transport liegen die Daten jedoch unverschlüsselt im Klartext vor. Einige Anbieter stellen ihren Kunden, unabhängig vom Transportweg der Daten, zusätzliche Verschlüsselungsmethoden zur Verfügung. Allerdings kann die Institution dabei oft nicht ausschließen, dass sich ein Innentäter, also ein Mitarbeiter des Online-Speicher-Anbieters, die entsprechenden Schlüssel verschafft und damit auch auf die verschlüsselten Informationen zugreifen, diese verfälschen oder veröffentlichen kann. Erlangt ein Angreifer Zugriff auf die Daten, indem er die Authentisierung kompromittiert, dann ist die Verschlüsselung beim Anbieter ebenfalls wirkungslos.

Sehen Institutionen ihre Daten also als besonders schützenswert an, sollten sie diese bereits auf ihren eigenen Systemen und damit vor dem eigentlichen Datentransfer verschlüsseln.

Das Bedürfnis nach einer sicheren Methode zur Nutzung von Online-Speicher-Lösungen, gerade im Behörden- oder Unternehmensumfeld, wird vom Markt jedoch zunehmend aufgegriffen. So hat sich mittlerweile eine Reihe von Verschlüsselungslösungen etabliert, die größtenteils speziell auf die Zusammenarbeit mit Online-Speicher-Diensten abgestimmt sind. Die Programme überprüfen bereits bei der Installation, ob ein passender Ordner eines Online-Speichers existiert, und erzeugen anschließend einen entsprechenden Unterordner, in dem die verschlüsselten Dateien abgelegt werden. Institutionen, die zusätzliche Verschlüsselungssoftware einsetzen, sollten darauf achten, dass für die Anwendung ein ausreichend starkes Passwort oder anderer Zugriffsschutz gewählt wird. Zudem sollte eine Kopie der eingesetzten Softwarelösung und der zugehörigen kryptografischen Schlüssel an einem sicheren Ort hinterlegt werden, um im Falle eines vollständigen Datenverlustes innerhalb der Institution noch auf die verschlüsselten Datensicherungen des Online-Speichers zugreifen zu können. Zu diesem Zweck kann die Verschlüsselungssoftware unverschlüsselt beim Online-Speicher-Dienst gesichert werden, der Schlüssel muss selbstverständlich anders gesichert werden. Auf diesem Weg ist die Institution unabhängig davon, ob die Verschlüsselungssoftware auch nach einem längeren Zeitraum noch in einer kompatiblen Version zur Verfügung steht.

Institutionen sollten sich zudem davon überzeugen, dass die Wiederherstellung der gespeicherten Daten vom Online-Speicher fehlerfrei funktioniert, und sollten dies darüber hinaus regelmäßig testen (siehe CON.3.A8 *Funktionstests und Überprüfung der Wiederherstellbarkeit*).

CON.3.M10 Verpflichtung der Mitarbeiter zur Datensicherung

Alle Benutzer sollten über die Regelungen zur Datensicherung informiert sein, um gegebenenfalls auf Unzulänglichkeiten (zum Beispiel zu geringes Zeitintervall für ihren Bedarf) hinweisen oder individuelle Ergänzungen vornehmen zu können (zum Beispiel zwischenzeitliche Spiegelung wichtiger Daten auf der eigenen Platte).

Auch die Information der Benutzer darüber, wie lange die Daten wieder einspielbar sind, ist wichtig. Werden zum Beispiel bei wöchentlicher Komplettsicherung nur zwei Generationen aufbewahrt, bleiben abhängig vom Zeitpunkt des Verlustes nur zwei bis drei Wochen Zeit, um die Daten wieder einzuspielen.

Mitarbeiter, die Aufgaben bei der Erstellung von Datensicherungen wahrnehmen sollen, sollten darüber informiert und darauf verpflichtet werden, dabei das Datensicherungskonzept bzw. das Minimaldatensicherungskonzept sorgfältig einzuhalten. Das ist vor allem dort wichtig, wo zentral durchgeführte Datensicherungen nicht greifen, also z. B. bei nicht-vernetzten oder mobilen Endgeräten. Die Mitarbeiter sollten regelmäßig an die Datensicherung erinnert und dazu motiviert werden.

CON.3.M11 Sicherungskopie der eingesetzten Software [IT-Betrieb]

Bei Problemen mit IT-Systemen ist es oft nötig, die eingesetzten Betriebssysteme und Anwendungen zeitnah neu installieren zu können. Hierfür müssen alle Dateien, die zur Installation benötigt werden, vorliegen. Daher ist es erforderlich, Kopien anzufertigen und an geeigneter Stelle zu archivieren.

Wird die Software auf Datenträgern (z. B. DVDs oder USB-Sticks) ausgeliefert, sollte von den Originaldatenträgern bzw. von der Originalsoftware bei Eigenentwicklungen eine Sicherungskopie erstellt werden, von der die Software wieder eingespielt werden kann. Die Originaldatenträger und die Sicherungskopien sind getrennt voneinander aufzubewahren.

Insbesondere Anwendungen werden oft nicht auf Datenträgern ausgeliefert, sondern nur als separate Installationsdateien, als Bestandteil einer Paket- oder Softwareverwaltung oder als Quelltextpakete. Auch diese Installationsquellen sollten an einem geeigneten Ort hinterlegt werden.

Um kostenpflichtige Betriebssysteme oder Anwendungen zu installieren, müssen oft Lizenznummern während der Installation eingegeben werden. Deshalb ist es nötig, dass neben den Installationsquellen auch die Lizenznummern geeignet hinterlegt werden. Ein unerlaubter Zugriff auf die Installationsmedien und die Lizenznummern muss ausgeschlossen sein.

Wurde die Software aus Quelltexten übersetzt, so sollte die Dokumentation sämtliche beim Übersetzen verwendeten Optionen (insbesondere die Optionen, mit denen ein etwaiges Skript *configure* aufgerufen wurde) enthalten. Wurde die Software aus einem Binärpaket installiert, so sollten alle Schritte dokumentiert werden, mit denen die Installation später nachvollzogen werden kann.

Jede Änderung an einer Konfigurationsdatei sollte dokumentiert werden. Es empfiehlt sich, eine Versionsverwaltung einzusetzen. Zusätzlich müssen alle Konfigurationsdateien regelmäßig gesichert werden.

CON.3.M12 Geeignete Aufbewahrung der Backup-Datenträger [IT-Betrieb]

Backup-Datenträger unterliegen besonderen Anforderungen hinsichtlich ihrer Aufbewahrung:

- Der Zugriff auf diese Datenträger darf nur befugten Personen möglich sein.
- Ein ausreichend schneller Zugriff muss im Bedarfsfall gewährleistet sein.
- Der Aufbewahrungsort muss auch die klimatischen Bedingungen für eine längerfristige Aufbewahrung von Datenträgern gewährleisten.
- Für den Notfall müssen die Backup-Datenträger räumlich getrennt vom gesicherten IT-System aufbewahrt werden, wenn möglich in einem anderen Brandabschnitt.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

CON.3.M13 Einsatz kryptografischer Verfahren bei der Datensicherung [IT-Betrieb] (CIA)

Der Vertraulichkeitsbedarf einer Datei überträgt sich bei einer Datensicherung auf die Sicherungskopie. Daher sollte bei erhöhtem Schutzbedarf die Sicherung verschlüsselt werden.

Für die Datensicherungen müssen geeignete Verschlüsselungsverfahren ausgewählt werden. Das entscheidende Merkmal eines Verschlüsselungsverfahrens ist die Güte des Algorithmus sowie der Schlüsselauswahl. Da die Sicherheitseignung der Verschlüsselungsverfahren durch die technische Entwicklung von Hard- und Software sowie Fortschritte in der Kryptografie beschränkt wird, müssen sie regelmäßig nach dem Stand der Technik aktualisiert werden.

Auch muss sichergestellt sein, dass die Schlüssel geeignet verwaltet werden.

Weitere Hinweise zu kryptografischen Verfahren finden sich im Baustein CON.1 *Kryptokonzept*.

3 Weiterführende Informationen

3.1 Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Datensicherungskonzept" finden sich unter anderem in folgenden Veröffentlichungen:

[27001] ISO/IEC 27001:2013

Information technology-Security techniques-Information security management systems-Requirements, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/SC 27, Oktober 2013

[BKBU] Leitfaden Backup / Recovery / Disaster Recovery

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom), Dezember 2016, https://www.bitkom.org/noindex/Publikationen/2017/Leitfaden/170125-LF-Backup-Recovery.pdf, zuletzt abgerufen am 05.10.2018

[ISF] The Standard of Good Practice for Information Security:

Information Security Forum (ISF), June 2018

[NIST80053] Security and Privacy Controls for Federal Information Systems and Organizations

NIST Special Publication 800-53, Revision 4, April 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf , zuletzt abgerufen am 30.08.2018

Umsetzungshinweise zum Baustein CON.4 Auswahl und Einsatz von Standardsoftware

1 Beschreibung

1.1 Einleitung

Unter Standardsoftware wird Software verstanden, die auf dem Markt angeboten und meistens über den Fachhandel bezogen wird, zum Beispiel über Kataloge oder Onlineportale. Sie zeichnet sich dadurch aus, dass sie der Anwender selbst installieren und mit wenig Aufwand anpassen kann.

In diesen Umsetzungshinweisen zum entsprechenden Baustein wird dargestellt, wie Institutionen unter Sicherheitsgesichtspunkten mit Standardsoftware umgehen sollten. So müssen Institution einen Anforderungskatalog für Standardsoftware erstellen, ein geeignetes Produkt auswählen, es sicher installieren, die Lizenzen geeignet verwalten und das Produkt auch wieder sicher deinstallieren können.

1.2 Lebenszyklus

Planung und Konzeption

In der Planungs- und Konzeptionsphase sollte ein für die Beschaffung der Standardsoftware verantwortlicher Mitarbeiter benannt werden (siehe CON.4.M4 *Festlegung der Verantwortlichkeiten im Bereich Standardsoftware*). Die Anforderungen an die zu beschaffende Standardsoftware sollten analysiert und in einem Anforderungskatalog festgehalten werden (CON.4.M5 *Erstellung eines Anforderungskatalogs für Standardsoftware*). Danach kann ein geeignetes Produkt ausgewählt werden (CON.4.M6 *Auswahl eines geeigneten Softwareproduktes*). Bei erhöhtem Schutzbedarf sollte zusätzlich entschieden werden, ob und wie eine zu beschaffende Anwendung zertifiziert sein sollte, um ein gewisses Sicherheitsniveau nachzuweisen (siehe CON.4.M11 *Nutzung zertifizierter Standardsoftware*).

Beschaffung

Bei der Beschaffung von Standardsoftware sollte definiert werden, wie mit deren Lieferungen verfahren wird. So sollte bei jeder Lieferung überprüft werden, ob sie vollständig ist (siehe CON.M7 *Überprüfung der Lieferung von Standardsoftware*).

Umsetzung

Vor dem Einsatz von Standardsoftware sollte sichergestellt werden, dass die Integrität der Installationssoftware gewährleistet ist (siehe CON.4.M1 *Sicherstellen der Integrität von Standardsoftware*). Darüber hinaus sollte Standardsoftware sicher installiert und danach konfiguriert werden (siehe CON.4.M3 *Sichere Installation und Konfiguration von Standardsoftware*). Für jede Anwendung ist außerdem eine Installationsanweisung zu erstellen (siehe CON.4.M2 *Entwicklung der Installationsanweisung für Standardsoftware*).

Betrieb

Es sollte sichergestellt werden, dass ausschließlich lizenzierte Standardsoftware eingesetzt wird (siehe CON.4.M8 *Lizenzverwaltung und Versionskontrolle von Standardsoftware*). Bei erhöhtem Schutzbedarf sollten gegebenenfalls ergänzende Sicherheitsfunktionen implementiert werden (siehe CON.4.M10 *Implementierung zusätzlicher Sicherheitsfunktionen*). Auch sollten dann Verschlüsselung, Checksummen oder digitale Signaturen eingesetzt werden (siehe CON.4.M12 *Einsatz von Verschlüsselung, Checksummen oder digitalen Signaturen*).

Aussonderung

Wenn Standardsoftware deinstalliert wird, sollte dafür gesorgt werden, dass alle (System-)Dateien der Anwendung gelöscht werden (siehe CON.4.M9 *Deinstallation von Standardsoftware*).

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Auswahl und Einsatz von Standardsoftware" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

CON.4.M1 Sicherstellen der Integrität von Standardsoftware

Es ist sicherzustellen, dass freigegebene Standardsoftware nur vom Originaldatenträgern oder von geprüften identischen Kopien des originalen Installationsprogramms installiert wird. Damit soll verhindert werden, dass gewollte oder ungewollte Veränderungen vorgenommen werden können, z. B. durch Malware, Bitfehler aufgrund technischer Fehler oder manipulierten Konfigurationsdateien.

Die Installation darf daher ausschließlich von Originaldatenträgern bzw. geprüften identischen Kopien des originalen Installationsprogramms erfolgen. Alternativ kann eine freigegebene Version über ein lokales Netz installiert werden. Dabei sollte sichergestellt sein, dass nur berechtigte Personen darauf zugreifen können.

Von den Originaldatenträgern sollten Sicherungskopien angefertigt und geprüft werden. Originaldatenträger und alle Kopien müssen vor unberechtigtem Zugriff geschützt aufbewahrt werden. Die angefertigten Kopien sollten nummeriert und in Bestandsverzeichnisse aufgenommen werden. Kopien, die nicht mehr benötigt werden, sollten gelöscht oder vernichtet werden. Auch Originaldatenträger und originale Installationsprogramme müssen vor der ersten Verwendung auf Schadprogramme geprüft werden.

Optional kann über die Originaldatenträger oder über eine während des Tests installierte Referenzversion eine Checksumme gebildet werden. Anhand dieser kann vor der Installation die Integrität der dafür eingesetzten Datenträger bzw. der in lokalen Netzen hinterlegten Versionen oder die korrekte Installation überprüft werden. Darüber hinaus können installierte Programme zusätzlich zum Schutz vor unberechtigten Veränderungen der freigegebenen Konfiguration mit Checksummen versehen werden. Auf diese Weise können auch Infektionen mit bisher unbekannter Schadsoftware erkannt werden. So kann auch festgestellt werden, ob eine Vireninfektion vor oder nach der Installation stattgefunden hat.

CON.4.M2 Entwicklung der Installationsanweisung für Standardsoftware

Nachdem sich die Institution für ein Produkt entschieden hat, muss dafür eine Installationsanweisung erstellt werden. Während des Testens wurde diejenige Konfiguration des Produktes ermittelt, die einen sicheren und effizienten Produktionsbetrieb erlaubt (siehe CON.4.M6 *Auswahl einer geeigneten Standardsoftware*). Damit sollte sichergestellt werden, dass die Software benutzerfreundlich, ordnungsmäßig und sicher am Arbeitsplatz funktioniert.

Um die geeignete Konfiguration des Produktes im Produktivbetrieb sicherzustellen, müssen bestimmte Parameter vorgegeben werden. Teilweise muss dies durch organisatorische Regelungen begleitet werden.

Für einige Eigenschaften eines Produktes wird im folgenden beispielhaft aufgezeigt, was in einer Installationsanweisung vorgegeben werden kann.

Beispiel:

Benutzerfreundlichkeit:

- Mit dem Produkt sind die jeweiligen Treiber zu installieren, um eine für den Benutzer akzeptable Arbeitsumgebung zu schaffen, z. B. Bildschirm flimmerfrei, genügende Druckaufbereitung.
- Einstellungen, bei denen die Funktionen die größte Verarbeitungsgeschwindigkeit haben, sind vorzuziehen, wenn nicht andere Kriterien wie Sicherheit dagegen sprechen (Beispiel: eine Datensicherung sollte verifiziert werden, obwohl die Verifikation zusätzlichen Zeitaufwand erfordert).

Sicherheit:

- Die Parameter für Sicherheitsfunktionen sind voreinzustellen, z. B. die Mindestlänge von Passwörtern oder die tägliche Erstellung von Datensicherungen.
- Werden mehrere sicherheitsrelevante Verfahren unterstützt (z. B. Verschlüsselungsalgorithmus, Hash-Funktionen), sind diejenigen auszuwählen, mit denen ein angemessenes Schutzniveau erreicht wird.

Funktion:

- Nur die benötigten Programmfunktionen sind zu aktivieren, unerwünschte oder nicht benötigte Funktionen sind abzuschalten.
- Die Funktion zur automatischen Speicherung ist mit dem Parameter "alle x Minuten" zu aktivieren.

Organisation:

- Ausschließlich ein Administrator darf die Software installieren.
- Es müssen Regelungen für den Betrieb erlassen werden, z. B. Datensicherungen sind eigenverantwortlich vom Benutzer durchzuführen, Passwörter müssen nach x Tagen gewechselt werden.

Randbedingungen:

- Die Konfiguration der Plattform, auf der das Standardsoftwareprodukt eingesetzt werden soll, muss insbesondere dann beschrieben und vorgegeben werden, wenn systembedingte Schwachstellen der Plattform damit beseitigt werden.

CON.4.M3 Sichere Installation und Konfiguration von Standardsoftware

Die Standardsoftware sollte entsprechend der Installationsanweisung (siehe CON.4.M2 *Entwicklung der Installationsanweisungen für Standardsoftware*) auf den vorgesehenen IT-Systemen installiert werden. Die Installationsanweisung beinhaltet neben den zu installierenden Programmen auch Konfigurationsparameter und die Einrichtung der Hardware- und Softwareumgebung.

Abweichungen von der Installationsanweisung müssen vom Vorgesetzten bzw. vom Mitarbeiter, der für den Freigabeprozess verantwortlich ist, genehmigt werden.

Da Standardsoftware für viele Einsatzfelder entwickelt wird, enthält sie meist mehr Funktionen als für die Fachaufgaben benötigt werden. Damit es zu weniger Problemen und Fehlern kommt, dürfen nur die tatsächlich benötigten Funktionen installiert werden. Funktionen, die zu Sicherheitsproblemen führen können, dürfen nicht freigegeben werden.

Sowohl vor als auch nach der Installation von Software sollte eine vollständige Datensicherung durchgeführt werden. Die erste Datensicherung kann benutzt werden, wenn es während der Installation zu Fehlern kommt. Mit der zweiten Datensicherung lässt sich bei späteren Problemen der Zustand nach der erfolgreichen Installation des Produktes wiederherstellen.

Die erfolgreiche Installation muss an die zuständige Stelle für den Produktivbetrieb gemeldet werden.

Beim Einsatz eines neuen Produktes müssen eventuell Datenbestände migriert werden, die mit einem Vorgängerprodukt erzeugt wurden. Hat sich bei den Tests gezeigt, dass es dabei zu Schwierigkeiten kommen kann, sind Hilfestellungen für die Benutzer zu erarbeiten. Alternativ kann auch geschultes Personal die alten Datenbestände zentral migrieren.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Auswahl und Einsatz von Standardsoftware".

CON.4.M4 Festlegung der Verantwortlichkeiten im Bereich Standardsoftware [Fachabteilung]

Vor der Einführung von Standardsoftware müssen eine Reihe von Verantwortlichkeiten geregelt werden, z. B.:

- Wer erstellt einen Anforderungskatalog?
- Wer wählt Produkte aus?
- Wer testet? Wer ist für die Freigabe zuständig?
- Wer installiert die Software?

Nachfolgend wird aufgezeigt, wie sich diese Verantwortlichkeiten sinnvoll verteilen lassen. Da jedoch die Bezeichnungen in den meisten Institutionen voneinander abweichen, werden vorab einige Instanzen anhand ihrer Aufgaben definiert, denen anschließend die einzelnen Verantwortlichkeiten zugeordnet werden können:

- Der Fachbereich ist der Anwender der Standardsoftware. Er äußert den Bedarf an neuer Software und stößt damit den Beschaffungsprozess an. Er wird bei Vorauswahl und Test beteiligt, um die Anforderungen der Benutzer einzubringen.
- Die Leitung der Institution ist dafür verantwortlich, Standardsoftware freizugeben. Diese Verantwortung wird meist an den Leiter der Fachabteilung delegiert. Damit geht nach der Freigabe die Verantwortung für den korrekten Einsatz der Standardsoftware auf die Fachabteilung über.
- Der IT-Bereich hat die Aufgabe, IT-Lösungen bereitzustellen, mit denen die Fachabteilungen ihre Aufgaben erfüllen können. Außerdem muss er den sicheren und zuverlässigen Betrieb der IT gewährleisten.
- Die Beschaffungsstelle muss sicherstellen, dass die Standardsoftware interoperabel und kompatibel ist. Auch muss sie dafür sorgen, dass Hausstandards und gesetzliche Vorschriften eingehalten werden. Oft gibt es in den einzelnen Fachabteilungen IT-Koordinatoren, die Teile der Aufgaben der Beschaffungsstelle für die Fachabteilung beratend wahrnehmen und eventuell auch die Haushaltsmittel der Fachabteilung koordinieren.
- Der Haushalt ist verantwortlich für das Rechnungswesen, die IT-Budgetverwaltung und für die Bereitstellung der benötigten Haushaltsmittel.
- Der IT-Sicherheitsbeauftragte muss überprüfen, ob mit den eingesetzten oder zu beschaffenden Produkten ein angemessenes Sicherheitsniveau gewährleistet werden kann. Im Rahmen des Sicherheitsmanagements muss er die Informationssicherheit im laufenden Betrieb sicherstellen.
- Der Datenschutzbeauftragte muss sicherstellen, dass die datenschutzrechtlichen Bestimmungen eingehalten werden und personenbezogene Daten ausreichend geschützt sind.
- Der Personal- bzw. Betriebsrat muss in vielen Fällen bei der Auswahl neuer Standardsoftware beteiligt werden, insbesondere wenn damit größere Änderungen im Arbeitsablauf verbunden sind oder wenn die zu beschaffende Software zur Leistungskontrolle geeignet ist.

Im Gesamtprozess "Standardsoftware" muss für jeden einzelnen Schritt festgelegt werden, welche der zuvor beschriebenen Instanzen für die Durchführung verantwortlich sind und welche Instanzen dabei beteiligt werden müssen. Die nachfolgende Tabelle zeigt, wie Verantwortung sinnvoll verteilt werden kann.

	Verantwortlich	Zu beteiligen
Erstellung des Anforderungskatalogs	Fachabteilung, IT-Bereich	Beschaffungsstelle, Haushalt, IT-Sicherheitsbeauftragter, Datenschutzbeauftragter, Personal- oder Betriebsrat
Vorauswahl eines geeigneten Produktes	Beschaffungsstelle	IT-Bereich, Fachabteilung
Testen	Fachabteilung und IT-Bereich	IT-Sicherheitsbeauftragter, Datenschutzbeauftragter, Personal- oder Betriebsrat
Freigabe	Leitung der Institution, meist delegiert an Leiter Fachabteilung	-
Beschaffung	Beschaffungsstelle	Haushalt
Sicherstellen der Integrität der Software	IT-Bereich	-
Installation und Konfiguration	IT-Bereich	-
Versionskontrolle und Lizenzverwaltung	IT-Bereich	-
Deinstallation	IT-Bereich	-
Kontrolle des IT-Betriebs	IT-Sicherheitsbeauftragter	-

Die getroffenen Zuordnungen sind verbindlich festzuschreiben und es ist regelmäßig zu kontrollieren, ob sie eingehalten werden.

CON.4.M5 Erstellung eines Anforderungskatalogs für Standardsoftware [Fachabteilung]

Der Markt bietet meist viele gleichartige Standardsoftwareprodukte an. In ihrer Grundfunktion vergleichbar, unterscheiden sie sich jedoch in Kriterien wie Anschaffungs- und Betriebskosten, Zusatzfunktionen, Kompatibilität, Administration, Ergonomie und Informationssicherheit.

Anforderungskatalog

Für die Auswahl eines geeigneten Produktes sollte daher zunächst ein Anforderungskatalog erstellt werden, der z. B. Aussagen zu den folgenden Punkten Aussagen enthalten kann:

- Funktionale Anforderungen, die das Produkt erfüllen muss, um die Fachabteilung geeignet zu unterstützen. Die für die Fachaufgabe relevanten Funktionen sollten hervorgehoben werden. Beispiel:
    - Textverarbeitung mit den Zusatzfunktionen: Einbinden von Grafiken, Makro-Programmierung, Rechtschreibprüfung und Silbentrennung. Makro-Programmierung muss abschaltbar sein, Rechtschreibprüfung muss in Englisch, Französisch und Deutsch verfügbar sein. Die spezifizierten Textformate müssen im- und exportiert werden können.
- IT-Einsatzumgebung: Diese wird einerseits beschrieben durch die Rahmenbedingungen, die durch die vorhandene oder geplante IT-Einsatzumgebung vorgegeben werden, und andererseits durch die Leistungsanforderungen, die das Produkt an die Einsatzumgebung stellt. Beispiel:
    - Erforderliche IT-Einsatzumgebung und Leistungsanforderungen: Betriebssystem, Prozessor, Hauptspeicher, Festplattenkapazität, Schnittstellen für externe Datenträger und für Vernetzung.
- Kompatibilitätsanforderungen zu anderen Programmen oder IT-Systemen, also Migrationsunterstützung und Aufwärts- und Abwärtskompatibilität. Beispiel:
    - Die Funktionen A, B, C müssen bei Versionswechseln erhalten bleiben.
- Performance-Anforderungen beschreiben die erforderlichen Leistungen hinsichtlich Durchsatz und Laufzeitverhalten. Für die geforderten Funktionen sollten möglichst genaue Angaben über die maximal zulässige Bearbeitungszeit getroffen werden.Beispiel:
    - Andere gleichzeitig verarbeitete Prozesse dürfen durch das Produkt maximal um 30 % verlangsamt werden.
- Interoperabilitätsanforderungen, d. h. die Zusammenarbeit mit anderen Produkten über Plattformgrenzen hinweg muss möglich sein. Beispiel:
    - Ein Textverarbeitungsprogramm sollte für Windows-, Unix- und macOS-Plattformen verfügbar sein. Dokumente sollen auf einem Betriebssystem erstellt und auf einem anderen weiterverarbeitet werden können.
- Zuverlässigkeitsanforderungen betreffen die Stabilität des Produktes, also Fehlererkennung und Toleranz sowie Ausfall- und Betriebssicherheit.Beispiel:
    - Fehleingaben des Benutzers müssen erkannt werden und dürfen nicht zum Programmabbruch oder Systemabsturz führen.
- Konformität zu Standards, das können internationale Normen, De-facto-Standards oder auch Hausstandards sein. Beispiel:
    - Das Produkt muss der EU-Bildschirmrichtlinie 90/270/EWG entsprechen.
- Einhaltung von internen Regelungen und gesetzlichen Vorschriften. Beispiel:
    - Da personenbezogene Daten verarbeitet werden, müssen die Bestimmungen des Bundesdatenschutzgesetzes mit den verfügbaren Funktionen erfüllt werden können.
- Anforderungen an die Benutzerfreundlichkeit, die durch die leichte Bedienbarkeit, Verständlichkeit und Erlernbarkeit gekennzeichnet ist, also insbesondere durch die Güte der Benutzeroberfläche sowie die Qualität der Benutzerdokumentation und der Hilfefunktionen. Beispiel:
    - Die Benutzeroberfläche muss so gestaltet sein, dass ungelernte Kräfte innerhalb von zwei Stunden in die Benutzung eingewiesen werden können.
- Anforderungen an die Wartung ergeben sich für den Anwender hauptsächlich aus der Fehlerbehandlung des Produktes.Beispiel:
    - Der Administrationsaufwand darf X Stunden pro Monat nicht überschreiten.
- Die Obergrenze für Kosten. Dabei müssen nicht nur die unmittelbaren Beschaffungskosten für das Produkt selber einbezogen werden, sondern auch Folgekosten, wie z. B. eine Aufrüstung der Hardware, Personalkosten oder notwendige Schulungen.
- Aus den Anforderungen an die Dokumentation muss hervorgehen, welche Dokumente in welcher Güte (Vollständigkeit, Verständlichkeit) erforderlich sind.Beispiele:
    - Die Benutzerdokumentation muss leicht nachvollziehbar und zum Selbststudium geeignet sein. Die gesamte Funktionalität des Produktes ist zu beschreiben.
- Bezüglich der Softwarequalität können Anforderungen gestellt werden, die von Herstellererklärungen zum eingesetzten Qualitätssicherungsverfahren, über ISO 9000 ff. Zertifikate bis hin zu unabhängigen Softwareprüfungen nach ISO/IEC 25051 reichen. Beispiel:
    - Der Software-Herstellungsprozess des Herstellers muss nach ISO 9001 zertifiziert sein.
- Sollen durch das Produkt selbst Sicherheitsaufgaben erfüllt werden, sind diese in Form von Sicherheitsanforderungen zu formulieren. Dies wird im Folgenden erläutert.

Sicherheitsanforderungen

Typische Sicherheitsanforderungen, die ein Produkt erfüllen kann, werden im Folgenden kurz erläutert. Weitere Ausführungen dazu sind in den Common Criteria (CC) zu finden.

- Identifizierung und Authentisierung: Zu vielen Produkten wird es Anforderungen geben, diejenigen Benutzer zu bestimmen und zu überwachen, die Zugriff auf das Produkt haben. Dazu muss nicht nur die Identität des Benutzers überprüft, sondern auch nachgeprüft werden, ob der Benutzer tatsächlich die Person ist, die er zu sein vorgibt. Das geschieht, indem der Benutzer dem Produkt Informationen liefert, die fest mit dem betreffenden Benutzer verknüpft sind.
- Zugriffskontrolle: Bei vielen Produkten wird es erforderlich sein, sicherzustellen, dass Benutzer daran gehindert werden, auf Informationen zuzugreifen, für die sie kein Zugriffsrecht haben oder auf die sie nicht zugreifen sollen. Weiterhin wird es eventuell erforderlich sein, zu verhindern, dass Benutzer unbefugt Informationen erzeugen, ändern oder löschen.
- Beweissicherung: Bei vielen Produkten muss sichergestellt werden, dass die Handlungen der Benutzer aufgezeichnet werden. So können die Folgen später dem betreffenden Benutzer zugeordnet werden und der Benutzer kann für seine Handlungen verantwortlich gemacht werden.
- Protokollauswertung: Bei vielen Produkten wird sicherzustellen sein, dass sowohl über gewöhnliche Vorgänge als auch über außergewöhnliche Vorfälle ausreichend Informationen aufgezeichnet werden, damit später festgestellt werden kann, ob tatsächlich Sicherheitsverletzungen vorgelegen haben und welche Informationen oder sonstigen Betriebsmittel davon betroffen waren.
- Unverfälschbarkeit: Bei vielen Produkten wird es erforderlich sein, sicherzustellen, dass bestimmte Beziehungen zwischen unterschiedlichen Daten korrekt bleiben und dass Daten zwischen einzelnen Prozessen ohne Änderungen übertragen werden. Daneben müssen auch Funktionen bereitgestellt werden, die es bei der Übertragung von Daten zwischen einzelnen Prozessen, Benutzern und Objekten ermöglichen, Verluste, Ergänzungen oder Veränderungen zu entdecken bzw. zu verhindern, und die es unmöglich machen, die angebliche oder tatsächliche Herkunft bzw. Bestimmung der Datenübertragung zu ändern.
- Zuverlässigkeit: Bei vielen Produkten wird es erforderlich sein, sicherzustellen, dass zeitkritische Aufgaben genau zu dem Zeitpunkt durchgeführt werden, zu dem es erforderlich ist, also nicht früher oder später. Auch wird sicherzustellen sein, dass zeitunkritische Aufgaben nicht in zeitkritische umgewandelt werden können. Desgleichen wird es bei vielen Produkten erforderlich sein sicherzustellen, dass ein Zugriff im erforderlichen Moment möglich ist und Betriebsmittel nicht unnötig angefordert oder zurückgehalten werden.
- Übertragungssicherheit: Dieser Begriff umfasst alle Funktionen, die für den Schutz der Daten während der Übertragung über Kommunikationskanäle vorgesehen sind: Authentisierung, Zugriffskontrolle, Datenvertraulichkeit, Datenintegrität, Sende- und Empfangsnachweis. Einige dieser Funktionen werden mittels kryptografischer Verfahren realisiert.

Darüber hinaus können weitere Sicherheitsanforderungen an Standardsoftware konkretisiert werden.

- Datensicherung: An die Verfügbarkeit der mit dem Produkt verarbeiteten Daten werden besondere Anforderungen gestellt. Darunter fallen im Produkt integrierte Funktionen, die Datenverlusten vorbeugen sollen, z. B. die automatische Speicherung von Zwischenergebnissen oder die automatische Erstellung von Sicherungskopien, bevor größere Änderungen durchgeführt werden.
- Verschlüsselung: Bei vielen Produkten wird es erforderlich sein, Nutzdaten vor einer Übertragung oder nach der Bearbeitung zu verschlüsseln und sie nach Empfang oder vor der Weiterverarbeitung wieder zu entschlüsseln. Hierzu ist ein anerkanntes Verschlüsselungsverfahren zu verwenden. Es ist sicherzustellen, dass die zur Entschlüsselung benötigten Parameter (z. B. Schlüssel) geeignet geschützt sind.
- Funktionen zur Wahrung der Datenintegrität: Für Daten, deren Integritätsverlust zu Schäden führen kann, können Funktionen eingesetzt werden, die Fehler erkennen lassen oder mittels Redundanz korrigieren können. Meist werden Verfahren zur Integritätsprüfung eingesetzt, die zuverlässig aufdecken können, ob ein Produkt oder die damit erstellten Daten absichtlich manipuliert oder Daten unbefugt wieder eingespielt wurden.
- Datenschutzrechtliche Anforderungen: Wenn mit dem Produkt personenbezogene Daten verarbeitet werden sollen, sind über die genannten Sicherheitsfunktionen hinaus zusätzliche spezielle technische Anforderungen zu stellen, um den Datenschutzbestimmungen genügen zu können.

Sicherheitsfunktionen werden durch Mechanismen umgesetzt. Je nach Einsatzzweck müssen diese Mechanismen eine unterschiedliche Stärke besitzen, mit der sie Angriffe abwehren können. Die erforderliche Stärke der Mechanismen ist im Anforderungskatalog anzugeben. Bei Anwendung der Common Criteria (CC) wird die Angriffsresistenz eines IT-Produktes bewertet, das in einer bestimmten Einsatzumgebung betrieben wird. Kriterien für die Bewertung sind die in den Sicherheitsvorgaben oder in einem Schutzprofil definierten Bedrohungen der zu schützenden Datenobjekte. Die geforderte Prüftiefe beinhaltet die Festlegung der Angriffsresistenz und richtet sich nach dem Schutzbedarf und dem Einsatzzweck des Produktes. Die Prüftiefe wird anhand eines Kataloges (siehe CC, Teil 3) meist mittels vordefinierter Evaluierungsstufen (EAL 1 bis 7) festgelegt.

Für die Bewertung der Angriffsresistenz werden die für das Einsatzszenario relevanten Angriffe nach dem Stand der Technik bis zu einer bestimmten Stärke unter Berücksichtigung der erforderlichen Angriffszeit, technischen Expertise des Angreifers, Kenntnissen über das Produkt, Gelegenheit zum Angriff und benötigten Hilfsmittel analysiert. Die Bestätigung der Angriffsresistenz im Rahmen der Zertifizierung erfolgt dabei dann in den Abstufungen niedrig (basic), erweitert (enhanced basic), mittel (moderate) und hoch (high). Basic bedeutet Schutz gegen öffentlich bekannte Angriffe und gegen Angreifer mit sehr begrenzten Fähigkeiten und Möglichkeiten. Hoch bedeutet, dass ein erfolgreicher Angriff sehr gute Fachkenntnisse, Produktkenntnisse, Gelegenheiten und Betriebsmittel erfordert, und damit insgesamt als extrem aufwändig gilt.

CON.4.M6 Auswahl einer geeigneten Standardsoftware [Beschaffungsstelle, Fachabteilung]

Um ein geeignetes Softwareprodukt auswählen zu können, muss die IT-Abteilung in Zusammenarbeit mit der Beschaffungsstelle zuerst anhand des Anforderungskatalogs (siehe CON.4.M5 *Erstellung eines Anforderungskatalogs für Standardsoftware*) eine Marktanalyse durchführen und diese möglichst tabellarisch aufbereiten. In dieser Tabelle müssen für die infrage kommenden Produkte Aussagen zu den im Anforderungskatalog festgehaltenen Punkten gemacht werden.

Die Marktübersicht sollte mithilfe von Produktbeschreibungen, Herstelleraussagen, Fachzeitschriften oder Händlerauskünften erstellt werden. Alternativ ist eine Ausschreibung möglich und in einigen Fällen vorgegeben. Die Grundlage dafür ist der Anforderungskatalog, sodass anhand der eingehenden Angebote eine vergleichbare Marktübersicht erstellt werden kann.

Anschließend müssen die in der Marktübersicht erfassten Produkte bewertet werden. Hierzu sollte eine Bewertungsskala erarbeitet werden. Anhand der vorliegenden Informationen wird nun festgestellt, welche der geforderten Eigenschaften das Produkt aufweist. Fehlen zwingend notwendige Eigenschaften, muss es verworfen werden. Über die Bewertung der einzelnen Eigenschaften jedes Produktes wird eine Summe gebildet. Im Ergebnis liegt nun eine Rangliste der infrage kommenden Softwareprodukte vor.

Die folgende Tabelle zeigt ein Beispiel für ein solches Vorgehen. Die im Anforderungskatalog geforderten und bewerteten Eigenschaften für ein Komprimierungsprogramm werden wie folgt gewichtet:

Eigenschaft	Notwendig/Wünschenswert	Bedeutung	Produkt 1	Produkt 2	Produkt 3	Produkt 4
korrekte Kompression und Dekompression	N	10	J	J	J	J
Erkennen von Bitfehlern in einer komprimierten Datei	N	10	J	J	K.O.	J
Löschung von Dateien nur nach erfolgreicher Kompression	N	10	J	J	J	J
kompatibel zu Windows 10	N	10	J	J	J	J
kompatibel zu macOS	W	3	N	J	J	J
kompatibel zu Linux	W	3	J	J	J	N
Kompressionsrate über 40 % bei Textdateien des Programms XYZ	W	4	J	J	N	N
Online-Hilfefunktion	W	3	N	N	N	J
maximale Kosten: 50 Euro pro Lizenz	N	10	J	J	J	J
Passwortschutz für komprimierte Dateien (Mechanismenstärke hoch)	W	2	J	J	N	J
Bewertung		65 (=Max.)	59	62	K.O.	58

Im Ergebnis zeigt sich, dass Produkt 3 herausfällt, da eine notwendige Eigenschaft fehlt. Ansonsten wird die Liste angeführt von Produkt 2, gefolgt von den Produkten 1 und 4.

Die erstellte Liste muss zusammen mit der Marktübersicht der Beschaffungsstelle vorgelegt werden, damit diese überprüfen kann, inwieweit die dort aufgeführten Produkte den internen Regelungen und gesetzlichen Vorgaben entsprechen. Dabei muss die Beschaffungsstelle auch darauf achten, dass die anderen Stellen, deren Vorgaben eingehalten werden müssen, wie der Datenschutzbeauftragte, der IT-Sicherheitsbeauftragte oder der Personal- bzw. Betriebsrat, rechtzeitig beteiligt werden.

Es muss entschieden werden, wie viele und welche Kandidaten getestet werden sollen. Sinnvollerweise sollten die ersten zwei oder drei Kandidaten ausgewählt werden und daraufhin getestet werden, ob sie die wichtigsten Kriterien des Anforderungskatalogs auch tatsächlich erfüllen. Dies ist insbesondere für die notwendigen Anforderungen wichtig. Hierfür sollten Testlizenzen beschafft werden und, wie in Baustein OPS.1.1.6 *Software-Tests und -Freigaben* beschrieben, Tests durchgeführt werden.

Neben den Kriterien des Anforderungskatalogs sollten für die Entscheidung noch die folgenden Punkte berücksichtigt werden:

Referenzen

Kann der Hersteller oder Vertreiber für sein Produkt Referenzinstallationen angeben, so können die dort gemachten Erfahrungen hinterfragt und in die Produktbeurteilung einbezogen werden.

Liegen externe Testergebnisse oder Qualitätsaussagen für das zu testende Softwareprodukt vor (z. B. Testergebnisse in Fachzeitschriften, Konformitätstests nach proprietären Standards, Prüfungen und Zertifikate nach einschlägigen Standards und Normen wie ISO 9001), so sollten auch diese Ergebnisse bei der Auswahl berücksichtigt werden.

Verbreitungsgrad des Produktes

Bei einem hohen Verbreitungsgrad hat der einzelne Anwender üblicherweise wenig oder keinen Einfluss auf den Hersteller des Produkts, wenn es darum geht, Fehler zu beheben oder bestimmte Funktionen zu implementieren. Er kann aber eher davon ausgehen, dass ein solches Produkt kontinuierlich weiterentwickelt wird. In einigen Fällen gibt es externe Tests, die durch den Hersteller beauftragt oder von Fachzeitschriften durchgeführt wurden. Bei Produkten mit hohem Verbreitungsgrad ist im Allgemeinen mehr über Schwachstellen bekannt, sodass der Anwender davon ausgehen kann, dass die wesentlichen Schwachstellen bereits bekannt sind, bzw. dass das Wissen über Schwachstellen schnell verbreitet wird und diese zeitnah geschlossen werden, nachdem sie bekanntgeworden sind.

Bei einem niedrigen Verbreitungsgrad kann ein Anwender eventuell mehr Einfluss auf den Hersteller nehmen. Externe Tests liegen hier jedoch oft nicht vor, da sie für Produkte kleiner Hersteller zu aufwendig und zu teuer sind. Produkte mit niedrigem Verbreitungsgrad enthalten meist nicht mehr oder weniger Schwachstellen als solche mit hohem Verbreitungsgrad. Nachteil ist hier, dass diese eventuell nicht so schnell bekannt und damit behoben werden können. Wenn es sich um Sicherheitslücken handelt, sind diese aber wahrscheinlich auch potenziellen Angreifern nicht bekannt bzw. keine lohnenden Angriffsziele.

Wirtschaftlichkeit / Kosten für Kauf, Betrieb, Wartung, Schulung

Vor der Entscheidung für ein Produkt sollte immer die Frage stehen, ob die Kosten für das Produkt in einem angemessenen Verhältnis zu dem damit erzielbaren Nutzen stehen. In die Rechnung sind neben den unmittelbaren Anschaffungskosten auch alle Folgekosten für Betrieb, Wartung und Schulung einzubeziehen. Dazu muss zum Beispiel geklärt werden, ob die IT-Infrastruktur aufgerüstet werden muss oder ob für Installation und Betrieb Schulungen erforderlich sind.

Nach Abschluss aller Tests müssen die Testergebnisse der Beschaffungsstelle vorgelegt werden. Die Entscheidung für ein Produkt sollte die Beschaffungsstelle unter Beteiligung der anfordernden Fachabteilung und des IT-Bereichs aufgrund der Testergebnisse treffen. Auch sollten der Kaufpreis sowie zusätzliche Funktionen der Produkte, die nicht im Anforderungskatalog aufgeführt wurden, aber dennoch für den Einsatz sinnvoll sind, bei der Entscheidung berücksichtigt werden.

CON.4.M7 Überprüfung der Lieferung von Standardsoftware [Fachabteilung]

Nach Eingang einer Lieferung ist anhand der vorhandenen Unterlagen zu überprüfen,

- ob die Lieferung bestellt wurde,
- für wen sie bestimmt ist,
- ob Transportschäden zu erkennen sind und
- ob sie vollständig ist, das heißt ob einerseits alle bestellten Komponenten und andererseits alle gemäß Produktbeschreibung zum Lieferumfang des Produktes gehörenden Komponenten vorhanden sind.

Die Ergebnisse dieser Prüfungen sind in einem Wareneingangsverzeichnis zu dokumentieren, zusammen mit:

- Produktname und Version,
- Produktart,
- Lieferumfang, also Beschreibung der einzelnen Komponenten inklusive Anzahl und Lieferform (zum Beispiel Buch, Datenträger),
- Lieferdatum,
- Lieferart,
- wer es in Empfang genommen hat,
- Aufbewahrungsort und
- an wen es weitergegeben wurde.

Danach müssen die gelieferten Produkte an die IT-Abteilung weitergegeben werden, damit sie funktionale Tests durchführt und das Produkt formell freigeben, installieren und konfigurieren kann.

Werden die Produkte nur vorübergehend eingesetzt oder zur Verfügung gestellt (zum Beispiel für einen Test) müssen zumindest die Seriennummer und andere produktspezifische Identifizierungsmerkmale in entsprechenden Bestandsverzeichnissen vermerkt werden. Wenn die gelieferten Produkte dauerhaft genutzt werden sollen, sind sie mit eindeutigen Identifizierungsmerkmalen (z. B. gruppierten fortlaufenden Inventarnummern) zu kennzeichnen. Anschließend müssen sie in ein Bestandsverzeichnis aufgenommen werden. Dieses muss Auskunft geben können über:

- Identifizierungsmerkmale,
- Beschaffungsquellen, Lieferzeiten,
- Verbleib,
- Freigabedatum,
- Installationsdatum und Konfigurationsbesonderheiten und
- Wartungsverträge, Wartungsintervalle.

CON.4.M8 Lizenzverwaltung und Versionskontrolle von Standardsoftware

Ohne eine geeignete Versions- und Lizenzkontrolle werden auf einem IT-System oder innerhalb einer Organisationseinheit erfahrungsgemäß schnell verschiedene Software-Versionen verwendet, von denen eventuell einige ohne Lizenz benutzt werden.

Auf allen IT-Systemen einer Institution darf ausschließlich lizenzierte Software eingesetzt werden. Diese Regelung muss allen Mitarbeitern bekanntgemacht werden. Die Administratoren der verschiedenen IT-Systeme müssen sicherstellen, dass nur lizenzierte Software eingesetzt wird. Dafür müssen sie mit geeigneten Werkzeugen zur Lizenzkontrolle ausgestattet und im Umgang damit geschult werden.

Häufig werden in einer Institution verschiedene Versionen einer Anwendung eingesetzt. Durch eine Lizenzkontrolle muss es möglich sein, einen Überblick über alle eingesetzten Software-Versionen zu erhalten. Damit sollte gewährleistet werden, dass alte Versionen durch neuere ersetzt werden, sobald das notwendig ist und dass bei der Rückgabe von Lizenzen alle Versionen gelöscht werden.

Darüber hinaus sollten die verschiedenen Konfigurationen der installierten Software dokumentiert werden. Damit muss es möglich sein, sich einen Überblick zu verschaffen, an welchem IT-System welche sicherheitsrelevanten Einstellungen eines Produktes durch die Freigabe vorgegeben und welche tatsächlich installiert wurden. Damit kann zum Beispiel schnell geklärt werden, an welchen Clients bei einem bestimmten Produkt Makro-Programmierung installiert worden ist und an welchen nicht.

Damit Lizenzen bei Hardware-Defekten nicht ungültig werden, sollten Hardware-unabhängige Lizenzen eingesetzt werden. So kann ein IT-System mit weniger Aufwand ersetzt werden, wenn die Hardware ausfällt. Ist das nicht möglich, sind geeignete Vorkehrungen für einen Ausfall zu treffen, etwa Vereinbarungen mit dem Hersteller bezüglich einer Lizenzübertragung.

Wenn es notwendig ist, ein Produkt online über einen Lizenzierungsserver des Herstellers zu aktivieren, kann die Lizenz nachträglich verfallen und das Produkt deaktiviert werden. Wenn möglich, sollten Produkte gewählt werden, die nicht online aktiviert werden müssen. Auch hier sind Vorkehrungen für einen Ausfall zu treffen.

Wenn es möglich und wirtschaftlich sinnvoll ist, sollten unbefristete Lizenzen bevorzugt werden. Damit kann eine Funktionseinschränkung verhindert werden, wenn die Lizenz abgelaufen ist oder die Systemzeit stark abweicht.

CON.4.M9 Deinstallation von Standardsoftware

Bei der Deinstallation von Standardsoftware sind grundsätzlich die Vorgaben des Bausteins CON.6 *Löschen und Vernichten* zu beachten. Darüber hinaus gelten einige Besonderheiten.

Bei der Deinstallation von Software müssen alle Dateien entfernt werden, die für den Betrieb der Software auf dem IT-System angelegt worden sind. Auch müssen alle Einträge in Systemdateien, die bezüglich des Produktes vorgenommen wurden, gelöscht werden. Bei vielen Softwareprodukten werden während der Installation in diversen Verzeichnissen auf dem IT-System Dateien angelegt oder bestehende Dateien verändert. In der Regel wird der Benutzer nicht über alle durchgeführten Veränderungen am IT-System informiert.

Um Standardsoftware wieder vollständige deinstallieren zu können, ist es daher hilfreich, die bei der Installation durchgeführten Systemänderungen entweder manuell oder mithilfe von speziellen Tools zu dokumentieren. Anderenfalls kann es sein, dass ein Produkt nicht komplett deinstalliert wird.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

CON.4.M10 Implementierung zusätzlicher Sicherheitsfunktionen (CIA)

Manchmal ist es notwendig, dass ergänzend zur Standardsoftware selbst Sicherheitsfunktionen wie eine Zugangskontrolle, eine Zugriffsrechteverwaltung und -prüfung oder eine Protokollierung genutzt und eventuell implementiert werden müssen:

- Reichen die Protokollierungsmöglichkeiten des IT-Systems einschließlich zusätzlich eingesetzter Sicherheitsprodukte nicht aus, um eine ausreichende Beweissicherung zu gewährleisten, so müssen diese geeignet implementiert werden.
- Reicht die Granularität der Zugriffsrechte des IT-Systems einschließlich zusätzlich eingesetzter Sicherheitsprodukte nicht aus, um einen ordnungsgemäßen Betrieb zu gewährleisten, so muss eine Zugriffsrechteverwaltung und -kontrolle implementiert werden.
- Ist es mit dem IT-System einschließlich zusätzlich eingesetzter Sicherheitsprodukte nicht möglich, den Administrator daran zu hindern auf bestimmte Daten zuzugreifen oder zumindest diesen Zugriff zu protokollieren und zu kontrollieren, dann muss dies bei Bedarf durch zusätzliche Sicherheitsfunktionen implementiert werden. Zum Beispiel kann mit einer Verschlüsselung der Daten verhindert werden, dass der Administrator diese Daten im Klartext liest, wenn er den zugehörigen Schlüssel nicht besitzt.

Diese zusätzlichen Anforderungen an Standardsoftware müssen schon in der Planung und bei der Auswahl berücksichtigt werden, da eine nachträgliche Implementierung meist unwirtschaftlich oder nicht einfach möglich ist.

CON.4.M11 Nutzung zertifizierter Standardsoftware (CIA)

Bei einem hohen Schutzbedarf kann die Vertrauenswürdigkeit von Standardsoftware hinsichtlich der Informationssicherheit nur dadurch gewährleistet werden, dass unabhängige Prüfstellen die Produkte untersuchen und bewerten. Darauf aufbauend kann dann ein Zertifikat erteilt werden.

Zertifizierung von Produkten

Allgemein anerkannte Grundlage der Evaluierung und Zertifizierung von Produkten bilden seit 1991 die europaweit harmonisierten "Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC)" und seit 1998 die weltweit angestimmten "Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik", kurz Common Criteria (CC). In Deutschland führt das BSI solche Zertifizierungen durch. Bei positivem Evaluationsergebnis und bei Einhaltung der Rahmenbedingungen von ITSEC bzw. der Common Criteria wird für das untersuchte Produkt vom BSI als Zertifizierungsstelle ein Sicherheitszertifikat erteilt.

Aus dem dazugehörenden Zertifizierungsdokument geht hervor, welche Funktion mit welcher Prüftiefe untersucht wurde und welche Bewertung vorgenommen wurde. Dabei reicht die Prüftiefe von Evaluationsstufe E 1 (geringste Prüftiefe) bis Evaluationsstufe E 6 (höchste Prüftiefe) bei den ITSEC bzw. von Vertrauenswürdigkeitsstufe EAL 1 (geringste Prüftiefe) bis Vertrauenswürdigkeitsstufe EAL 7 (höchste Prüftiefe) bei den CC. Dabei entspricht die Evaluationsstufe E 1 der ITSEC in etwa der Vertrauenswürdigkeitsstufe EAL 2 der CC usw. Zusätzlich wird die geprüfte Mechanismenstärke der Implementation der Sicherheitsfunktionen angegeben, die ein Maß für den Aufwand darstellt, der erforderlich ist, um die Sicherheitsfunktionen zu überwinden. ITSEC und CC unterscheiden hier die Mechanismenstärken niedrig, mittel und hoch. Darüber hinaus werden Hinweise gegeben, welche Randbedingungen beim Einsatz des Produktes beachtet werden müssen.

Stehen bei der IT-Beschaffung mehrere Produkte mit angemessenem Preis-/Leistungsverhältnis zur Auswahl, sollten nur solche mit Sicherheitszertifikat berücksichtigt werden. Hierbei sollten Sicherheitszertifikate insbesondere dann berücksichtigt werden, wenn der evaluierte Funktionsumfang die Mindestfunktionalität (weitestgehend) umfasst und die Mechanismenstärke dem Schutzbedarf entspricht. Je höher dann die im Zertifikat angegebene Prüfungstiefe ist, desto mehr Vertrauen in Wirksamkeit und Korrektheit der Sicherheitsfunktionen kann dem Produkt entgegengebracht werden.

Übersichten zertifizierter Produkte

Die Zertifizierungsstellen geben regelmäßig Übersichten heraus, welche Produkte ein Zertifikat erhalten haben. Eine Zusammenstellung der vom BSI zertifizierten IT-Produkte findet sich auf der BSI-Website. Weiterhin veröffentlicht das BSI neu erteilte Zertifikate in der Zeitschrift <kes> - Die Zeitschrift für Informations-Sicherheit. Diese Informationen lassen sich ebenfalls von den Internetseiten des BSI abrufen.

CON.4.M12 Einsatz von Verschlüsselung, Checksummen oder digitalen Signaturen (CI)

Werden vertrauliche Informationen oder Informationen mit hohem Integritätsanspruch übertragen, sollte ein kryptografisches Verfahren zum Schutz der Daten für den Transport oder die Übermittlung eingesetzt werden.

Vertraulichkeitsschutz durch Verschlüsselung

Das entscheidende Merkmal eines Verschlüsselungsverfahrens ist die Güte des Algorithmus sowie der Schlüsselauswahl. Ein anerkannter Algorithmus ist beispielsweise der Advanced Encryption Standard (AES).

Um die Vertraulichkeit der zu übertragenden Informationen zu gewährleisten, müssen die IT-Systeme des Absenders und des Empfängers den Zugriff auf das Verschlüsselungsprogramm ausreichend schützen. Gegebenenfalls sollte dieses Programm auf einem auswechselbaren Datenträger gespeichert, in der Regel verschlossen aufbewahrt und nur bei Bedarf eingespielt und genutzt werden.

Integritätsschutz durch Checksummen, Verschlüsselung oder digitaler Signaturbildung

Ist für den Datenaustausch lediglich die Integrität der zu übermittelnden Daten sicherzustellen, muss unterschieden werden, ob ein Schutz nur gegen zufällige Veränderungen, z. B. durch Übertragungsfehler, oder auch gegen Manipulationen realisiert werden soll. Sollen ausschließlich zufällige Veränderungen erkannt werden, können Checksummen-Verfahren (z. B. Cyclic Redundancy Checks) oder fehlerkorrigierende Codes eingesetzt werden. Schutz gegenüber Manipulationen bieten darüber hinaus Verfahren, die unter Verwendung eines symmetrischen Verschlüsselungsalgorithmus (z. B. Triple-DES) aus der zu übermittelnden Information einen sogenannten Message Authentication Code (MAC) erzeugen. Andere Verfahren bedienen sich eines asymmetrischen Verschlüsselungsalgorithmus (z. B. RSA) in Kombination mit einer Hashfunktion und erzeugen eine digitale Signatur. Die jeweiligen erzeugten Fingerabdrücke (Checksumme, fehlerkorrigierende Codes, MAC, digitale Signatur) werden zusammen mit der Information an den Empfänger übertragen und können von diesem überprüft werden.

3 Weiterführende Informationen

3.1 Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Auswahl und Einsatz von Standardsoftware" finden sich unter anderem in folgenden Veröffentlichungen:

[27001A12.1.1] ISO/IEC 27001:2013

Information technology - Security techniques - Information security management systems - Requirements, insbesondere Annex A, A.12.1.1 Documented operating procedures, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/SC 27, Oktober 2013

[27001A12.1.2] ISO/IEC 27001:2013

Information technology - Security techniques - Information security management systems - Requirements, insbesondere Annex A, A.12.1.2 Change management, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/SC 27, Oktober 2013

[27001A12.6.2] ISO/IEC 27001:2013

Information technology - Security techniques - Information security management systems - Requirements, insbesondere Annex A, A.12.6.2 Restriction of software installation, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/SC 27, Oktober 2013

[27001A8.1.1] ISO/IEC 27001:2013

Information technology - Security techniques - Information security management systems - Requirements, insbesondere Annex A, A.8.1.1 Inventory of assets, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/SC 27, Oktober 2013

[27001A8.1.3] ISO/IEC 27001:2013

Information technology - Security techniques - Information security management systems - Requirements, insbesondere Annex A, A.8.1.3 Acceptable use of assets, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/SC 27, Oktober 2013

[27001A8.1.4] ISO/IEC 27001:2013

Information technology - Security techniques - Information security management systems - Requirements, insbesondere Annex A, A.8.1.4 Return of assets, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/SC 27, Oktober 2013

[CC] Common Criteria for Information Technology Security Evaluation (CC)

(siehe auch ISO/IEC 15408-2:2008 ISO, Information technology - Security techniques - Evaluation criteria for IT security), www.commoncriteriaportal.org , zuletzt abgerufen am 24.08.2018

[ISFBA] The Standard of Good Practice for Information Security

Area BA Business Application Management, Information Security Forum (ISF), June 2018

[NIST80053] Security and Privacy Controls for Federal Information Systems and Organizations

NIST Special Publication 800-53, Revision 4, April 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf , zuletzt abgerufen am 30.08.2018

Umsetzungshinweise zum Baustein CON.5 Entwicklung und Einsatz von Allgemeinen Anwendungen

1 Beschreibung

1.1 Einleitung

In Unternehmen und Behörden werden Geschäftsprozesse oder Fachverfahren betrieben, die durch spezialisierte Anwendungssoftware, kurz (Fach-)Anwendungen, unterstützt werden. Hierfür sind im IT-Grundschutz-Kompendium keine spezifischen IT-Grundschutz-Bausteine, also keine spezifischen Gefährdungslagen und Sicherheitsanforderungen, vorhanden. Gleichzeitig beschreiben aber zahlreiche Prozess-Bausteine einen umfassenden Managementrahmen, also Prozesse und Vorgehensmodelle, die für alle Phasen des Lebenszyklus beim Einsatz von Anwendungen relevant sind. Insbesondere sind hier zu nennen:

Grundsätzlich:

- DER.4 Notfallmanagement
- Bausteine aus OPS.1.1 Kern-IT-Betrieb
- CON.4 Auswahl und Einsatz von Standardsoftware
- ORP.5 Compliance Management (Anforderungsmanagement)

Im Bedarfsfall:

- CON.1 Kryptokonzept
- Bausteine aus OPS.2 Betrieb von Dritten
- OPS.1.2.2 Archivierung

Bis auf wenige Ausnahmen richten sich diese Bausteine und die darin enthaltenen Sicherheitsanforderungen an das Informationssicherheitsmanagement und die IT-Betriebsleitung. Die Perspektive der Verantwortlichen für Auswahl, Inbetriebnahme, Betrieb und Aussonderung einer Anwendung tritt dabei in den Hintergrund.

Dieser Baustein fasst aus Sicht der Verantwortlichen für Anwendungen wesentliche Anforderungen an die Informationssicherheit zusammen. Er referenziert dabei wesentliche Maßnahmen aus den oben genannten Bausteinen und verweist somit auf die dort beschriebenen Prozesse. Führen diese Prozesse im jeweiligen zu Rahmenkonzepten, etwa für den Einsatz von Verschlüsselung, Datensicherung oder Notfallvorsorge, so ist es sinnvoll, diese Konzepte bezogen auf die jeweilige betrachtete Anwendung fortzuschreiben.

Dieser Baustein deckt die folgenden Typen von Anwendungen ab:

- Individualsoftware, die durch interne oder externe Entwickler erstellt wurde,
- Standardsoftware mit eigenen Anpassungen, zum Beispiel durch Programmänderungen oder durch Entwicklung spezifischer Module (Customizing) und
- Standardsoftware, die wie vom Hersteller geliefert eingesetzt und nur entsprechend der Fachaufgaben und der Sicherheitsvorgaben konfiguriert wird.

Fokus dieses Bausteins sind komplexe Anwendungen, die für spezifische fachliche Aufgaben konzipiert sind, wie Personalverwaltungssoftware oder wie Verfahren zur Verwaltung von Sozialdaten oder Meldedaten. Fach- oder funktionsübergreifende Standardsoftware, die fachlich nicht fokussiert ist und wie Office-Anwendungen für viele Branchen nutzbar ist, wird in CON.4 Auswahl und Einsatz von Standardsoftware behandelt. Je nach Typ der Anwendung können dabei einige der in diesem Baustein vorgeschlagenen Maßnahmen entbehrlich sein.

Unabhängig vom Geschäftsprozess oder Verwaltungsverfahren, in dem die Anwendung eingesetzt wird, werden in diesem Baustein wesentliche, übergreifende Gefährdungen und Standardsicherheitsmaßnahmen beschrieben. Eine Ergänzung dieses Bausteins um spezifische Bausteine für bestimmte Anwendungen ist möglich, wie beispielsweise durch die Bausteine der Schichten APP.4 Business-Anwendungen oder APP.3 Netzbasierte Dienste.

1.2 Lebenszyklus

Für Anwendungen sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung des Einsatzes über die Beschaffung bis zu ihrer Außerbetriebnahme und der Notfallvorsorge. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Planung und Konzeption

Bevor eine neue Anwendung beschafft oder programmiert wird, müssen die Rahmenbedingungen für den Einsatz geklärt werden (siehe CON.5.M1 Festlegung benötigter Sicherheitsfunktionen der Fachanwendung).

Je nach Einsatzzweck kann eine Anwendung fertig eingekauft werden, die eventuell angepasst werden muss, oder es muss eine spezielle Anwendungssoftware entwickelt werden. Dafür sollte ein Anforderungskatalog bzw. ein Lastenheft erstellt werden (siehe CON.5.M6 Umfassende Dokumentation der Anforderungen an die Anwendung).

Beschaffung

Anhand der konkreten Vorgaben des Anforderungskatalogs kann geprüft werden, ob ein am Markt vorhandenes Produkt für den Einsatzzweck geeignet ist. Anderenfalls sollten andere Lösungen überlegt werden, beispielsweise könnten externe Dienstleister mit der Entwicklung einer passenden Anwendungssoftware beauftragt werden.

Stützt sich die Institution bei Beschaffung, Entwicklung oder Betrieb der Anwendung auf Dienstleister ab, sollten geeignete vertragliche Rahmenbedingungen geschaffen werden (siehe CON.5.A11 Geeignete und rechtskonforme Vergabe und Vertragsgestaltung).

Umsetzung

Aufbauend auf dem Lastenheft ist zur Anwendungsentwicklung ein Pflichtenheft zu erstellen (siehe CON.5.M6 Umfassende Dokumentation der Anforderungen an die Anwendung). Im Rahmen des Pflichtenheftes sind auch eine Reihe von Teilkonzepten zu berücksichtigen. Diese sollten die Pflege der Anwendung, die geeignete Behandlung der Nutzerauthentisierung und die Protokollierung beinhalten.

Bei der Inbetriebnahme der Anwendung sind Test und Freigabe (siehe CON.5.M2 Test und Freigabe von Fachanwendungen), die sichere Installation (siehe CON.5.M3 Sichere Installation einer Fachanwendung) sowie die geeignete Schulung von Administratoren und Anwendern zu berücksichtigen.

Betrieb

In der Phase des Betriebes einer Anwendung ist dafür Sorge zu tragen, dass die Sicherheit gewährleistet bleibt (siehe CON.5.M5 Sicherer Betrieb einer Fachanwendung).

Aussonderung

Wird eine Anwendung auf eine neue betriebliche Infrastruktur migriert oder wird die Anwendung endgültig außer Betrieb genommen, so sind in der abgelösten betrieblichen Umgebung die Deinstallation, die Löschung und Vernichtung von nicht mehr benötigten Daten und Außerbetriebnahme der bisherigen betrieblichen Infrastruktur zu planen und umzusetzen (siehe CON.5.M9 Außerbetriebnahme von Anwendungen).

Notfallvorsorge

Hinweise zur anwendungsspezifischen Planung der Notfallvorsorge sind in der Maßnahme CON.5.M10 Notfallvorsorge für Anwendungen zusammengefasst. Wurde die Anwendung durch Dienstleister entwickelt und kann fehlende Unterstützung durch den Dienstleister, zum Beispiel durch Insolvenz, die Existenz der Institution gefährden, so ist eine Hinterlegung des Quellcodes zu empfehlen (siehe CON.5.A12 Treuhänderische Hinterlegung (Escrow)). Bei hohem Schutzbedarf hinsichtlich der Verfügbarkeit ist die Erstellung eines Verfügbarkeitskonzeptes zu empfehlen (siehe CON.5.M13 Entwicklung eines Redundanzkonzeptes für Anwendungen).

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Entwicklung und Einsatz von Allgemeinen Anwendungen" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

CON.5.M1 Festlegung benötigter Sicherheitsfunktionen der Fachanwendung [IT-Betrieb]

Bevor eine neue Anwendung geplant und projektiert wird, sollten die Rahmenbedingungen für den Einsatz geklärt werden, also beispielsweise

- welche Geschäftsprozesse sie wie unterstützen soll,
- welche Informationen mit welchem Schutzbedarf mit ihr verarbeitet werden sollen,
- wer auf welche Teile der Anwendung zugreifen darf und soll,
- welche rechtlichen Rahmenbedingungen einzuhalten sind (siehe CON.5.M6 Umfassende Dokumentation der Anforderungen an die Anwendung),
- wie der Informationsverbund aussieht, in dem sie eingesetzt werden soll, also beispielsweise, wie die Netzstrukturen aussehen, und
- welche IT-Komponenten für den Betrieb der Anwendung benötigt werden, also beispielsweise Hardware-Plattform, Betriebssysteme, Datenbanken).

Es empfiehlt sich, bereits bei der initialen Planung über Bedrohungen und Risiken zu diskutieren, die beim Betrieb der Anwendung relevant sein können. Hierzu sollte eine erste Analyse durchgeführt werden, um potenzielle Angriffe und andere Risiken für Vertraulichkeit, Integrität und Verfügbarkeit der Anwendung frühzeitig zu identifizieren. Die dokumentierten Ergebnisse zu den Sicherheitsrisiken fließen dann in die detaillierte Risikoanalyse ein, die im Zuge der Erstellung des Lastenhefts durchgeführt wird (siehe CON.5.A6 Umfassende Dokumentation der Anforderungen an eine Anwendung). Auch im späteren Projektverlauf sollten mögliche Bedrohungen regelmäßig betrachtet werden, sowohl seitens der Fachverantwortlichen als auch der Entwickler, damit alle sicherheitsrelevanten Anforderungen berücksichtigt werden. Darauf aufbauend können passende Sicherheitsmaßnahmen und Testanforderungen abgeleitet werden, die in die Sicherheitsarchitektur mit einfließen.

Wenn sich während des Betriebes einer Anwendung die Rahmenbedingungen wesentlich ändern, also beispielsweise neue Serverplattformen installiert werden, müssen die Sicherheitsmaßnahmen neu bewertet werden.

Daher müssen innerhalb des Sicherheitsmanagements Prozesse aufgebaut werden, um Anwendungen sicher zu entwickeln, zu installieren, zu betreiben, zu überwachen und zu warten sowie die Administratoren und Benutzer in deren sicherer Handhabung zu trainieren.

Im Rahmen dieser Prozesse müssen die Rollen, Verantwortlichkeiten und Aufgaben für Konzeption, Aufbau und Betrieb der jeweiligen Anwendungen festgelegt werden. Darauf aufbauend können die Berechtigungen in den verschiedenen Lebenszyklusphasen einer Anwendung geeignet festgelegt werden. Außerdem sollte im Rahmen des Rollenkonzepts festgehalten werden, welche Qualifikationen erforderlich sind, um die Rollen wahrnehmen zu können. So kann auch etwaiger Schulungsbedarf identifiziert und die jeweiligen Rolleninhaber gezielt zu ihrer Sicherheitsverantwortung sensibilisiert werden.

CON.5.M2 Test und Freigabe von Fachanwendungen [Datenschutzbeauftragter, Leiter IT]

Für einen geordneten Betriebsübergang einer Anwendung und bei wesentlichen Änderungen ist ein geeignetes Vorgehen bei Test und Freigabe erforderlich. Für die Planung und Umsetzung von Tests sowie der darauf basierenden Freigabe sind üblicherweise vier Ebenen zu berücksichtigen, bei denen jeweils andere Funktionsträger mit ihrer fachlichen Perspektive einzubeziehen sind:

- die fachliche Ebene (Vertreten durch Fachverantwortliche)
- die Ebene des IT-Betriebs (Vertreten durch den IT-Leiter)
- die Ebene der Informationssicherheit (Vertreten durch den IT-Sicherheitsbeauftragten)
- die Ebene des Datenschutzes (Vertreten durch den Datenschutzbeauftragten)

Je nach Art und Komplexität einer Anwendung können noch weitere Funktionsträger benötigt werden, z. B. die Personalvertretung.

Für alle genannten Ebenen sind Test- und Überprüfungsszenarien sowie Kriterien für die Freigabe zu entwickeln. Hierbei sollte Berücksichtigung finden:

- Auf der fachlichen Ebene sollten aus Baustein CON.4 Auswahl und Einsatz von Standardsoftware die Maßnahmen zu Software-Abnahme- und Freigabe-Verfahren und zum Testen von Standardsoftware angewendet werden, die ein Vorgehen für Tests, Abnahme und Freigabe beschreiben und die auch auf Individualsoftware anwendbar sind.

- Der IT-Betrieb sollte sicherstellen, dass die Anwendung in die IT-Infrastruktur und die IT-Betriebsabläufe integriert werden kann.
- Die Anwendungskonzeption und der Anwendungsbetrieb müssen konform mit dem Regelwerk (Leitlinien, Richtlinien), den Konzepten (z. B. Kryptokonzept) und den Best Practices (z. B. OWASP) zur Informationssicherheit sein. Es ist insbesondere darauf zu achten, dass die benötigten Sicherheitsfunktionen umgesetzt wurden und einwandfrei funktionieren.
- Es muss geplant werden, dass, sofern notwendig, eine datenschutzrechtliche Freigabe eingeholt wird.

Die Ergebnisse der Tests bzw. Prüfungen sind zu dokumentieren und zu bewerten. Beispielsweise können Abweichungen und Fehler in drei Kategorien hinsichtlich ihrer Kritikalität (z. B. niedrig, mittel, hoch) bewertet werden. Auf Grundlage dieser Bewertung entscheidet der Freigabeverantwortliche über die Freigabe. Der Freigabeverantwortliche ist üblicherweise die Institutionsleitung oder ein von ihr beauftragter Funktionsträger. Die Freigabe ist geeignet zu dokumentieren, insbesondere sind rechtliche Vorgaben, z. B. zur Schriftform, zu berücksichtigen.

CON.5.M3 Sichere Installation einer Fachanwendung [IT-Betrieb]

Nach erfolgreichem Abschluss der Tests und der Freigabe der Anwendung ist der Roll-Out bzw. die Installation der Anwendung zu planen. Hierbei ist es zweckmäßig, eine Installationsanweisung zu erstellen (siehe Baustein CON.4 Auswahl und Einsatz von Standardsoftware). Bevor die Software installiert wird, ist die Vollständigkeit und Korrektheit der Software-Lieferung zu überprüfen und die Integrität der eingesetzten Software sicherzustellen. Auch bei der Installation ist die entsprechende Maßnahme zu Installation und Konfiguration von Standardsoftware umzusetzen, die ebenfalls für Individualsoftware anwendbar ist.

Um später im laufenden Betrieb überprüfen zu können, ob die Anwendung korrekt konfiguriert wurde und um eine Neuinstallation der Anwendung zu vereinfachen, sollte die Installation einer Anwendung mit allen ihren Schritten dokumentiert werden. Dies kann beispielsweise in Form von aufeinanderfolgenden Screenshots der Installationsbildschirme erfolgen, in denen jeweils die relevanten Einstellungen vorgenommen werden.

Bei der Durchführung späterer Änderungen der Konfiguration oder bei Updates der Anwendung ist darauf zu achten, dass diese Dokumentation aktualisiert wird. Eine ausschließliche Dokumentation von späteren Konfigurationsänderungen in einem Ticketsystem oder Change-Tool führt in der Regel dazu, dass die Soll-Konfiguration nicht ohne erheblichen Aufwand nachvollziehbar ist. Damit ist die Konfiguration der Anwendung später nicht ohne Weiteres prüfbar (siehe auch die Maßnahme zur Dokumentation der Veränderungen an einem bestehenden System in OPS.1.1.1 Ordnungsgemäße IT-Administration).

CON.5.M4 Heranführen von Nutzerinnen und Nutzern an die Anwendung

Um eine geordnete Nutzung der Anwendung sicherzustellen und um Schäden durch unsachgemäßen Umgang zu vermeiden, muss der Fachverantwortliche dafür Sorge tragen, dass Benutzer und Administratoren an die korrekte Nutzung und Administration der Anwendung (einschließlich der Sicherheitsfunktionen) herangeführt werden. Hierzu können beispielsweise die folgenden Mittel eingesetzt werden:

- Richtlinien und Arbeitsanweisungen zur Nutzung und Administration der Anwendung
- Schulungen und Einweisungen
- Handbücher und Online-Hilfen
- Benutzerunterstützung durch Schlüsselanwender

Darüber hinaus müssen auch bei umfangreichen Änderungen in einer Anwendung erneut enstprechende Einweisungen erfolgen.

Die Mitarbeiter sollten ausreichende Möglichkeiten und Zeit bekommen, um sich in neue Aufgaben und Anwendungen einzuarbeiten.

CON.5.M5 Sicherer Betrieb einer Fachanwendung [IT-Betrieb]

Während des Betriebes einer Anwendung oder eines Fachverfahrens sollte sichergestellt sein, dass die Benutzer ausreichend bei Fragen und Problemen unterstützt werden. Dies kann beispielsweise über den IT-Betrieb, etwa über das Bereitstellen eines IT-Ansprechpartners oder einen sogenannten Service- oder User-Help-Desk (SD / UHD), erfolgen.

Darüber hinaus sollten die Benutzer auch bezogen auf fachliche Aspekte geeignet unterstützt werden. Dies kann etwa durch einen Key-User oder eine so genannte fachliche Leitstelle erfolgen. Diese organisieren die Einführung und Schulung neuer Benutzer, unterstützen bei der korrekten Bedienung der Anwendung und nehmen Anforderungen für kommende Versionen der Anwendung auf.

Ein wichtiger Aspekt der Sicherheit einer Anwendung im laufenden Betrieb ist die geeignete Vergabe von Zugriffsrechten und die stets aktuelle Dokumentation von zugelassenen Benutzern und Rechteprofilen (siehe ORP.4 Identitäts- und Berechtigungsmanagement). Die Korrektheit der vergebenen Berechtigungen sollte regelmäßig überprüft werden.

Es ist darauf zu achten, dass die Protokolldaten der Anwendung regelmäßig ausgewertet werden (siehe OPS.1.1.5 Protokollierung). Hierbei sind die jeweils geltenden spezifischen gesetzlichen und vertraglichen Vorgaben zu Speicherfristen für Protokolldateien, deren Zugreifbarkeit durch Dritte (z. B. Aufsichtsbehörden) und Vorgaben zur Auswertung zu beachten.

Typischerweise ergibt sich im laufenden Anwendungsbetrieb die Notwendigkeit, die Anwendung funktional anzupassen, Fehler zu beheben oder Sicherheitslücken zu schließen. Bei der Durchführung des Patch- und Änderungsmanagements sind die Vorgaben des Bausteins OPS.1.1.3 Patch- und Änderungsmanagement zu berücksichtigen. Insbesondere ist darauf zu achten, dass

- sicherheitskritische Patches und Updates zeitnah eingespielt werden ,
- Konfigurationsänderungen einschließlich Patchs und Updates vorher geeignet getestet, freigegeben und sorgfältig durchgeführt werden, und
- Konfigurationsänderungen geeignet dokumentiert werden (siehe CON.5.M3 Sichere Installation einer Fachanwendung).

Ferner ist sicherzustellen, dass Datensicherungen wie vorgesehen (siehe CON.3 Datensicherungskonzept) durchgeführt werden und eine Wiederherstellung der Anwendung aus den vorhandenen Datensicherungen erfolgreich möglich ist, also entsprechende Übungen zur Datenrekonstruktion durchgeführt werden. Hierzu sind Art und Umfang der Datensicherungen festzulegen, dabei kann es für die verschiedenen Komponenten unterschiedliche Vorgehensweisen zur Datensicherung geben, beispielsweise für Quellcode, Konfigurationsdaten, Protokolldaten und Inhaltsdaten.

Bei von Dritten entwickelten Anwendungen ist unter Umständen, um Urheberrechtsverstößen vorzubeugen, eine Lizenzverwaltung erforderlich. Ebenso ist es zur Sicherstellung des störungsfreien Betriebes sinnvoll, dass auf allen Arbeitsplätzen einer Institution einheitliche Versionen der Anwendungen eingesetzt werden (siehe CON.4 Auswahl und Einsatz von Standardsoftware).

Gemeinsam mit den Basismaßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich Allgemeine Anwendungen.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Entwicklung und Einsatz von Allgemeinen Anwendungen".

CON.5.M6 Umfassende Dokumentation der Anforderungen an die Anwendung

Rechtsgrundlagen

Um sicherstellen zu können, dass Geschäftsprozesse oder Verwaltungsverfahren, die die Anwendungen unterstützen sollen, rechtskonform betrieben werden, wird zu Planungs- (und später auch zu Audit-/Prüfungszwecken) eine vollständige Übersicht über einschlägige Rechtsgrundlagen benötigt (siehe ORP.5 Compliance Management (Anforderungsmanagement)). Diese Übersicht ist auch hilfreich für die Erstellung eines Verfahrensverzeichnisses nach Bundesdatenschutzgesetz (BDSG). Wenn in der Institution ein Justiziariat vorhanden ist, kann es bei der Erstellung dieser Zusammenstellung unterstützen. Die Rechtsgrundlagen sollten in einer Übersicht zusammengefasst werden, die als Anlage für das Lastenheft, das Datenschutzkonzept und das Sicherheitskonzept verwendet werden kann.

Aus den für die jeweiligen Institutionen geltenden Rechtsgrundlagen können sich konkrete Vorgaben für die Informationssicherheit ergeben, zum Beispiel:

- Vorgaben zum Schutzbedarf (zum Beispiel Verarbeitung besonderer Arten personenbezogener Daten nach § 3 Absatz 9 BDSG , bereichsspezifische Amtsgeheimnisse wie das Steuer- oder Sozialgeheimnis etc.)
- Vorgaben zur inhaltlichen Ausrichtung und Ausgestaltung von Sicherheitsmaßnahmen. Insbesondere bei der Verarbeitung personenbezogener Daten sind rechtliche Vorgaben wie die Einhaltung der Zweckbindung (wirkt sich zum Beispiel auf die Anforderungen zur Gestaltung und Absicherung von externen Schnittstellen und Berichten aus) oder der Datenminimierung und Datensparsamkeit (wirkt sich zum Beispiel auf die Anforderung an die Gestaltung von Löschfristen aus) zu beachten.
- Vorgaben zu konkreten Sicherheitsmaßnahmen, wie zum Beispiel der Einsatz von Spiegeldatenbanken, der Qualifizierten Elektronischen Signatur (QES), zur Pseudonymisierung oder Anonymisierung der zu verarbeitenden Daten oder zur Gestaltung der Protokollierung
- Vorgaben zu Speicher- oder Archivierungsfristen

Erstellung eines Lastenheftes

Ein Lastenheft beschreibt die Anforderungen, die eine Anwendung im Rahmen des betrachteten Geschäftsprozesses oder Verwaltungsverfahrens erfüllen soll. Dabei sind nicht nur die fachlichen (funktionalen) Anforderungen an die Anwendung zu betrachten, sondern auch nicht-funktionale Anforderungen.

Neben den fachlichen und IT-betrieblichen Anforderungen sind dabei auch Sicherheitsanforderungen zu betrachten. Auch bei diesen sind funktionale und nicht-funktionale Sicherheitsanforderungen zu unterscheiden. Funktionale Sicherheitsanforderungen decken konkrete Funktionen der Anwendung ab wie beispielsweise:

- Identitäts- und Berechtigungsmanagement
- Passwort-Management
- Kryptographische Absicherung der Daten

Die Art und Ausprägung von funktionalen Sicherheitsanforderungen wie beispielsweise zu der Integration einer Zwei-Faktor-Authentisierung, dem Aufbau einer PKI, die Nutzung von SAML oder WS-Security sind stark von dem jeweiligen Schutzbedarf der Anwendung abhängig.

Über nicht-funktionale Sicherheitsanforderungen wird beschrieben, welche Qualitätseigenschaften die Anwendung haben soll. Hierzu gehören Aspekte wie Softwarequalität, Zuverlässigkeit, Fehlertoleranz, Wartbarkeit und natürlich die Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit. Ein Beispiel einer nicht-funktionalen Anforderung ist es, die Anwendung resistent gegenüber bestimmten Angriffen zu machen.

Bei einem Lastenheft handelt es sich um das Grobkonzept aus Sicht des Auftraggebers, das die Art der Umsetzung in weiten Teilen noch offen lassen kann. Das Lastenheft ist die wesentliche Grundlage, um ein Entwicklungsprojekt zu starten, in ähnlicher Weise wie dies der Anforderungskatalog im Fall von Standardsoftware ist (siehe Baustein CON.4 Auswahl und Einsatz von Standardsoftware).

Bei der Erstellung des Lastenheftes müssen die folgenden Aspekte Berücksichtigung finden:

- Schutzbedarf der im Geschäftsprozess oder Verwaltungsverfahren verarbeiteten Informationen (Daten)
- Rechtsgrundlagen, die beim Betrieb und somit auch bereits bei der Konzeption der Anwendung zu beachten sind (siehe CON.5.M6 Umfassende Dokumentation der Anforderungen an die Anwendung)
- Vorgaben, Standards und Kriterienwerke, die zu berücksichtigen sind. Je nach Anwendungsgebiet können hierzu Sicherheitskriteriensysteme, technische Richtlinien oder Architekturempfehlungen gehören und auch Anforderungen hinsichtlich Barrierefreiheit

Beispiele für solche Vorgaben und Kriterienwerke sind:

- Common Criteria for Information Technology Security Evaluation (ISO 15408), insbesondere Teil 2 "Security functional requirements"
- Technische Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik
- Standards und Architekturen für eGovernment (SAGA)
- Mindestanforderungen der Rechnungshöfe zum Einsatz der Informations- und Kommunikationstechnik
- Best Practices wie "Die zehn goldenen Regeln der IT-Sicherheit" aus dem Secologic-Projekt des deutschen Bundesministeriums für Wirtschaft, die Guides des Open Web Application Security Projects (OWASP), der Leitfaden "Sicheres Programmieren, Einführung in die sichere Anwendungsentwicklung" der Sicherheitsinitiative Deutschland sicher im Netz und weitere Dokumente von Unternehmen (siehe Hilfsmittel)

Zur Vorbereitung des Lastenheftes, insbesondere um die benötigten Sicherheitsfunktionen herzuleiten und auszugestalten, hat es sich als zweckmäßig erwiesen, bei Bedarf (d. h. insbesondere bei hohem oder sehr hohem Schutzbedarf) bereits eine erste Risikoanalyse, beispielsweise auf Grundlage der im BSI-Standard 200-3 beschriebenen Methode, durchzuführen. Diese erste Fassung der Risikoanalyse muss dann im Zuge der Erstellung des Pflichtenheftes, bei der Fertigstellung der Anwendung und der Vorbereitung der Freigabe fortgeschrieben werden. In dieser ersten Runde der Risikoanalyse kann natürlich nur untersucht werden, gegen welche Gefährdungen die Anwendung widerstehen können soll und erste Sicherheitsziele gesetzt werden. Konkrete Sicherheitsmaßnahmen können erst im Pflichtenheft festgelegt werden.

Das Lastenheft sollte so detailliert, wie in dieser Phase möglich, über die funktionalen (fachlichen) Anforderungen hinaus Aussagen zu folgenden nicht-funktionalen Aspekten enthalten:

- Qualitätsanforderungen (zum Beispiel Benutzerfreundlichkeit, Zuverlässigkeit, Performance),
- Vorgaben hinsichtlich der Architektur und IT-Infrastruktur, für die die Anwendung ausgelegt wird. Jede Institution sollte eine klar umrissene Vorgabe haben, wie IT in der Institution eingesetzt wird und zusammenspielt. Dies kann z. B. in einem IT-Rahmenplan und einem Architekturkonzept festgelegt sein. Bei der Planung neuer IT-Komponenten und Anwendungen ist sicherzustellen, dass diese in die Infrastruktur und die generellen Planungen passen.
- Weitere technische Anforderungen (zum Beispiel Anwendungsarchitektur, Programmiersprache, Betriebssystem, Erweiterbarkeit),
- Anforderungen an die Dokumentation (zum Beispiel Modellierung in UML),
- Vorgaben zur geplanten Einführung. Hier ist zu unterscheiden, ob es sich um eine Migration, bei der Daten und Bearbeitungsabläufe aus einer vorhandenen Anwendung übernommen werden oder um eine komplette Neuentwicklung handelt. Wichtig kann auch sein, ob die Einführung der neuen Anwendung mit einer Stichtagsumstellung oder durch schrittweise Einführung geplant ist. Wertvolle Hinweise zur Planung des Vorgehens bei der Migration von Anwendungen gibt in einem Phasenmodell der Migrationsleitfaden der Beauftragten der Bundesregierung für Informationstechnik.

- Anforderungen an die Abnahme (Grundsätzliches zu Abnahmetests und Pilotbetrieb).
- Vorgaben zu den benötigten Sicherheitsfunktionen

Diese Sicherheitsfunktionen können unter anderem beinhalten:

- Vorgaben für die Verfügbarkeit des Verfahrens (tolerable Ausfallzeiten, Wiederherstellungszeiten etc.)
- Anforderungen an die Mandantentrennung (siehe CON.5.A7 Erstellung eines Mandantenkonzeptes)
- Anforderungen an die Datensicherung (siehe Baustein CON.3 Datensicherungskonzept) und, falls erforderlich, zur Archivierung (OPS.1.2.2 Archivierung)
- Anforderungen an externe Schnittstellen und deren Absicherung
- Anforderung an die Verschlüsselung der Datenhaltung und des Datentransports (siehe Baustein CON.1 Kryptokonzept)
- Anforderungen an Authentisierung und Autorisierung
- Anforderungen an die Datenhaltung und -strukturierung
- Anforderungen zur effizienten und effektiven Löschung von Daten

Das Lastenheft sollte die Anforderungen an die Anwendung so ausreichend beschreiben, dass hierauf aufbauend die Anwendung so erstellt werden kann, dass sich mit ihr die erforderlichen Sicherheitsmaßnahmen umsetzen lassen und sich eine dem Schutzbedarf angemessene Gesamtsicherheit erreichen lässt.

Erstellung eines Pflichtenheftes

Ein Pflichtenheft beschreibt, wie das Lastenheft technisch umgesetzt werden soll. In der Regel gibt der Auftraggeber, also z. B. die verantwortliche Fachabteilung, das Lastenheft vor. Darauf aufbauend erarbeitet die (interne oder externe) Entwicklungsabteilung, die die Anwendung erstellen soll, das Pflichtenheft, in dem die technische Umsetzung der Anforderungen des Lastenhefts ausformuliert wird. Das Pflichtenheft muss vom Auftraggeber daraufhin überprüft werden, ob alle Anforderungen aus dem Lastenheft so abgebildet werden, dass die angestrebten Entwicklungsziele erreicht werden können. Es ist sinnvoll, dabei das Sicherheitsmanagement mit einzubinden, um zu gewährleisten, dass die auch die formulierten Sicherheitsziele erreicht werden.

Dabei sind mindestens die folgenden Aspekte zu berücksichtigen:

Beschreibung der fachlichen Anforderungen

Es ist detailliert zu beschreiben, wie die fachlichen Anforderungen umgesetzt werden sollen (z. B. Workflows, Dialoge, Bearbeitungsmasken, Datenstrukturen).

Einbettung in den Informationsverbund

Es sollte im Pflichtenheft ausgearbeitet werden, wie sich die Anwendung in den Informationsverbund einpassen wird bzw. welche Anpassungen durchzuführen sind. Dazu ist beispielsweise zu klären, welche und wie viele Betriebsumgebungen (Entwicklung, Test, Qualitätssicherung, Produktion etc.) benötigt werden und wie sie infrastrukturell umgesetzt werden sollen (z. B. unter Nutzung virtueller Maschinen (VM) oder Terminalserver-Dienste).

Planung der Einführung einer Anwendung

Die Einführung der neuen Anwendung ist zu planen. Hierfür sind im Pflichtenheft unter anderem folgende Punkte zu berücksichtigen:

- Bevor eine Anwendung in den Echtbetrieb übernommen werden darf, muss sie getestet und freigegeben werden. Im Pflichtenheft sind mindestens die geplanten Abläufe und Kriterien für die Tests und Freigaben zu nennen. Es hat sich als zweckmäßig erwiesen, im Pflichtenheft zumindest die für eine erfolgreiche Freigabe kritischen Testszenarien zu beschreiben (siehe CON.5.M2 Test und Freigabe von Fachanwendungen).
- Migration: Wenn durch die neue Anwendung eine bestehende Anwendung abgelöst wird, müssen Geschäftsprozesse und die IT-Umgebung angepasst und Datenbestände in die neue Anwendung migriert werden. Die Migrationsphase ist erfahrungsgemäß immer besonders sicherheitskritisch und muss sorgfältig vorbereitet und durchgeführt werden. Gegen Ende der Migrationsphase müssen auch die zugehörigen Daten in die neue Anwendung und die dort verwendeten Datenformate übertragen werden. Weitere Hinweise finden sich auch in Baustein SYS.1.1 Allgemeiner Server. Wertvolle Hinweise zur Planung des Vorgehens bei der Migration von Anwendungen gibt der Migrationsleitfaden der Beauftragten der Bundesregierung für Informationstechnik.

Sicherheitsfunktionen in der Anwendung:

Es muss festgelegt werden, welche Sicherheitsfunktionen die Anwendung enthalten soll und wie diese realisiert werden sollen (siehe auch CON.4 Auswahl und Einsatz von Standardsoftware). Diese können beinhalten:

- Verfügbarkeitskonzeption bzw. Redundanzkonzept (siehe CON.5.M13 Entwicklung eines Redundanzkonzeptes für Anwendungen)
- Mandantentrennung: Im Pflichtenheft muss ausformuliert werden, wie durch die Anwendung gewährleistet werden kann, dass die Mandanten sauber getrennt werden (siehe CON.5.M7 Erstellung eines Mandantenkonzeptes)
- Planung und Dokumentation des Einsatzes von Verschlüsselung, Checksummen und anderen kryptografischen Verfahren. Kryptografie kann bei geeigneter Einsatzkonzeption genutzt werden, um die Daten während des Transports innerhalb des der Anwendung, beim Transport über externe Schnittstellen und innerhalb der Anwendung gegen unbefugten Zugriff abzusichern.
- Die Planung und Umsetzung angemessener kryptographischer Verfahren ist eine komplexe Aufgabe, daher empfiehlt es sich, die Anforderungen und Überlegungen hierzu in einem Kryptokonzept zusammenzufassen, siehe Baustein CON.1 Kryptokonzept.
- Datensicherungskonzept (siehe Baustein CON.3 Datensicherungskonzept)
- Archivierungskonzept (siehe Baustein OPS.1.2.2 Archivierung): Bei der Archivierung ist darauf zu achten, dass alle Komponenten der Anwendung archiviert werden, die für eine eventuelle Wiederaufnahme des Betriebs erforderlich sind, also beispielsweise Software, Konfigurationsdaten und Inhaltsdaten. Unter Umständen kann es aber auch sinnvoll sein, Hardware-Komponenten zu archivieren, wie beispielsweise Authentisierungstoken. Das Archivierungskonzept sollte ein Rollenkonzept (siehe Baustein ORP.1 Organisation), ein Authentisierungskonzept (siehe CON.5.M1 Festlegung benötigter Sicherheitsfunktionen der Fachanwendung), eine Konzeption der Softwarepflege (siehe CON.5.A5 Aufrechterhaltung der Sicherheit im laufenden Anwendungsbetrieb) und eine Konzeption der Nutzung und Absicherung der externen Schnittstellen beinhalten.

Des Weiteren sind die Anforderungen an Form, Sprache, Tiefe und ggf. auch die Auslieferungszeitpunkte der Quellcodedokumentation sowie an Aufbau, Inhalt und Format (Papier, PDF-Dokument, Online-Hilfe) der Handbücher zu formulieren.

Dabei ist zu beschreiben, welche der an der Einführung der neuen Anwendung beteiligten Institutionen (Auftraggeber, Dienstleister etc.) welche der beschriebenen Aufgaben wahrnimmt.

Außerdem sollte ein Protokollierungskonzept erstellt werden, in dem festgelegt wird, welche Ereignisse in der Anwendung auf welche Art protokolliert werden sollen und wie mit den Protokolldaten umgegangen wird (siehe Baustein OPS.1.1.5 Protokollierung). Dabei sind unter anderem die folgenden Aspekte zu berücksichtigen:

- Welche Ereignisse sollen wie protokolliert werden?
- Wie wird die Löschung nicht mehr benötigter Protokolldaten umgesetzt?
- Wie soll der Zugriff auf die Protokolldaten abgesichert werden? Ist eine revisionssichere Speicherung erforderlich?
- Sollen zur Unterstützung der Auswertung standardisierte Reports eingesetzt werden?
- Sollen bei bestimmten, protokollierten Ereignissen in der Anwendung weitere Ereignisse ausgelöst werden (Einsatz von Security Incident und Event Monitoring, SIEM)?

Da bei der Protokollierung immer auch personenbezogene Daten anfallen, müssen hierbei auch die Vorgaben des Datenschutzes berücksichtigt werden.

CON.5.M7 Erstellung eines Mandantenkonzeptes [Leiter IT]

Häufig werden von mehreren Institutionen zentrale IT-Infrastrukturen oder Dienste eines Dienstleisters gemeinsam genutzt. Hierbei können auch Anwendungen gemeinsam betrieben und genutzt werden, wobei Datenhaltung und Datenverarbeitung z. B. infolge rechtlicher Anforderungen oder aufgrund von Betriebs- und Geschäftsgeheimnissen getrennt erfolgen müssen. In diesen Fällen wird häufig von mandantenfähigen Anwendungen gesprochen, wobei jeder nutzenden Institution ein Mandantenbereich, kurz Mandant, zugeordnet wird.

Ein Beispiel hierfür sind in der öffentlichen Verwaltung Registeranwendungen wie das ePersonenstandsregister, in denen mehrere Kommunen als eigenständige datenverarbeitende Stellen ihre Personenstandsdaten ablegen und verwalten. Cloud-basierende Anwendungen (auch als "Software as a Service", SaaS bezeichnet) sind ein weiteres Beispiel.

In jedem dieser Fälle ist durch ein geeignetes Mandantenkonzept sicherzustellen, dass die Anwendungen mandantenfähig betrieben werden. Dazu gehört, dass jede datenverarbeitende Stelle innerhalb ihres Bereichs, also ihres Mandantensystems, die fachlichen Vorgaben (z. B. bezogen auf Protokollierungsumfang und Speicherfristen) umsetzen sowie ihren Kontrollpflichten nachkommen kann. Das Mandantenkonzept ist durch den Betreiber der mandantenfähigen Anwendung zu erstellen und den nutzenden Institutionen zur Verfügung zu stellen. Diese müssen sich überzeugen, dass das Mandantenkonzept für ihren Schutzbedarf eine angemessene Sicherheit bietet, bevor sie solche Systeme oder Dienste gemeinsam mit weiteren Anwendern nutzen. Das Mandantenkonzept ist somit Bestandteil des Sicherheitskonzeptes, das für ein Outsourcingvorhaben zu stellen ist (siehe OPS.3.1 Outsourcing für Dienstleister, insbesondere OPS.3.1.A3 Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben).

Auch unter datenschutzrechtlichen Gesichtspunkten sind Anforderungen an die Trennung von Mandanten zu beachten. Hinweise dazu gibt die "Orientierungshilfe Mandantenfähigkeit" des Arbeitskreises Technik der Datenschutzbeauftragten des Bundes und der Länder.

Wenn eine Anwendung neu beschafft, erstellt oder wesentlich geändert wird, muss außerdem zunächst grundsätzlich sichergestellt sein, dass diese Anwendung Mandanten sauber trennen kann (siehe CON.5.M6 Umfassende Dokumentation der Anforderungen an die Anwendung).

Ein Mandantenkonzept sollte mindestens folgende Punkte berücksichtigen:

- Geeignete Rechtsgrundlagen: Rechtliche Vorgaben dürfen einem gemeinsamen, mandantenfähigen Verfahrensbetrieb nicht entgegenstehen. Ferner muss sichergestellt werden, dass die technische Ausgestaltung der Mandantentrennung dem Schutzbedarf der Daten in den jeweiligen Mandanten entspricht.
- Die Abgeschlossenheit von Transaktionen: Datenverarbeitungsschritte, die in einem Mandanten durchgeführt werden, dürfen nicht dazu führen, dass die Daten in anderen Mandanten verändert werden oder lesend auf sie zugegriffen werden kann.
- Konfigurative Unabhängigkeit der Mandanten untereinander: Es sollten mindestens zwei administrative Ebenen vorhanden sein. Die erste Ebene dient der Mandantenadministration: Hier werden Mandantensysteme eingerichtet und gelöscht, mandantenübergreifende konfigurative Einstellungen durchgeführt, die Rollen der Mandantenadministratoren zugewiesen, die mandantenübergreifende Protokollierung angestoßen und deren Revision durchgeführt. Die zweite Ebene dient der Administration eines Mandantensystems: Hier werden die Berechtigungen im Mandantensystem vergeben, mandanteninterne Konfigurationen durchgeführt, die mandanteninterne Protokollierung konfiguriert und die Protokollrevision durchgeführt.
- Trennung von Berechtigungskontexten: Jeder Mandant hat seinen eigenen, abgeschlossenen Berechtigungskontext. Die Berechtigungen in einem Mandantensystem dürfen sich nicht in anderen Mandantensystemen auswirken. Die Vergabe oder Veränderung von Berechtigungen durch die Administratoren der jeweiligen Mandanten darf sich nicht auf Berechtigungen in anderen Mandanten auswirken.
- Es muss eine administrative Ebene zur Mandantenadministration seitens des Betreibers geben, die aber keine Berechtigung zur Verarbeitung von Daten innerhalb eines Mandanten besitzen sollte.
- Trennung von Protokollierungskontexten: Protokollrevisoren eines Mandatensystems dürfen keinen Zugriff auf Protokolldaten anderer Mandantensysteme haben. Beispielsweise können Mandanten eigene Log-Dateien haben. Eine andere Lösung könnte sein, dass eine Institution über vom Dienstleister entsprechend eingerichtete Filter oder Report-Generatoren auf die Protokolldaten ihres Mandanten zugreifen kann.
- Beschränkung der mandantenübergreifenden Datenverarbeitung: Die Ebene der Mandantenadministration sollte grundsätzlich keine Verarbeitung von Daten innerhalb eines Mandanten außerhalb der Mandantenadministration zulassen. Der Datenaustausch zwischen Mandanten sollte über definierte und geeignet abgesicherte Schnittstellen erfolgen (siehe Schnittstellenkonzept).

Die Umsetzung dieser Anforderungen kann auf vielfältige Weise erfolgen. Eine herausragende Rolle spielt dabei ein geeignetes Rollen- und Berechtigungskonzept innerhalb von Anwendungen. Darüber hinaus können auf der Infrastruktur- und Diensteebene hierzu z. B. Virtualisierungstechniken eingesetzt werden wie:

- Einsatz verschiedener Datenbanken (auch Instanzen genannt) in einem gemeinsamen Datenbankmanagementsystem (DBMS)
- VPD (Virtual Private Database) auf der Diensteebene bei Datenbanken
- Speicherung von mit einem Mandantenattribut versehenen Datensätzen in einer gemeinsamen Datenbank und gemeinsamen Tabellen, sodass die Mandantentrennung durch die Anwendung erfolgt.
- Virtuelle Maschinen auf der Systemebene
- VLAN (Virtual LAN), VRF (Virtual Routing and Forwarding), VPN (Virtual Private Network) in der Netzinfrastruktur.

Der Auftraggeber sollte prüfen, ob die vom Dienstleister gewählte Lösung zur Mandantentrennung effektiv ist.

CON.5.M8 Geeignete Steuerung der Anwendungsentwicklung [Leiter IT]

Kann für einen bestimmten Einsatzzweck keine Standardsoftware beschafft werden, wird die Entwicklung von Individualsoftware erforderlich. Dies kann in der Institution selbst oder mithilfe externer Auftragnehmer erfolgen.

Neben wirtschaftlichen Aspekten ist eine geeignete Steuerung der Softwareentwicklung auch aus Sicherheitsgesichtspunkten wichtig, weil sie hilft, Fehler in Anwendungen und Sicherheitslücken zu vermeiden. Je früher Fehler und Sicherheitsrisiken identifiziert werden, desto einfacher ist es, diese zu beheben.

Für die Steuerung der Entwicklung und das Projektmanagement sollte ein geeignetes Steuerungs- und Projektmanagementmodell festgelegt werden, das den besonderen Gegebenheiten der Institution und den dort eingesetzten Methoden von Softwareentwicklungsprojekten Rechnung trägt. Dieses sollte die folgenden Aspekte berücksichtigen:

- Das für die Entwicklung vorgesehene Personal sollte über die notwendige Qualifizierung verfügen.
- Für die Steuerung der Erstellung und Pflege der Anwendungen sollte ein Gesamtprozess eingeführt werden, der alle Phasen des Lebenszyklus (Application Lifecycle Management, ALM) abdeckt. Dabei sollten geeignete Phasen der Softwareentwicklung berücksichtigt werden, um die notwendigen Aktivitäten entsprechend aufteilen und bearbeiten zu können (Geschäftsprozessmodellierung, Anforderungsanalyse, Softwaredesign, Implementierung, Test, Auslieferung etc.). Für die erfolgreiche Einführung des Gesamtprozesses hat sich die sorgfältige Beschreibung und Abgrenzung der benötigten Rollen und Funktionsträger als besonders wichtig erwiesen.
- Zur geordneten Durchführung des Anwendungsprojektes sollten die benötigten Voraussetzungen geschaffen werden. Diese beinhalten die Bestellung eines Projektleiters, die Besetzung der Rollen im beschriebenen Gesamtprozess und die Auswahl eines Vorgehensmodells für die Entwicklung, das für die jeweilige Institution sowie die Art und Größe des Softwareprojektes geeignet ist. Dies kann beispielsweise sequenzielles Durchlaufen der Phasen (Wasserfallmodell) oder iteratives Durchlaufen (Spiralmodell) vorsehen.
- Die Risiken bei der Softwareentwicklung sind zu bewerten und zu behandeln. Hierbei sind spezifische Sicherheitsrisiken zu berücksichtigen, die üblicherweise durch Einsatz von Sicherheitsfunktionen reduziert werden, und Risiken im Entwicklungsvorhaben selbst, wie unzureichende Dokumentation, unzureichende Qualitätssicherungsmaßnahmen, Überschreiten des Zeitplans etc.. Auch die Risiken im Entwicklungsvorhaben können sich mittelbar auf die Sicherheit der Anwendung auswirken, etwa wenn aus Zeitdruck Sicherheitsfunktionen nicht oder nur unzureichend implementiert werden.
- Es müssen die Qualitätsaspekte des Entwicklungsprozesses ausreichend berücksichtigt werden, ie auch für die Gesamtsicherheit wichtig sind. So lässt sich beispielsweise gut dokumentierter und strukturierter Code nicht nur einfacher warten, auch sicherheitsrelevante Probleme lassen sich schneller identifizieren.

Für die Entwicklung von Software haben sich eine Reihe von Vorgehensmodellen und Best Practices bewährt. Diese lassen sich grob in zwei Kategorien unterscheiden:

- Schwergewichtige Vorgehensmodelle: Diese haben einen formalen Charakter, verfolgen eher einen vorab festgelegten Plan und legen ein starkes Gewicht auf Verträge und Dokumentation. Sie eignen sich vor allem für große Projektteams oder bei einer sehr formalen Beziehung zwischen Auftraggeber und Auftragnehmer und setzen eine umfassende Anforderungsklärung zum Projektbeginn voraus. Bekannte Vertreter sind das V-Modell XT und der Rational Unified Process (RUP).
- Leichtgewichtige, agile Vorgehensmodelle: Sie setzen stärker auf die persönliche Interaktion der Projektbeteiligten und weniger auf die formale Durchführung und eignen sich für kleinere Projekte oder Projekte mit intensiver Beteiligung des Auftraggebers. Sie bieten die Möglichkeit, vage Anforderungen während des Projektverlaufs zu präzisieren oder auf Änderungen der Anforderungen flexibel zu reagieren. Beispiele für agile Vorgehensmodelle sind Scrum, Kanban, Crystal Clear.

Vorgehensmodelle lassen sich kombinieren: So können beispielsweise Arbeitsmethoden aus eXtreme Programming (Pair Programming) bei Scrum angewendet werden. Innerhalb eines V-Modell XT-Projektes können kleine Entwicklungszyklen als Scrum-Sprints angelegt werden.

Die für Softwareentwicklung relevanten Teilgebiete und Prozesse werden unter anderem beschrieben in:

- IEEE Software Body of Knowledge (SWEBOK) und
- ISO/IEC 12207 "Systems and software engineering - Software life cycle processes"

Auch für die Qualitätssicherung im Softwareentwicklungsprozess existieren verschiedene Vorgehensmodelle und -methoden. Dazu gehören unter anderem CMMI (Capability Maturity Model Integration) und SPICE (Software Process Improvement and Capability Determination) bzw. ISO/IEC 15504 "Information technology - Process assessment".

Ebenfalls relevant in diesem Bereich ist die Normenreihe ISO 250xx. Die Norm ISO/IEC 25000 "Software-Engineering - Qualitätskriterien und Bewertung von Softwareprodukten (SQuaRE) - Leitfaden für SquaRE" gibt einen Überblick über die Grundbegriffe und Prinzipien dieser Reihe.

Es muss festgelegt werden, welche Qualitätssicherungsmethode und welches konkrete Verfahren in der Institution oder für das jeweilige Projekt genutzt wird. Dabei sollten auch Sicherheitsaspekte ausreichend berücksichtigt werden.

Aus wirtschaftlichen Gründen sind in der Regel nicht alle Arten von Prüfungen in allen möglichen Tiefen möglich. Daher muss entschieden werden, welche davon zu welchem Zeitpunkt und für welche Teile der Anwendung sinnvoll sind. Dabei ist sicherzustellen, dass die Sicherheitsanforderungen ausreichend abgedeckt sind.

CON.5.M9 Außerbetriebnahme von Anwendungen [Leiter IT]

Bevor Anwendungen außer Betrieb genommen werden, sollte geklärt werden, wie dies ablaufen soll und wie mit den in diesen gespeicherten Informationen umzugehen ist. Bei der Planung der Außerbetriebnahme von Anwendungen sollten folgende Aspekte Berücksichtigung finden:

- Was soll mit den Daten der Anwendungen geschehen? Werden diese auf andere Systeme übertragen (Migration), archiviert oder gelöscht?
- Sollen die für die Anwendungen genutzten IT-Systeme und Datenträger vernichtet oder weiterverwendet werden? Bei Weiterverwendung sollte darauf geachtet werden, dass alle Daten sicher gelöscht werden.

Dabei sollte vor allem sichergestellt werden, dass weder wichtige Daten verloren gehen, noch, dass vertrauliche Daten auf ausgesonderten IT-Systemen oder Datenträgern zurück bleiben. Daten, die noch benötigt werden, müssen gesichert bzw. archiviert werden. Es sollte überprüft werden, dass wirklich alle Daten korrekt gesichert wurden. Weitere Informationen zu diesem Themenkomplex finden sich in den Bausteinen CON.3 Datensicherungskonzept und OPS 1.2.2 Archivierung.

Bei der Deinstallation von Anwendungen sollte darauf geachtet werden, dass neben der Anwendung selber alle Konfigurationsparameter (gespeichert in Konfigurationsdateien oder der Registry des Betriebssystems) und die mit der Anwendung verarbeiteten Daten gelöscht werden. Auch sollten durch die Installation veränderte Bibliotheken des Betriebssystems wieder durch die Version des Betriebssystems ersetzt werden. Häufig liefern die Softwarehersteller zu diesem Zweck Deinstallationsroutinen, aber auch Betriebssysteme bringen zur Unterstützung der Deinstallation Werkzeuge mit.

Außerdem sollte geprüft werden, ob noch Datensicherungsmedien vorhanden sind, die für die Anwendungen benutzt wurden. Auch diese müssen gelöscht oder unbrauchbar gemacht werden, wenn die darauf gespeicherten Daten nicht mehr benötigt werden.

Bei der Weiterverwendung von IT-Systemen sollte ferner darauf geachtet werden, dass Datenträger sicher gelöscht werden. Da die Mittel der Betriebssysteme in der Regel kein sicheres Löschen sicherstellen, sollten hierzu Spezialanwendungen verwendet werden. Darüber hinaus sollte darauf geachtet werden, dass für viele Typen von Datenträgern, z.B. Microfishes oder Chipkarten keine zuverlässigen Methoden zum Löschen existieren. In diesen Fällen sollten Datenträger daher geeignet physikalisch vernichtet werden. Hinweise zu sicheren Vernichtung von Datenträgern können dem Baustein CON.6 Löschen und Vernichten entnommen werden.

Die Vorgehensweise für die Außerbetriebnahme von Anwendungen, IT-Systemen und Datenträgern innerhalb der Institution sollte nachvollziehbar dokumentiert sein. Es wird empfohlen, anhand der oben gegebenen Empfehlungen eine Checkliste zu erstellen, die bei der Außerbetriebnahme von Anwendungen abgearbeitet werden kann. Auf diese Weise kann vermieden werden, dass einzelne Schritte vergessen werden. Es empfiehlt sich, dass die einzelnen Schritte vom jeweils Zuständigen schriftlich bestätigt werden.

CON.5.M10 Notfallvorsorge für Anwendungen [Leiter IT]

Alle Anwendungen sind in die Planung zur Notfallvorsorge und in das Notfallmanagement aufzunehmen (siehe Baustein DER.4 Notfallmanagement).

- Die Bedeutung der jeweiligen Anwendung im Rahmen der Geschäfts- oder Verwaltungsprozesse der Institution ist festzustellen und zu dokumentieren. Darauf aufbauend ist die Anwendung im Vergleich mit anderen Anwendungen zu priorisieren.
- Die getroffenen technischen und organisatorischen Maßnahmen zur Notfallvorsorge sind zu beschreiben und im Notfallmanagementkonzept zu beschreiben.
- Es ist zu planen, wie bei einem eingeschränkten IT-Betrieb vorgegangen werden sollte (Wer sollte wo welche Aufgaben mit der Anwendung bevorzugt wahrnehmen? Welche Aufgaben können zurückgestellt werden?).
- Die Wiederherstellung des geregelten Anwendungsbetriebes ist zu planen.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

CON.5.M11 Geeignete und rechtskonforme Beschaffung (CIA)

Für ein Vergabeverfahren zur Beschaffung einer Standard- oder Individualsoftware kann es eine Reihe von Vorgaben geben, die zu beachten sind. Während dies im Bereich von Unternehmen meistens eigene Vorgaben oder Konzernrichtlinien sind, sind für die öffentliche Hand in Deutschland die folgenden Vorgaben zu berücksichtigen:

- Vergabeordnung der Länder und des Bundes (insbesondere die Vergabeordnung für Leistungen (VOL) und die Vergabeordnung für freiberufliche Leistungen (VOF)). Diese regeln detailliert, wie (zum Beispiel als Freihandvergaben, öffentliche Ausschreibungen etc.) und in welchen Schritten Vergabeverfahren durchzuführen sind.
- Mindestanforderungen der Rechnungshöfe zum Einsatz der Informations- und Kommunikationstechnik. Diese beschreiben die Vorgaben der Rechnungshöfe für Anwendungen, mit denen Mittel der öffentlichen Hand verwaltet werden.

Jede Institution sollte im Vorfeld von Beschaffungen geklärt haben, welche rechtlichen oder sonstigen Rahmenbedingungen dabei zugrunde zu legen sind. Für Beschaffungen und Auftragsvergaben sollte es definierte Prozesse und festgelegte Ansprechpartner in der Institution geben (siehe CON.5.M6 Umfassende Dokumentation der Anforderungen an die Anwendung).

In jedem Falle ist es sinnvoll, frühzeitig zu klären, welche Rolle Zertifikate bei der Vergabeentscheidung spielen sollen. Dazu gehören Zertifikate, die die Sicherheit von Produkten bewerten wie die Common Criteria, solche, die die Managementsysteme bewerten, wie das Zertifikat " ISO 27001 auf Basis IT-Grundschutz", und auch Personenzertifikate).

Vertragsgestaltung

Bei Beschaffung, Entwicklung oder Betrieb einer Anwendung kann sich eine Institution auf einen oder mehrere Dienstleister abstützen. Dies können interne oder externe Dienstleister sein. Typischerweise sind mindestens drei Parteien zu unterscheiden: die späteren Nutzer, Entwickler und Betreiber der Anwendung. Wird die Anwendung von Externen entwickelt oder betrieben, müssen geeignete vertragliche Rahmenbedingungen geschaffen werden.

Die Umsetzung der im Lasten- und Pflichtenheft sowie in den Teilkonzepten vorgegebenen, auch sicherheitstechnischen Eigenschaften einer Anwendung ist vertraglich mit den beteiligten Institutionen und Dienstleistern zu vereinbaren.

Hierbei sind unter Sicherheitsgesichtspunkten insbesondere die folgenden Aspekte zu berücksichtigen:

- Der Liefer- bzw. Leistungsumfang (Funktionsumfang einschließlich Sicherheitsfunktionen, Bereitstellungsformat, Lizenztyp, Dokumentation, Handbücher etc.) sollte geeignet beschrieben werden.
- Es sollten Vereinbarungen über die Softwarepflege getroffen werden (siehe CON.5.M5 Sicherer Betrieb einer Fachanwendung). Bei Entwicklungen im Auftrag müssen geeignete Nutzungsrechte für den erzeugten Quellcode und Zugriff auf diesen vereinbart werden (siehe auch CON.5.M12 Treuhänderische Hinterlegung).

Beim Betrieb einer Anwendung durch einen Dienstleister sind die Maßnahmen aus dem Baustein OPS.2.1 Outsourcing für Kunden zu berücksichtigen.

In der öffentlichen Verwaltung in Deutschland sind die "Ergänzenden Vertragsbedingungen für die Beschaffung von Informationstechnik" (EVB-IT) rechtlich vorgegeben (siehe auch § 9 Abs. 1 Satz 2 und § 11 EG Abs. 1 Satz 2 VOL/A und § 55 BHO). Diese enthalten sowohl Vertragsvorlagen für die Entwicklung als auch den Betrieb einer Anwendung durch einen Dienstleister.

CON.5.M12 Treuhänderische Hinterlegung (CA)

Je geschäftskritischer ein Prozess ist, desto wichtiger ist es, diesen gegen einen Ausfall abzusichern. Bei der Lieferung vieler Produkte, die Geschäftsprozesse unterstützen (Software, Maschinen, Automaten etc.), erhält der Käufer nicht alle Bestandteile, die zur Wartung des Produktes notwendig sind. Die Wartung wird in diesem Fall häufig durch den Lieferanten sichergestellt. Fällt der Hersteller oder Lieferant aus, ist das Produkt unter Umständen nicht mehr wartbar. Es sollte geprüft werden, ob dieses Risiko durch eine Hinterlegung (Escrow) der fehlenden Bestandteile gemindert werden kann.

Escrow ist die "treuhänderische" Hinterlegung von nicht im Lieferumfang enthaltenen Materialien, die zur Wartung und Pflege eines Produktes notwendig sind, bei einem Dritten (Escrow-Agentur). Bei diesen Materialien kann es sich um Software (ausführbar oder als Quellcode), Handbücher, Konstruktionspläne, Konfigurationszustände, Abnahmedaten, Schlüssel, Passwörter oder andere Bestandteile handeln.

Je nach Art des Produktes können sich Unternehmen oder Behörden mit diesem Instrument beispielsweise gegen folgende Risiken absichern:

- Wegfall der Leistungen eines Auftragnehmers im Hinblick auf Fertigstellung, Pflege oder Weiterentwicklung des Produktes
- Ausfall von Zulieferern von Bauteilen und Baugruppen
- Speziell im Fall von Software: Verlust von Quell- und/oder Objektcodes bei Großschäden im IT-Bereich
- Fehlende Möglichkeiten nachzuweisen, wann welcher Versionsstand vorgelegen hat, beispielsweise im Hinblick auf Urheberrecht, Haftung oder Insolvenz

Funktionsweise

Der Anwender eines Produktes sichert mit Escrow die kontinuierliche Fortführung eines oder mehrerer geschäftskritischer Prozesse. Hierzu erhält er das Recht, unter definierten Bedingungen auf das hinterlegte Material zuzugreifen und dieses zur Pflege des Produktes zu nutzen, z. B. wenn der Lieferant die im Vertrag festgelegten Leistungen gegenüber dem Anwender nicht erbringt. Auf der anderen Seite schützt der Lieferant seine Wettbewerbsvorteile und seine Betriebsgeheimnisse, solange wie er seinen Verpflichtungen nachkommt. Die Escrow-Agentur prüft und verwahrt das Material für beide Parteien.

Anwender und Lieferant schließen mit der Escrow-Agentur einen Vertrag, der mindestens folgende Aspekte definiert:

- Sicherung der Rechte und Bedingungen zur Herausgabe des hinterlegten Materials
- Verifikation des Materials
- Fachgerechte Lagerung des Materials und angemessene Absicherung
- Aktualisierung des Materials

Die Bedingungen der Hinterlegung und insbesondere auch die Pflichten der Escrow-Agentur im Hinblick auf die Verifizierung und die Herausgabe sind im Escrow-Vertrag genau zu beschreiben. Die individuelle Ausgestaltung dieses Vertrages hängt sowohl von der Einschätzung der Risiken, gegen die sich der Hinterleger absichern will, als auch vom Rechtsraum ab.

Folgende Hinweise sollten bei der Formulierung und beim Abschluss des Escrow-Vertrages beachtet werden:

- Diskrepanzen zwischen dem Nutzungsvertrag und dem Escrow-Vertrag müssen vermieden werden.
- Hilfreich ist es, den Nutzungsvertrag und den Escrow-Vertrag parallel abzuschließen. Eine zeitliche Verschiebung könnte Nachteile für den Anwender mit sich bringen.
- Je nach Rechtsraum kann ein Escrow-Vertrag gefährdet werden, wenn er zu spät abgeschlossen wird, z. B. kurz vor der Insolvenz des Lieferanten.
- Die Herausgabe des Materials sollte klar definiert sein. Der Escrow-Vertrag sollte ein genaues Verfahren beinhalten, wie die Herausgabe einzuleiten und durchzuführen ist.
- Die Escrow-Agentur muss für beide Seiten vertrauenswürdig sein und sichere und geeignete Aufbewahrungsmöglichkeiten für das zu hinterlegende Material bieten.
- Die technischen Aspekte der Hinterlegung müssen geregelt werden. Die Escrow-Agentur sollte die nötige technische Kompetenz aufweisen, um die Weiterverwendbarkeit des Materials prüfen und die Nachsorge gegenüber Updates leisten zu können.
- Die Verwendbarkeit des Materials nach der Herausgabe ist bereits bei der Zulieferung geeignet zu prüfen. Die Prüfungstiefe hängt von der Einschätzung der Risiken und der verwendeten Technik ab. Beispiele für Prüfungen sind das Kompilieren einer Software aus dem hinterlegten Quellcode oder das Durchspielen einer Montage-Anleitung.
- Durch die Festlegung geeigneter Update-Zyklen ist das Material aktuell zu halten. Welche Zyklen erforderlich sind, hängt vorrangig von der Einschätzung der Risiken und von den Produktionsprozessen des Anwenders ab.

CON.5.M13 Entwicklung eines Redundanzkonzeptes für Anwendungen [Leiter IT] (A)

Besteht bei einem Geschäftsprozess oder bestimmten Informationen hoher Schutzbedarf hinsichtlich des Grundwertes der Verfügbarkeit, so kann hierfür die Erstellung und Umsetzung eines Redundanzkonzeptes sinnvoll sein (allgemeine Informationen zur Redundanz sind in der entsprechenden Maßnahme "Redundanz, Modularität und Skalierbarkeit in der technischen Infrastruktur" im Baustein INF.2 Rechenzentrum sowie Serverraum zu finden). Für ein Redundanzkonzept wird auf Grundlage einer Risikoanalyse (siehe BSI-Standard 200-3) ermittelt, auf welche Raum- und Gebäudeinfrastrukturen, Systeme, Netzkomponenten und Leitungswege sich der hohe Schutzbedarf des Geschäftsprozesses oder der Informationen auswirkt. Darauf aufbauend wird im Redundanzkonzept festgelegt, mit welchen technischen und organisatorischen Maßnahmen die benötigte Verfügbarkeit sichergestellt werden soll.

Das Redundanzkonzept muss auf Plausibilität mit dem allgemeinen Notfallkonzept (siehe B*austein DER.4 Notfallmanagement*) geprüft und bei Bedarf entsprechend den allgemeinen Anforderungen angepasst werden. Die Maßnahmen aus dem Redundanzkonzept müssen getestet und geübt werden. Diese Tests und Übungen sind mit den Tests und Übungen des Notfallmanagements der Institution abzustimmen. Je nach Anforderung an die Verfügbarkeit der jeweiligen Elemente des Informationsverbundes können die folgenden Ansätze berücksichtigt werden, um deren Ausfälle überbrücken zu können:

Verfahren

- Es sollten organisatorische Regelungen für einen Notbetrieb erstellt werden. Diese Regelungen können für einige Anwendungen vorsehen, zum papiergestützten Arbeiten zurückzukehren. Zudem sollten Anwendungen priorisiert werden und überlegt werden, Anwendungen, die eine geringere Priorität haben, abzuschalten und die damit freigewordenen Ressourcen höher priorisierten Anwendungen zur Verfügung zu stellen.
- Es sollte geprüft werden, ob Räumlichkeiten, IT-Systeme und weitere Infrastrukturen von Datenverarbeitungsanlagen in anderen Institutionen genutzt werden können, mit denen eine Kooperation besteht.
- Es ist für Anwendungen mit höherer Priorität zu prüfen, ob die Anwendungen fähig sind, Redundanz auf der Systemebene zu nutzen. Dazu gehören Load-Balancing-, Cluster- oder Cloud-Fähigkeiten. Diese können entsprechend genutzt werden, unter Umständen müssen sie auch zunächst hergestellt werden.
- Es ist für Anwendungen mit höherer Priorität zu prüfen, ob diese Anwendungen fähig sind, Redundanz auf der Diensteebene zu benutzen, z. B. kurzfristiges Schwenken auf eine alternative Datenbank. Diese können entsprechend genutzt werden, unter Umständen müssen sie auch zunächst hergestellt werden.

Systeme

- Teil- oder Vollredundanz auf Komponentenebene: Anwendungen benötigen zum Betrieb eine Reihe von Komponenten. Zur Steigerung der Verfügbarkeit können diese teil- oder vollredundant ausgelegt werden, beispielsweise durch Einsatz von Festplatten- s, redundanten Netzwerkkarten, Netzteilen etc.
- Es sollte geprüft werden, ob Ersatzsysteme im Cold-, Warm- oder Hot-Standby-System betrieben werden sollten oder System-Cluster eingesetzt werden sollten. Bei Cold-Standby-Systemen sind Ersatzsysteme vorkonfiguriert, aber ausgeschaltet und enthalten nicht alle aktuellen Daten. Bei Warm-Standby-Systemen sind Ersatzsysteme vorkonfiguriert und mit einem Datenbestand aus dem letzten Backup versorgt, aber ausgeschaltet. Bei Hot-Standby-Systemen laufen Ersatzsysteme und übernehmen bei Ausfall die Funktion des Hauptsystems. Zusätzlich enthalten die Ersatzsysteme im Hot-Standby alle nötigen Daten über eine synchrone Spiegelung und können im Idealfall sofort die Arbeit des ausgefallenen Systems übernehmen, ohne dass ein Datenverlust entsteht oder der Anwender den Ausfall bemerkt. Bei System-Clustern wird die Anwendung über mehrere Systeme verteilt, wobei ein oder mehrere Systeme die Lastverteilung vornehmen und die übrigen die Aufgaben bearbeiten. Dies setzt die Clusterfähigkeit der fraglichen Anwendung voraus, siehe Maßnahme "Verwendung von hochverfügbaren Architekturen für Server" im Baustein SYS.1.1 Allgemeiner Server). Clusterlösungen können auch in Kombination mit Virtualisierung von Maschinen (Hardware-Emulation oder Hardware-Virtualisierung) eingesetzt werden (siehe *Baustein SYS.1.5 Virtualisierung*).

Kommunikationsverbindungen

Falls die Anwendung Kommunikationsverbindungen zu ihrem Betrieb benötigt, können zur Steigerung der Verfügbarkeit:

- zusätzlich alternative Kommunikationsverbindungen wie Fax, Telefon, Mobiltelefon und Sprechfunkverbindungen vorgesehen werden (siehe NET.1.1 Netzarchitektur und -design),
- die für die Kommunikationsverbindungen genutzten physischen oder virtuellen Leitungen redundant ausgelegt werden (siehe INF.3 Elektrotechnische Verkabelung),
- die genutzten zentralen Netzkomponenten redundant ausgelegt werden (siehe NET.1.1 Netzarchitektur und -design).

3 Weiterführende Informationen

3.1 Wissenswertes

Bestandsliste über die Anwendungen

Alle Anwendungen, die auf IT-Systemen der Institution eingesetzt werden, sollten in einer Bestandsliste aufgeführt werden. Die Bestandslisten sollten immer auf dem aktuellen Stand sein. Darüber hinaus sollten die verschiedenen Konfigurationen der installierten Anwendungen dokumentiert werden. Solche Bestandslisten dienen verschiedenen Zielen:

- Sie erleichtern Risikobewertungen.
- Unautorisierte Anwendungen können einfacher identifiziert werden.
- Sie unterstützen das Lizenz- und Konfigurationsmanagement (siehe auch Baustein CON.4 Auswahl und Einsatz von Standardsoftware). Auch in ITIL (Prozess "Asset and Configuration Management") findet sich die Anforderung, eingesetzte Software in einer Configuration Management Database (CMDB) aufzuführen.
- Sie können für das datenschutzrechtliche Verfahrensverzeichnis herangezogen werden. In diesem müssen die Verfahren bzw. Prozesse zur Verarbeitung personenbezogener Daten mit der zugehörigen Datenverarbeitungsinfrastruktur benannt werden. Die dabei eingesetzte Software gehört in das Verzeichnis.

Rechtzeitige Beteiligung der Personalvertretung

Bei allen Maßnahmen, die prinzipiell die Verhaltens- oder Leistungsüberwachung von Mitarbeitern ermöglichen, zum Beispiel Protokollierung, bedarf es der Mitbestimmung der Personalvertretung. Grundlage dessen sind in Deutschland die Betriebsverfassungs- und Personalvertretungsgesetze von Bund und Ländern. In anderen Ländern ist die Einbeziehung der Personalvertretung nicht immer erforderlich. Die rechtzeitige und umfassende Information des Betriebs- oder Personalrates empfiehlt sich aber grundsätzlich, da dies die Akzeptanz von Maßnahmen im Bereich der Informationssicherheit verbessert und Zeitverzögerungen bei deren Umsetzung verhindern kann.

Bei bereits bestehendem Verdacht, dass ein Sicherheitsvorfall (siehe Baustein DER 2.1 Behandlung von Sicherheitsvorfällen) durch einen internen Mitarbeiter ausgelöst wurde und entsprechende Nachforschungen durchgeführt werden sollen, die auf Sanktionen hinauslaufen, sind die Beteiligungsrechte des Personal- beziehungsweise Betriebsrates unbedingt zu beachten. Unterbleibt eine ordnungsgemäße Beteiligung der Mitarbeitervertretung, kann das eventuell erforderliche weitere Verfahren (gegebenenfalls vor dem Arbeitsgericht) je nach Schwere des Vorfalls für eine Abmahnung oder Kündigung aufgrund von Formfehlern gravierend beeinflusst werden.

Große Outsourcing-Dienstleister berichten aus der Praxis, dass eine frühzeitige Einbindung der Personalvertretung des Auftraggebers, möglichst schon in der Angebotsphase, sehr zum Gelingen des Projektes beitragen kann. Wechselbereitschaft der Mitarbeiter, Motivation, Arbeitszufriedenheit und zügige Projektabwicklung können durch Kooperation aller Beteiligten positiv beeinflusst werden. Gleiches gilt für die geplante Nutzung von Cloud-Diensten. Als Besonderheit ist hierbei anzusehen, dass die oben genannten Vorgaben auch dann zu beachten sind, wenn sich eine Institution für eine Private Cloud entscheidet.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Entwicklung und Einsatz von Allgemeinen Anwendungen" finden sich unter anderem in folgenden Veröffentlichungen:

[12207] ISO/IEC 12207:2008

System and software engineering - Software life cycle process, International Organziation for Standardization (Hrsg.), ISO/IEC JTC 1/SC 7, Februar 2008

[27001A14] ISO/IEC 27001:2013

Information technology - Security technigues - Information security management systems - Requirements, insbesonder Annex A, A.14 System acquisition, development and maintenance, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/SC 27, Oktober 2013

[CC] Common Criteria for Information Technology Security Evaluation (CC)

(siehe auch ISO/IEC 15408-2:2008 ISO, Information technology - Security techniques - Evaluation criteria for IT security), www.commoncriteriaportal.org , zuletzt abgerufen am 24.08.2018

[CMMI] CMMI (Capability Maturity Model Integrated)

CMMI Institute,
http://www.cmmiinstitute.com zuletzt abgerufen am 01.09.2018

[EVBIT] Ergänzende Vertragsbedingnungen für die Beschaffung von Informationstechnik (EVB-IT)

Beauftragter der Bundesregierung für Informationstechnik
http://www.cio.bund.de/Web/DE/IT-Beschaffung/it_beschaffung_node.html
zuletzt abgerufen am 01.09.2018

[ISFBA] The Standard of Good Practice for Information Security

Area BA Business Application Management, Information Security Forum (ISF), June 2018

[MIGR] Migrationsleitfaden

Leitfaden für die Migration von Software, Beauftragte der Bundesregierung für Informationstechnik, Version 4.0, März 2012

http://www.cio.bund.de/Web/DE/Architekturen-und-Standards/Migrationsleitfaden-und-Migrationshilfen/migrationsleitfaden_node.html zuletzt abgerufen am 01.09.2018

[NIST80053F145] Security and Privacy Controls for Federal Information Systems and Organizations

NIST Special Publication 800-53, Revision 4, insbesondere Appendix F-PS Page F-145, Family: System and Services acquisition, Family: System and communications protection and Family: System and information integrity, April 2013

[OHM] Technische und organisatorische Anforderungen an die Trennung von automatisierten Verfahren bei der Benutzung einer gemeinsamen IT-Infrastruktur - Orientierungshilfe Mandantenfähigkeit

Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Version 1.0 vom 11.10.2012

http://www.lfd.niedersachsen.de/startseite/technik_und_organisation/orientierungshilfen_und_handlungsempfehlungen/mandantenfaehigkeit/mandantenfaehigkeit-109520.htmlzuletzt abgerufen am 01.09.2018

[OWASP] Open Web Application Security Project (OWASP)

https://www.owasp.org, zuletzt abgerufen am 05.10.2018

[RH] IuK Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informations- und Kommunikationstechnik

https://www.bundesrechnungshof.de/de/veroeffentlichungen/weitere/mindestanforderungen-der-rechnungshoefe-des-bundes-und-der-laender-zum-einsatz-der-informations-und-kommunikationstechnik/view) zuletzt abgerufen am 01.09.2018

[SAGA] Standards und Architekturen für eGovernment (SAGA)

http://www.cio.bund.de/Web/DE/Architekturen-und-Standards/SAGA/saga_node.html zuletzt abgerufen am 01.09.2018

[SECO] Die zehn goldenen Regeln der IT-Sicherheit

aus dem Secologic-Projekt des BMWi

http://www.secologic.org/downloads/software/070205_10GoldenRules_SAP_CoBa_V1.pdf zuletzt abgerufen am 01.09.2018

[SWEBOK] IEEE Software Body of Knowledge (SWEBOK)

[TR] Technische Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik

https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/index_htm.html zuletzt abgerufen am 01.09.2018

[VMXT] V-Modell XT

Verein zur Weiterentwicklung des V-Modell XT e.V. (Weit e.V.)

http://www.cio.bund.de/SharedDocs/Kurzmeldungen/DE/2017/20170106_vmodellxt_vs_21.html zuletzt abgerufen am 01.09.2018

[VOL] Vergabeordnung der Länder und des Bundes

insbesondere die Vergabeordnung für Leistungen (VOL) und die Vergabeordnung für freiberufliche Leistungen (VOF), siehe http://www.bmwi.de/Redaktion/DE/Artikel/Wirtschaft/vergabe-uebersicht-und-rechtsgrundlagen.html zuletzt abgerufen am 01.09.2018

Umsetzungshinweise zum Baustein CON.7 Informationssicherheit auf Auslandsreisen

1 Beschreibung

1.1 Einleitung

Zahl und Umfang berufsbedingt notwendiger Reisetätigkeiten hat in den letzten Jahren durch die Globalisierung und die dadurch zunehmende internationale Vernetzung von Behörden und Unternehmen stetig zugenommen. Dabei ist das Mitführen von Informationstechnik, sei es z. B. das Notebook, Smartphone, Tablet, Wechselfestplatte oder USB-Stick, sowie Informationen in anderer papierener oder geistiger Form auf Auslandsreisen in der heutigen Gesellschaft gänzlich unabdingbar geworden, um die Aufnahme von Geschäftstätigkeiten außerhalb des regulären Arbeitsumfeldes gewährleisten zu können. Bei Geschäftsreisen, vor allem bei Auslandsreisen, sind eine Vielzahl an Bedrohungen und Risiken für die Informationssicherheit zu beachten, die im normalen Geschäftsbetrieb nicht existieren.

Jede Reise ist grundsätzlich verschieden, da sich aufgrund der Abhängigkeit von Parametern, wie dem Reisezweck (geschäftliche Besprechung, Tagung, Kongress, Seminar), der Reisedauer und dem Reiseziel, jeweils eine neue Bedrohungslage, auch in Bezug auf den Schutz geschäftskritischer Informationen, ergibt.

1.2 Lebenszyklus

Für eine bestmögliche Realisierung der Informationssicherheit auf Auslandsreisen sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung und Konzeption über die Umsetzung bis hin zur Notfallvorsorge. Die Schritte, die dabei durchlaufen werden sowie die Maßnahmen, die in den jeweiligen Schritten berücksichtigt werden sollten, sind im Folgenden aufgeführt.

Planung und Konzeption

Es muss eine Sicherheitsrichtlinie erstellt werden, in welcher der Rahmen der Informationssicherheit auf Auslandsreisen gesetzt wird und vordefinierte Sicherheitsmaßnahmen, Verhaltensanweisungen für Mitarbeiter sowie weiterführende Aspekte aufgezeigt werden (siehe CON.7.M1 Sicherheitsrichtlinie zur Informationssicherheit auf Auslandsreisen).

Außerdem sollte ein Sicherheitskonzept zum Umgang mit tragbaren IT-Systemen auf Auslandsreisen bzw. der Telearbeit erstellt und regelmäßig überprüft werden, das alle Sicherheitsanforderungen und -maßnahmen angemessen detailliert beschreibt.

Umsetzung

Die Verantwortung für die Erstellung, Einführung und Umsetzung der Informationssicherheit auf Auslandsreisen sollte beim Sicherheitsmanagement liegen. Zur angemessenen Umsetzung der Sicherheitsrichtlinie durch Geschäftsreisende sollte eine Sensibilisierung durch Schulung und Trainings verpflichtend sein, um die Wahrnehmungssicht aller Sachverhalte zu verbessern.

Die verschiedenen Sicherheitsanforderungen, die während der Auslandstätigkeit an die Informationssicherheit gestellt werden, sollten dementsprechend von allen Mitarbeitern aufmerksam gelebt werden. Die Berücksichtigung der aufgestellten Sicherheitsanforderungen sowie achtsame Mitarbeiter ermöglichen die Identifizierung von Sicherheitsproblemen und die zeitnahe Reaktion auf diese, um mögliche Schäden zu verhindern bzw. zu mildern. Sicherheitsprobleme und Veränderungen werden so rechtzeitig erkannt, sodass etablierte Sicherheitsmaßnahmen weiterentwickelt bzw. den Reiseszenarien entsprechend angepasst werden können.

Neben den organisatorischen Aspekten einer Reise ins Ausland sind auch technische Vorkehrungen zu treffen und physische Maßnahmen umzusetzen. Hierfür sind insbesondere der Einsatz von Verschlüsselung / Kryptographie, die Möglichkeit des sicheren Löschens von Daten und Informationen sowie die Absicherung der Kommunikation über öffentliche oder unbekannte Internetzugänge, wie z. B. Hotspots, zu betrachten.

Notfallvorsorge

Im Rahmen der Notfallvorsorge sollte sichergestellt werden, dass Sicherheitsvorfälle auf Auslandsreisen detektiert bzw. zeitnah gemeldet oder über die festgelegten Wege eskaliert werden (siehe Baustein DER.1 Detektion von Sicherheitsvorfällen). Die gemeldeten Vorfälle sollten hinsichtlich Notfallrelevanz bewertet werden (siehe Baustein DER.2.1 Behandlung).

Es sollten angemessene Maßnahmen vorgehalten werden, um auf Notfälle bei Reisen ins Ausland reagieren zu können.

Für weitere Informationen bspw. zum personellen Schutz kann der Wirtschaftsschutz-Baustein Reisesicherheit verwendet werden.

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Informationssicherheit auf Auslandsreisen" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

CON.7.M1 Sicherheitsrichtlinie zur Informationssicherheit auf Auslandsreisen

Mit der Sicherheitsrichtlinie wird nachvollziehbar der Rahmen für die Konzeption und Umsetzung der Informationssicherheit auf Auslandsreisen gesetzt. Sie dokumentiert die wesentlichen Anforderungen und Bedingungen, die es bei Reisen im Ausland in Bezug auf Informationssicherheit zu berücksichtigen gilt.

Die Sicherheitsrichtlinie zur Informationssicherheit auf Auslandsreisen sollte folgende Themenbereiche enthalten:

- eine kurze Darstellung, was die Institution unter Informationssicherheit auf Auslandsreisen versteht,
- der Geltungsbereich der Informationssicherheit auf Auslandsreisen,
- der Stellenwert und die Zielsetzung der Informationssicherheit auf Reisen für die Institution,
- die zu berücksichtigenden Kernaspekte der Informationssicherheit auf Reisen,
- die Übernahme der Verantwortung durch die Leitung der Institution und des ISB, die zusätzlich durch die explizite Freigabe mit einer Unterschrift dokumentiert wird,
- die Übernahme der Verantwortung und Pflichten durch den reisenden Mitarbeiter, diese sollte dokumentiert werden,
- die Verpflichtung der Leitungsebene und ISB regelmäßige Schulungen und Trainings zur Sensibilisierung der im Ausland tätigen Mitarbeiter durchzuführen,
- die Referenz auf relevante Gesetze, Richtlinien und Vorschriften, die es in Bezug auf die Informationssicherheit auf Auslandsreisen zu berücksichtigen gilt (z. B. Datenschutz im Ausland, Ein- und Ausreisebestimmungen).

Folgende Kernaspekte sollten in der Sicherheitsrichtlinie typischerweise berücksichtigt werden:

- Informationspflicht zu länderspezifischen Regelungen, Reise- und Umgebungsbedingungen
- Beobachtung, Analyse und Bewertung der Risiko- und Sicherheitslage der Destination
- Umgang mit verlorenen oder gestohlenen IT-Systemen oder Informationen
- Regelungen zur Durchführung von Schulungen und Sensibilisierungsmaßnahmen
- Umgang mit tragbaren IT-Systemen (z. B. Aufbewahrung, Passwort, Sichtschutz, nicht unbeaufsichtigt offen liegen lassen)
- Angemessener Schutz tragbarer IT-Systeme (z. B. Verschlüsselung, Virenschutz)
- Verschlüsselung, Sicherung und Schutz von Daten und Datenträgern
- Sicheres und physisches Löschen von Daten und Datenträgern bzw. Dokumenten
- Einwahl mit VPN-Zugang
- Einwahl in fremde Netze (in ein sicheres bzw. verschlüsseltes Netz, z. B. Benutzername, Passwort)
- Sicherheitsregelungen zum Datenaustausch mit Externen
- Berechtigungsprozess zur Mitnahme und Erfassung von Daten
- 24/7-Hotline bei Fragen oder Verlustmeldung von tragbaren IT-Systemen

Darüber hinaus kann optional die Eingliederung der Sicherheitsrichtlinie zur Informationssicherheit auf Reisen in das bestehende Managementsystem zur Informationssicherheit in Betracht gezogen werden.

Die Sicherheitsrichtlinie zur Informationssicherheit auf Auslandsreisen ist durch die Leitung schriftlich freizugeben. Sie ist allen internen Mitarbeitern, die eine Auslandstätigkeit ausüben, bekannt zu geben. Die Bekanntgabe sollte dabei so erfolgen, dass allen Mitarbeiter der Stellenwert der Informationssicherheit auf Auslandsreisen deutlich wird.

CON.7.M2 Sensibilisierung der Mitarbeiter zur Sicherheitsrichtlinie Informationssicherheit auf Auslandsreisen [Datenschutzbeauftragter, IT-Betrieb]

Sicherheit im Allgemeinen und Informationssicherheit auf Auslandsreisen im Besonderen kommt nicht ohne aufmerksame und geschulte Mitarbeiter aus. Deshalb stellen Schulungen und Sensibilisierungsmaßnahmen einen wesentlichen Bestandteil der Vorbereitung von Mitarbeitern dar. Im Ausland tätige Mitarbeiter sollten daher kontinuierlich und angemessen für Informationssicherheit auf Auslandsreisen sensibilisiert und regelmäßig geschult werden. Insbesondere sollten ihnen die Gefahren, die durch den unangemessenen Umgang mit Informationen, die unsachgemäße Vernichtung von Daten und Datenträgern, Schadsoftware und unsicheren Datenaustausch entstehen, vermittelt, aber auch die Grenzen der eingesetzten Sicherheitsmaßnahmen aufgezeigt werden.

Ebenso sollten Benutzer hinsichtlich des Schutzbedarfs mobiler IT-Systeme sowie der darauf befindlichen Daten sensibilisiert werden. Dabei sollten spezifische Gefährdungen bzw. entsprechende Maßnahmen bei der Nutzung mobiler IT-Systeme aufgezeigt werden. Auch sollten die Benutzer darauf hingewiesen werden, welche Art von Informationen während ihrer Auslandsaufenthalte auf z. B. dem Notebook oder Smartphone verarbeitet werden dürfen.

Die Reisenden sind dafür verantwortlich, keine Gelegenheiten für den Missbrauch von kritischen, institutionsinternen Informationen und Daten zu schaffen. Die Institution ist ihrerseits dafür verantwortlich, die Basis für den richtigen Umgang mit tragbaren IT-Systemen bzw. Informationen auf Auslandsreisen zu schaffen.

Die Mitarbeiter sollten dazu befähigt und bestärkt werden, bei Ungereimtheiten fachliche Beratung einzuholen bzw. einem Verlust oder Diebstahl vorzubeugen. Außerdem sollten Mitarbeiter auf gesetzliche Anforderungen einzelner Reiseziele in Bezug auf die Reisesicherheit hingewiesen werden. Hier steht der ISB in der Verantwortung, sich über gesetzliche Anforderungen im Rahmen der Informationssicherheit (z. B. Datenschutz, IT-Sicherheitsgesetz) zu informieren und die Mitarbeiter zu sensibilisieren.

Um dies zu erreichen, muss den Mitarbeitern plausibel und nachvollziehbar dargestellt werden, warum und in welchem Maß Informationssicherheit für die Institution, speziell auf Geschäftsreisen, wichtig ist. Sie müssen Gefährdungen und Auswirkungen von Sicherheitsvorfällen genauso kennen wie die erforderlichen Maßnahmen und die relevanten Regelungen in den Sicherheitsdokumenten.

Um Mitarbeiter für Informationssicherheit auf Reisen zu sensibilisieren, müssen sie immer wieder auf verschiedenen Wegen und über verschiedene Medien angesprochen werden. Dazu kann auf bereits etablierte Wege und Medien zurückgegriffen werden, aber auch können Neue gestaltet werden. Als geeignete Wege und Medien bieten sich z. B. an:

- Newsletter
- Flyer zum Mitnehmen
- Kurzanleitungen
- Videoclips zu ausgewählten Sensibilisierungsthemen

Folgende Aspekte sollten für Mitarbeiter auf Auslandsreisen aufbereitet und von diesen beachtet werden:

- Inhalte der geltenden **internen Regelungen** zu Geschäftsreisen ins Ausland und Überblick über zu schützende Informationen, Gefährdungen sowie Maßnahmen zur Sicherheit von Informationen, mit und ohne IT-Einsatz.

- **Arbeitsplatzumgebung**: Die Mitarbeiter sind anzuweisen, vor jedem mobilen Einsatz bei Auslandsreisen zu entscheiden, ob die jeweilige Umgebung als mobiler Arbeitsplatz geeignet ist, insbesondere im Hinblick auf die Informationssicherheit.
- **Nutzungsverbot nicht freigegebener Hard- und Software**: Alle Mitarbeiter sind vor Auslandsreisen erneut über das Verbot der Nutzung nicht freigegebener Hard- und Software zu informieren.
- **Schadprogramme**: Es sollten Sicherheitshinweise bzw. zu berücksichtigende Regelungen an die Mitarbeiter ausgegeben werden, die eine Infektion der tragbaren IT-Systeme mit Schadprogrammen vermeiden bzw. verringern. Sollte dennoch ein tragbares IT-System mit einem Schadprogramm infiziert werden, ist der Vorfall unverzüglich an eine zentrale Meldestelle der Institution zu kommunizieren. Dabei müssen zentrale Ansprechpartner benannt und bekannt gemacht werden. Außerdem sollte die Einhaltung der Regelungen zum Schutz vor Schadprogrammen regelmäßig und stichprobenartig geprüft werden.
- **Passwortgebrauch**: Die Benutzer sind anzuweisen, dem Schutzbedarf angemessene Passwörter mit ausreichender Komplexität zu verwenden. Darüber hinaus sollten diese einen besonderen Wert auf die Geheimhaltung ihres Passworts legen. Passwörter sind sofort zu wechseln, sobald sie unautorisierten Personen bekannt geworden sind oder der Verdacht darauf besteht. Der Zugriff auf IT-Systeme der Institution sollte mit einer Multi-Faktor-Authentifizierung abgesichert werden.
- **Verhinderung ungesicherter Netz-Zugänge**: Die Benutzer dürfen nicht direkt bzw. ungesichert ein öffentliches Netz bzw. einen Netzzugang fremder Institutionen (WLAN sowie LAN) nutzen, um auf interne Ressourcen zuzugreifen. Solche Zugänge sind generell als nicht vertrauenswürdig einzustufen.
- **Mitnahme von IT-Systemen und Datenträgern**: Etablierte Regeln zur Mitnahme von tragbaren IT-Systemen und Datenträgern sollten zur Kenntnis genommen und umgesetzt werden. In einigen Fällen muss zusätzlich der hohe Schutzbedarf bezüglich der Vertraulichkeit von Informationen berücksichtigt werden. Daher sollten mobile IT-Systeme und Datenträger vollständig verschlüsselt werden.
- **Informationspflicht zu Länder-spezifischen Regelungen, Reise- und Umgebungsbedingungen**: Bevor Mitarbeiter eine Reise antreten, sollten sie sich über die aktuelle Sicherheitslage sowie gesetzliche und regulatorische Anforderungen informieren. Spezifische Reise- und Sicherheitshinweise können beim deutschen Auswärtigen Amt eingeholt werden, siehe https://www.auswaertiges-amt.de/DE/Laenderinformationen/SicherheitshinweiseA-Z-Laenderauswahlseite_node.html. Informationen zu sicherheitsrelevanten Themen sollten durch den ISB eingeholt und den Mitarbeitern zur Verfügung werden.
- **Kommunikation mit der eigenen Institution und Geschäftspartnern**: Für die Kommunikation unterwegs sollten institutionsinterne Regelungen getroffen und gelebt werden (z. B. Nutzung gesicherter Verbindungen). Sowohl E-Mails als auch Festnetz- und Mobiltelefone können leicht ausgespäht werden, weshalb jede Art der Kommunikation zur Weitergabe hochschutzbedürftiger Informationen mit einer Ende-zu-Ende-Verschlüsselung gesichert werden müssen.
- **Aufmerksamkeit der Mitarbeiter während der Auslandstätigkeit**: Es sollten Regelungen zum Verhalten der Mitarbeiter im Ausland getroffen werden. Dazu zählt, dass Mitarbeiter zum Schutz geschäftskritischer Daten nicht mit Fremden über den Zweck ihrer Reise und ihren Arbeitgeber sprechen sollten. Dementsprechend sollte ein Mitarbeiter bei ungewöhnlich starker Nachfrage zu Themen der Arbeit oder des Arbeitgebers misstrauisch werden.
- **Annahme von Geschenken**: Die Annahme von Geschenken erweist sich oft als schwierig, da in der Regel Gegenleistungen erwartet werden. Daher müssen Mitarbeiter darüber informiert werden, wie in solchen Fällen zu verfahren ist.
- **Keine Verwendung von Geschenken mit digitalem Speicher**: Die Annahme bzw. Verwendung von Geschenken mit digitalem Speicher ist immer als äußerst kritisch zu betrachten. Zum Umgang mit derartigen Situationen sollten ebenfalls Regeln definiert werden. Generell empfiehlt es sich, keine Geschenke mit digitalem Speicher, z. B. USB-Sticks anzunehmen und zu verwenden.

Es ist wichtig, diese Sensibilisierungen kontinuierlich durchzuführen und regelmäßig zu wiederholen.

CON.7.M3 Identifikation länderspezifischer Regelungen, Reise- und Umgebungsbedingungen [Personalabteilung]

Bestimmungen zum Umgang mit länderspezifischen Regelungen, Reise- und Umgebungsbedingungen sollten in der Sicherheitsrichtlinie zur Informationssicherheit auf Auslandsreisen definiert sein. Dabei muss einerseits der ISB bzw. die Personalabteilung die jeweils geltenden Regelungen der einzelnen Länder prüfen und die ländereigenen Gegebenheiten im Rahmen der Informationssicherheit sowie der persönlichen Sicherheit an die entsprechenden Mitarbeiter kommunizieren, bevor diese eine Reise antreten. Auf der anderen Seite sind aber auch die Reisenden verpflichtet, sich selbst über das Reiseziel und seine Spezifika ausreichend Hintergrundkenntnisse zu verschaffen.

Voraussetzung hierfür ist, dass entsprechende Regelungen zum Informationsaustausch bei Auslandsaufenthalten erstellt und allen Beteiligten bekannt gegeben worden sind. Die Sicherheitsrichtlinie zur Informationssicherheit auf Auslandsreisen muss regelmäßig aktualisiert werden, vor allem wenn aufgrund geänderter Rahmenbedingungen Anpassungsbedarf besteht.

Umwelteinflüsse im Ausland, wie z. B. eine hohe Luftfeuchtigkeit, Hitze, Kälte oder Staub, können auch die Funktionsfähigkeit von elektronischen Geräten wie Notebooks oder Smartphones beeinflussen. Personalabteilung, ISB und Mitarbeiter sollten sich hier vor Reiseantritt mit den klimatischen Bedingungen des Reiseziels auseinandersetzen und Schutzmaßnahmen treffen, um Mitarbeiter sowie mitgeführte Informationstechnik und Informationen zu schützen. Tragbare IT-Systeme sollten vor besonderen klimatischen Bedingungen bzw. Umwelteinflüssen, wie z. B. Feuchtigkeit durch Regen oder Spritzwasser, gesichert werden. Mobile IT-Systeme sollten nicht extrem niedrigen oder hohen Temperaturen ausgesetzt werden, sofern sie nicht speziell dafür ausgelegt sind. Sowohl Akku als auch Display können durch extreme Temperaturen in ihrer Funktion gestört oder sogar zerstört werden, z. B. wenn IT-Geräte in Autos belassen werden, was jedoch aufgrund der möglichen Diebstahlgefahr nicht empfehlenswert ist.

Die jeweils geltenden Regelungen der einzelnen Länder sollten situativ vor jedem Reiseantritt geprüft werden. Sind bestehende Regelungen zum Informationsaustausch definiert und bekannt gegeben worden? Sollte hier situativ eine Anpassung vorgenommen werden? Sind bestehende Verschlüsselungsarten oder Kommunikationsverfahren geeignet bzw. sicher?

Außerdem kann sich das Problem ergeben, dass Notebooks von Geschäftsreisenden in bestimmten Ländern, wie z. B. den USA, bei der Ein- oder Ausreise durchsucht werden können. Dieser Aspekt steht mit dem Schutz vertraulicher Informationen vor dem Zugriff Dritter im Widerspruch. Denn es ist den US-Behörden nicht nur erlaubt, IT-Systeme zu durchsuchen, sie dürfen diese auch an sich nehmen und Daten kopieren. IT-Systeme können darüber hinaus auch bis zu einem Monat beschlagnahmt werden, was sich für Reisende als problematisch erweisen kann, wenn sie in der Durchführung ihrer Tätigkeit beschränkt oder sogar gehindert werden. Deshalb muss die Institution hier Regelungen erstellen, die den Schutz unternehmensinterner Daten ermöglicht. Ein Beispiel sind Unternehmensregeln, bei denen Passwörter zum Zugriff auf mitgeführte IT-Systeme erst nach erfolgreicher Einreise zugesendet werden, bestimmte Daten vor Reiseantritt sicher gelöscht werden oder keine schützenswerten Daten auf Smartphones gespeichert werden.

CON.7.M4 Verwendung von Sichtschutz-Folien [Benutzer]

Um das Display von Notebooks, Tablets oder Smartphones und damit die dargestellten internen Daten vor neugierigen Blicken anderer zu schützen, ist die Verwendung geeigneter Sichtschutz-Folien eine praxiserprobte Möglichkeit. Diese bedecken das Display des verwendeten Geräts und erschweren es, Informationen auszuspähen (sogenanntes Shoulder Surfing).

CON.7.M5 Verwendung der Bildschirm-/Code-Sperre [Benutzer]

Durch die Verwendung einer Bildschirm-/Code-Sperre wird verhindert, dass Dritte auf Daten auf mobilen Endgeräten, wie z. B. Notebooks oder Mobiltelefonen zugreifen können. Dazu muss ein angemessener Code bzw. ein sicheres Gerätepasswort verwendet werden.

Der Zeitraum, nach dem sich eine Bildschirmsperre wegen fehlender Benutzereingaben automatisch aktiviert, sollte gewisse Grenzen weder unter- noch überschreiten. Der Zeitraum sollte nicht zu knapp gewählt werden, damit die Bildschirmsperre nicht bereits nach kurzen Denkpausen anspringt. Dieser Zeitraum darf aber auf keinen Fall zu lang sein, damit die Abwesenheit des Benutzers nicht von Dritten ausgenutzt werden kann. Eine sinnvolle Vorgabe ist eine Zeitspanne von 10 Minuten für Notebooks und 2 Minuten für weitere mobile Geräte. Der ISB sollte Vorgaben für die Einstellung der Wartezeit machen, die die Sicherheitsanforderungen der jeweiligen IT-Systeme und deren Einsatzumgebung berücksichtigen. Diese Vorgaben sollten möglichst zentral auf den Endgeräten durchgesetzt werden, beispielsweise über Gruppenrichtlinien oder ein MDM.

CON.7.M6 Zeitnahe Verlustmeldung [Benutzer, Notfallbeauftragter]

Mitarbeiter müssen ihrer Institution umgehend melden, wenn Informationen, IT-Systeme oder Datenträger verloren oder gestohlen wurden. Hierfür muss es klare Meldewege und Ansprechpartner innerhalb der Institution geben. Es empfiehlt sich, z. B. eine Notfall-Hotline einzurichten, die täglich 24 Stunden erreichbar ist.

Auf Laptops, Smartphones, Tablets, PDAs und ähnlichen Geräten, aber auch auf mobilen Datenträgern wie USB-Sticks können sich vertrauliche Daten befinden, nach deren Verlust umgehend gehandelt werden muss, beispielsweise:

- Zugangsdaten wie Passwörter: Alle Zugangsdaten der betroffenen IT-Systeme müssen umgehend geändert werden.
- Als vertraulich eingestufte Informationen (z. B. Patientenakten): Alle betroffenen Bereiche (z. B. Fachabteilung, Kunden, etc.) müssen benachrichtigt werden, um entsprechende Maßnahmen ergreifen zu können.
- Zusätzlich sollten auch VPN-Zugänge, Maschinen- oder Client-Zertifikate sowie Computer- und Userkonten gesperrt werden. Falls vorhanden, sollten auch über ein entsprechendes Monitoring Anmelde- oder Eindringversuche erkannt und unterbunden werden.

Bei Verlust von mobilen Endgeräten mit einer Funkverbindung sollten Maßnahmen zum Sperren, Löschen und Lokalisieren der mobilen Endgeräte genutzt werden. Die meisten Mobile-Device-Management-Lösungen bieten diese Funktionen an. Dafür sind im Vorfeld klare Regeln zu definieren und entsprechende Maßnahmen in Absprache mit dem Benutzer, dessen Endgerät verloren ging, unverzüglich zu ergreifen (siehe SYS.3.2.2 Mobile Device Management)

Wenn das verschwundene Notebook oder Smartphone wieder auftaucht, sollte es auf eventuelle Manipulationen untersucht werden, z. B. ob Schrauben geöffnet oder Siegel entfernt wurden oder sich das Gewicht gegenüber dem Ursprungszustand geändert hat. Hat der Benutzer selbst nicht die notwendigen Möglichkeiten hierzu oder besteht ein Verdacht auf Manipulation, sollte das jeweilige Gerät nicht mehr verwendet werden und an einen Spezialisten zur weiteren Überprüfung übergeben werden. Es sollte eine klare Regelung bestehen, wie beim Wiederauffinden des Gerätes noch während der Reise verfahren werden muss. Bei einem mobilen Datenträger sollte die Anforderung CON.7.M9 Sicherer Umgang mit mobilen Datenträgernangewendet werden, um sicherzustellen, dass sich keine manipulierten Programme oder Schadsoftware auf den wiedererlangten Datenträgern befinden.

CON.7.M7 Sicherer Remote-Zugriff [Benutzer, IT-Betrieb]

Da IT-Systeme beim mobilen Arbeiten im Ausland oft in nicht kontrollierbaren Umgebungen betrieben werden, müssen bei Fernzugriffen auf das Netz der Institution spezielle Mechanismen, Verfahren und Maßnahmen zum Einsatz kommen, die den Schutz der IT-Systeme gewährleisten können. Insbesondere mobile VPN-Clients sind hier einer besonderen Gefahr ausgesetzt, da diese physikalisch besonders leicht anzugreifen sind (z. B. Diebstahl, Manipulation). Ist ein VPN-Client kompromittiert, besteht die Gefahr, dass dadurch auch die Sicherheit des LANs beeinträchtigt wird.

Für den sicheren Betrieb der mobilen IT-Systeme müssen diese mit einer sicheren Grundkonfiguration versehen sein (siehe Bausteine SYS.2.1 Allgemeiner Client und SYS.3.2 Mobile Device Management). Für Auslandsreisen sind dabei folgende spezifische Punkte zu berücksichtigen:

- Für den direkten Anschluss mobiler IT-Systeme an das Internet ist es unabdingbar, sie durch eine restriktiv konfigurierte Personal Firewall gegen Angriffe aus dem Netz zu schützen. Der Virenschutz reicht alleine nicht aus, um alle zu erwartenden Angriffe abzuwehren.
- Ebenso ist es unbedingt erforderlich, die Software der IT-Systeme auf aktuellem Stand zu halten und notwendige Sicherheitspatches zeitnah einzuspielen. Es ist sinnvoll, vor einem Zugriff auf das Produktivnetz zu überprüfen, ob Personal Firewall, andere Sicherheitsprogramme und Sicherheitspatches auf dem Laptop auf dem aktuellsten Stand sind.
- Empfehlenswert ist es, über entsprechende Tools diese Prüfungen automatisiert durchzuführen, so dass bei Sicherheitsmängeln der Zugriff auf das interne Netz abgewiesen werden kann.
- Die auf dem IT-System installierten Internet-Anwendungsprogramme, vor allem Browser und E-Mail-Client, sollten mit sicheren Einstellungen betrieben werden.

Für den sicheren Fernzugriff von Mitarbeitern auf das institutionseigene Netz muss zuvor ein sicherer Remote-Zugang über VPN eingerichtet werden, siehe auch NET.3.3 Virtual Private Networks. Der VPN-Zugang muss kryptographisch abgesichert werden, um ein unbefugtes Lauschen zwischen dem Endgerät und dem Netz der Institution zu verhindern.

Ein mobiles IT-System kann leicht in falsche Hände geraten. Die Verbindung in das interne Netz (der Tunnelaufbau) sollte daher nicht automatisiert, sondern erst nach einer Authentisierung erfolgen. Benutzer müssen über angemessene Zugangsdaten verfügen, um sich einerseits gegenüber dem Endgerät und andererseits dem Netz erfolgreich zu authentisieren.

Außerdem muss die Kommunikation über das VPN verschlüsselt erfolgen. Hierfür muss eine der aktuellen Situation angemessene Schlüssellänge eingesetzt werden. Außerdem muss sichergestellt werden, dass etablierte kryptographische Algorithmen verwendet werden, von denen keine Sicherheitsprobleme bekannt sind.

Außerdem müssen folgende Aspekte für den Einsatz des VPN berücksichtigt werden:

- Es ist zu regulieren, für welche Geschäftsprozesse und Anwendungszwecke das jeweilige VPN genutzt und welche Informationen darüber kommuniziert werden dürfen.
- Es muss festgelegt werden, welche Dienste nur genutzt werden dürfen, wenn hierfür ein sicherer Remote-Zugang zur Verfügung steht. Wenn beispielsweise ein Remote-Zugang verfügbar ist, dürfen keine Dienste wie E-Mail an diesem vorbei genutzt werden.
- Es ist festzulegen, z.B. anhand ihrer Vorkenntnisse, welche Mitarbeiter welche Berechtigungen über den Remote-Zugang bekommen sollen.
- Geeignete Verfahren zur Identifikation und Authentisierung für die Nutzung des VPN-Zugangs sind festzulegen.
- Zuständigkeiten und Meldewege für Betrieb und Nutzung von VPN sind zu bestimmen.
- Es sollte sichergestellt werden, dass alle zwischengespeicherten Authentisierungsinformationen, die den Aufbau eines VPNs ermöglichen, nach dem Ende der VPN-Nutzung automatisch gelöscht werden.
- Für jedes VPN ist festzulegen, von wo auf welches Netz zugegriffen werden darf.
- Eine VPN-Sicherheitsrichtlinie ist zu erstellen.
- Jedem VPN-Benutzer ist ein Exemplar der VPN-Richtlinie oder ein Merkblatt mit einem Überblick der wichtigsten Sicherheitsmechanismen auszuhändigen.
- Die Richtlinie für die VPN-Nutzung muss den Mitarbeitern erläutert werden, beispielsweise im Rahmen von Schulungen oder Sensibilisierungsveranstaltungen.

CON.7.M8 Sichere Nutzung von öffentlichen WLANs [Benutzer]

WLAN-Hotspots, wie sie an öffentlichen Orten wie beispielsweise in Hotels, Flughäfen, Messehallen, Bahnhöfen, Restaurants und Kongresszentren zu finden sind, sollten immer als unsicheres Netz betrachtet werden, da das dort vorhandene Sicherheitsniveau von außen nur schwer einzuschätzen ist. Der Benutzer muss dafür sensibilisiert werden, dass Hotspots grundsätzlich nicht als vertrauenswürdig eingestuft werden können.

Der Zugriff von mobilen IT-Systemen auf Ressourcen der Institution über öffentlich zugängliche WLANs sollte daher nur über ein Virtual Private Network (VPN) oder mit einer vergleichbaren Absicherung möglich sein.

Weitere Informationen hierzu sind in folgenden Bausteinen zu finden:

- NET.2.2 WLAN-Nutzung (Allgemein)
- INF.10 Mobiler Arbeitsplatz (für WLAN Hotspots)
- NET.3.3 Virtual Private Networks

Für die Nutzung von öffentlichen WLANs im Ausland sollten nachfolgende Regelungen berücksichtigt werden.

Unverschlüsselte WLAN-Hotspots sollten nach Möglichkeit nicht genutzt werden. Es sollten WLAN-Hotspots genutzt werden, die eine verschlüsselte Anmeldung mit Benutzernamen und Passwort erfordern. Dabei müssen die Anmeldedaten vom Hotspot-Betreiber verschlüsselt übertragen werden, damit diese nicht in Reichweite der Funkverbindung mitgelesen werden können.

Unabhängig davon kann der Betreiber eines Hotspots den Datenverkehr mitlesen, wenn dieser nicht geeignet verschlüsselt oder insgesamt durch ein VPN abgesichert ist.

Bei mehreren WLAN-Netzen mit ähnlichen Namen muss darauf geachtet werden, das richtige WLAN-Netz auszuwählen. WLAN-Hotspots können jedoch auch absichtlich unter bekannten Namen von öffentlichen WLAN Netzen aufgebaut werden, um Nutzer anzulocken. Viele Endgeräte bauen außerdem automatisch Verbindungen zu namentlich bereit s bekannten Netzen auf.

Geschäftskritische Daten dürfen nur über externe Hotspots übertragen werden, wenn entsprechende Sicherheitsmaßnahmen und sichere Protokolle verwendet werden. Der Zugriff auf das interne Netz der Institution darf nur über vertrauenswürdige Verbindungen erfolgen. Zudem sollte geregelt werden, ob die Gültigkeit der Hotspot-Zertifikate bei der Authentisierung überprüft werden muss. Es sollte in Betracht gezogen werden, bei Nutzung externer Hotspots auf dem eigenen IT-System separate Benutzerkonten mit einer sicheren Grundkonfiguration und restriktiven Berechtigungen zu verwenden. Keinesfalls dürfen sich Benutzer mit Administratorrechten von einem mobilen Client an externen Netzen anmelden.

CON.7.M9 Sicherer Umgang mit mobilen Datenträgern [Benutzer]

Beim normalen Löschen von Daten wird in der Regel nur die Referenz zu den Daten aufgehoben und die Daten selbst bleiben bis zur erneuten Verwendung des genutzten Speicherbereichs weiterhin vorhanden. Hinzu kommen technische Artefakte, in denen sich Duplikate von zumindest Teilen der Daten befinden.

Wird ein sicheres Verschlüsselungsverfahren für die Daten genutzt, genügt es in der Regel, den Schlüssel und alle seine Kopien sicher zu löschen. Damit liegen die verschlüsselten Daten weiterhin auf dem Datenträger, können aber nicht mehr mit vertretbarem Aufwand entschlüsselt werden. Es wird daher empfohlen, alle Datenträger (auch von stationären Rechnern) grundsätzlich zu verschlüsseln, um das sichere Löschen zu vereinfachen. Die Verwaltung der Schlüssel ist dabei zu dokumentieren, insbesondere die Ablage von Wiederherstellungsschlüsseln.

Eine für den normalen Schutzbedarf ausreichende Löschung kann erreicht werden, indem der komplette Datenträger überschrieben wird. Mit speziellen Softwarewerkzeugen werden dabei die Datenträger einmal oder mehrfach mit vorgegebenen Zeichenfolgen oder Zufallszahlen überschrieben. Die Datenträger müssen intakt sein und sind auch nach dem Überschreiben weiterhin nutzbar.

Für den höheren Schutzbedarf sollte die Überschreibprozedur aus mindestens zwei Durchläufen und einer Verifikation des Überschreibvorgangs bestehen. Als Datenmuster werden Zufallsdaten empfohlen. Eine andere Möglichkeit ist, beim mehrfachen Überschreiben beim zweiten Durchlauf das zum ersten Durchlauf komplementäre Datenmuster (Bit-Folge) zu verwenden. Um Datenträger zu löschen, auf denen Verschlusssachen (VS) gespeichert waren, dürfen nur vom BSI für den jeweiligen Geheimhaltungsgrad empfohlene bzw. zugelassene Produkte eingesetzt werden.

Bei manchen Endgeräten, wie etwa von BlackBerry und Apple, gibt es ebenfalls keinen direkten Zugang zu dem eingebauten Speicher. Es müssen Funktionen des Betriebssystems genutzt werden, um die Daten zu löschen. Nach der Löschung sollte nach Möglichkeit manuell geprüft werden, dass alle Datenartefakte entfernt wurden.

Wurden vertrauliche Daten verarbeitet, sollten Datenträger nach dem Löschen nicht wieder verwendet, sondern direkt geeignet vernichtet werden.

Ist ein sicheres Löschen oder Vernichten nicht möglich, so wird empfohlen, die Datenträger wieder mit in die eigene Institution zu nehmen und dort nach einem geregelten Verfahren zu entsorgen.

In den folgenden Abschnitten werden die konkreten Vorgehensweisen für verschiedene Geräte und Datenträger beschrieben.

Sicheres Löschen von mobilen Festplatten und USB-Sticks

Grundsätzlich können mobile Datenträger ähnlich wie eingebaute Festplatten gelöscht werden. Steht kein Rechner mit der Löschsoftware zur Verfügung, kann auch von einem externen Medium gebootet und geeignete Software genutzt werden.

Mit Verschlüsselung

Wurde der mobile Datenträger mit einem sicheren Verfahren vollständig verschlüsselt oder sind alle Daten in einem sicher verschlüsselten Container abgelegt, ist es ausreichend, das Schlüsselmaterial sicher zu löschen.

Als flankierende Maßnahme sollten alle Kopien von möglichen Schlüsselmaterial (z. B. Recovery Keys) gelöscht werden. Dafür ist eine Dokumentation der Schlüsselverwaltung hilfreich.

Ist unklar, ob alle Kopien des Schlüsselmaterials gelöscht wurden, oder ist die Qualität der Umsetzung der Festplattenverschlüsselung unklar, sollte zusätzlich die Löschung wie in den folgenden Abschnitten beschrieben durchgeführt werden.

Alle durchgeführten Schritte sollten protokolliert werden.

Flash-Speicher basierende Datenträger (USB-Stick, SSD)

USB-Sticks bieten im Allgemeinen keine speziellen Befehle zum Löschen bzw. ist bei SSDs oftmals die Qualität der Umsetzung unklar. Daher sollten auf Flash-Speicher basierende Medien mit einem Zufallsmuster mindestens zweimal vollständig überschrieben werden. Solche Medien besitzen mehr Speicherblöcke als sie zur Verfügung stellen. Die Datenmenge und das Muster beim Überschreiben dienen hier im Gegensatz zur Festplatte dazu, die Lastverteilung des Mediums dazu zu bringen, alle internen Speicherblöcke zu überschreiben.

Da die internen Speicherblöcke von außen nicht direkt adressiert werden können, kann nicht geprüft werden, ob alle Speicherblöcke überschrieben wurden. Allerdings wäre ein Zugriff auf solche Datenartefakte für einen Angreifer auch nur mit sehr hohem Aufwand möglich (Auslöten der Bausteine, Rekonstruieren der Datenstrukturen). Für Daten mit normalen Schutzbedarf und vertrauliche Daten ist dieses Vorgehen daher ausreichend.

Für unverschlüsselte streng vertrauliche Daten empfiehlt sich die physische Zerstörung und entsprechende Entsorgung der Medien, nachdem sie wie beschrieben gelöscht wurde. Vormals verschlüsselte Medien können nach dem Löschen wieder für Bereiche mit der gleichen Klassifizierung eingesetzt werden.

Als defekt deklarierte Medien sollten zuerst an mindestens einem weiteren System geprüft werden. Lassen sie sich dort auch nicht löschen, sollte das Medium physisch vernichtet und dann entsorgt werden, etwa durch ein spezielles Entsorgungsunternehmen.

Alle durchgeführten Schritte sollten protokolliert werden.

Sicheres Löschen von BlackBerry-OS-Geräten

Zum sicheren Löschen aller Daten auf dem BlackBerry muss die "Secure Wipe"-Funktion angestoßen werden. Dies ist über die folgenden Wege möglich:

- Mittels des Mobile Device Management-Tool BlackBerry Enterprise Service durch die verantwortlichen Administratoren oder durch das Self-Service-Portal durch den Anwender selbst.
- Bei einem entsperrten Gerät in der App "Einstellungen" den Menüpunkt "Sicherheit und Datenschutz" wählen, dort dann die Funktion „Sicherheitslöschung“ anwählen und die Löschung durch Eingabe von "blackberry" bestätigen.
- Bei einem gesperrten Gerät mehrfach das falsche Passwort eingeben.

Um die korrekte Löschung zu überprüfen, sollte das Gerät danach testweise mit einem Testnutzer wieder aktiviert werden und geprüft werden, ob sich noch Verknüpfungen, z. B. mit dem Mail-Account des ursprünglichen Benutzers finden lassen.

Bei erhöhtem Schutzbedarf kann der BlackBerry zusätzlich zur Verifikation mit einem Forensik-Tool ausgelesen werden. In diesem Fall muss der Testnutzer über eine gültige Blackberry-ID verfügen. Es wird empfohlen, dafür eine eigene Mailadresse einzurichten und darüber eine Blackberry-ID anzumelden.

Da die Löschung nur von der Betriebssoftware des Geräts ausgelöst wird und kein vollständiger Zugriff auf den eingebauten Datenspeicher möglich ist, ist eine vollständige Verifikation dennoch nicht möglich. Daher sollten Geräte auf denen vertrauliche Daten verarbeitet wurden, nach der sicheren Löschung vernichtet werden.

Alle durchgeführten Schritte sollten protokolliert werden.

Sicheres Löschen von iOS-Devices von Apple

Zum sicheren Löschen aller Daten auf einem iOS-Gerät muss das Zurücksetzen in den Werkszustand über einen der folgenden Wege angestoßen werden.

- Durch den Anwender über die Löschfunktion über die Onlineplattform icloud.com. Hierzu muss sich der Anwender mit der Apple-ID anmelden unter der das Gerät aktiviert wurde.
- Durch die verantwortlichen Administratoren der verwendeten Mobile-Device-Lösung, welche den Befehl zum zurücksetzen auf den Werkszustand (Wipe) auslösen.
- Bei einem entsperrten Gerät in der App "Einstellungen" den Menüpunkt "Allgemein" wählen, dort dann die Funktion "zurücksetzen" anwählen und die Löschung durch Auswahl "Alle Einstellungen" initialisieren.
- Bei einem gesperrten Gerät 10mal das falsche Passwort eingeben.

Um die korrekte Löschung zu überprüfen, sollte das Gerät danach testweise mit einem Testnutzer wieder aktiviert werden und geprüft werden, ob sich noch Verknüpfungen z. B. mit dem Mail-Account des ursprünglichen Benutzers finden lassen.

Bei erhöhtem Schutzbedarf kann das iPhone oder iPad zusätzlich zur Verifikation mit einem Forensik-Tool ausgelesen werden. In diesem Fall muss der Testnutzer über eine gültige Apple-ID verfügen. Es wird empfohlen dafür eine eigene Mailadresse einzurichten und darüber eine Apple-ID anzumelden.

Da die Löschung nur von der Betriebssoftware des Geräts ausgelöst wird und kein vollständiger Zugriff auf den eingebauten Datenspeicher möglich ist, ist eine vollständige Verifikation dennoch nicht möglich. Daher sollten Geräte, auf denen vertrauliche Daten verarbeitet wurden, nach der sicheren Löschung vernichtet werden.

Alle durchgeführten Schritte sollten protokolliert werden.

CON.7.M10 Verschlüsselung tragbarer IT-Systeme und Datenträger [Benutzer, IT-Betrieb]

Um zu verhindern, dass schützenswerte Informationen durch unberechtigte Dritte eingesehen werden können, muss vor Reiseantritt durch den Mitarbeiter sichergestellt werden, dass alle schützenswerten Informationen entsprechend den internen Richtlinien abgesichert sind.

Mobile Datenträger und Clients sollten vor Reiseantritt nach unternehmensinternen Verfahren und Regelungen verschlüsselt werden, um schützenswerte Daten vor unbefugten Zugriff zu schützen. Dies gilt insbesondere für wiederbeschreibbare Datenträger. Es besteht die Möglichkeit, Datenträger nur partiell zu verschlüsseln. Im Rahmen der Benutzerfreundlichkeit empfiehlt es sich allerdings, den gesamten Datenträger zu verschlüsseln, wenn dieser nicht für einen Datenaustausch mit Dritten benötigt wird. Eine Verschlüsselung des Datenträgers erreicht man entweder mit Software, wie z. B. BitLocker von Microsoft oder FileVault von Apple, oder auch mit spezieller Hardware. Zur Entschlüsselung von Clients ist ein kryptographischer Schlüssel notwendig, der in Form einer separaten Chipkarte oder eines USB-Tokens verwendet werden sollte. Hierbei sollte der Benutzer den kryptographischen Schlüssel und den verschlüsselten Datenträger bzw. Client getrennt voneinander aufbewahren.

Zudem ist es wichtig, Vorkehrungen gegen Datenverlust zu treffen, um Fehlfunktionen (Stromausfall, Abbruch der Verschlüsselung) systemseitig abzufangen. Darüber hinaus sind folgende Anforderungen sinnvoll:

- Der genutzte Verschlüsselungsalgorithmus sollte den Anforderungen der Institution entsprechen.
- Das Schlüsselmanagement muss mit den Funktionen des mobilen IT-Systems harmonisieren.
- Das mobile IT-System muss die sicherheitskritischen Parameter wie Schlüssel sicher verwalten. So dürfen Schlüssel (auch mittlerweile nicht mehr benutzte) nie ungeschützt, das heißt auslesbar oder unverschlüsselt, abgelegt werden. Sie müssen möglichst getrennt vom verschlüsselten Gerät aufbewahrt werden.

Bei der Verschlüsselung von Daten ist auf vorhandene gesetzliche Regelungen des Ziellandes zu achten. So sind beispielsweise landesspezifische Gesetze über die Herausgabe von Passwörtern und Entschlüsselung von Daten zu beachten.

CON.7.M11 Einsatz von Diebstahl-Sicherungen [Benutzer]

Diebstahl-Sicherungen sind überall dort einzusetzen, wo große Werte zu schützen sind bzw. dort, wo andere Maßnahmen nicht umgesetzt werden können, wie etwa bei Laptops im mobilen Einsatz. Diebstahl-Sicherungen sind außerdem dort sinnvoll, wo Publikumsverkehr herrscht oder die Fluktuation von Benutzern sehr hoch ist. Dabei sollte immer bedacht werden, dass die zu schützenden Werte nur zu einem kleinen Teil aus den Wiederbeschaffungskosten für das Gerät bestehen, sondern bei Laptops und ähnlichen IT-Systemen der Wert der darauf gespeicherten Daten berücksichtigt werden muss.

Verhindern einer "Cold Boot Attacke"

In Bereichen, die nicht ausreichend gegen unbefugten Zutritt geschützt sind, könnte beispielsweise durch eine "Cold Boot Attacke" der Arbeitsspeicher ausgelesen werden. Gleiches gilt für Systeme, die durch "Suspend to RAM" in einen Energiesparmodus versetzt wurden.

Bei einer Cold Boot Attacke werden die Speicherbausteine stark gekühlt, bevor das System ausgeschaltet wird. Der Speicherinhalt bleibt dadurch mehrere Minuten erhalten und kann währenddessen mit geeignetem Gerät ausgelesen werden.

Cold Boot Attacken können nur verhindert werden, wenn Angreifer keine Möglichkeit haben, ungestört auf den Arbeitsspeicher eines aktiven IT-Systems zuzugreifen. Ein Zugriffsschutz, wie ein physisch verriegeltes Computer-Gehäuse, erschwert es, ein IT-System unbefugt zu öffnen, um den Arbeitsspeicher zu kühlen und auszubauen, kann es aber nicht dauerhaft unterbinden. Daher sollte ein unbenutztes IT-System stets ausgeschaltet werden, wenn es in keinem zutrittsgeschützten Bereich steht.

Arten von Diebstahl-Sicherungen

Mit Diebstahl-Sicherungen sollte je nach zu schützendem Objekt nicht nur das IT-System selbst, sondern auch Zubehör ausgestattet werden.

Auf dem Markt sind die unterschiedlichsten Diebstahl-Sicherungen erhältlich. Diese können zunächst in mechanische und elektronische Sicherungen unterteilt werden.

Mechanische Sicherungen

Zu den mechanischen Sicherungen gehören unter anderem Kabelsicherungen, Gehäusesicherungen (um das Gehäuse gegen Öffnung zu schützen), Sicherheitsplatten und Sicherheitsgehäuse. Es gibt hier zum einem Hardware-Sicherungen, die dem Diebstahl von IT-Geräten vorbeugen, z. B. durch das Verbinden des IT-Systems mit einem Schreibtisch. Es gibt zum anderen auch eine Reihe von Sicherungsmechanismen, die das Öffnen des Gehäuses verhindern sollen, um dem Diebstahl von Teilen oder der Manipulation von sicherheitsrelevanten Einstellungen wie dem Entfernen von Sicherheitskarten vorzubeugen.

Bei der Beschaffung mechanischer Sicherungen ist die Wahl eines guten Schlosses wichtig, das über eine auf die jeweiligen Bedürfnisse abgestimmte Schließanlage verfügt. Je nach Produkt sind verschiedene Schließanlagen möglich:

- gleichschließend: Ein Schlüssel passt auf alle Gerätesicherungen einer Institution, Abteilung und so weiter. Dies hat den Vorteil, dass der Aufwand für die Schlüsselverwaltung geringer ist. Es hat aber auch den Nachteil, dass sehr viele gleichartige Schlüssel im Umlauf sein können und dass im Schadensfall häufig keine Beweissicherung möglich ist.
- verschiedenschließend: Jede Gerätesicherung hat einen individuellen Schlüssel. Dies hat den Nachteil, dass der Aufwand für die Schlüsselverwaltung höher ist. Es hat aber den Vorteil, dass es weniger Schlüsseldubletten gibt.
- Hauptschlüsselsystem: Jede Gerätesicherung hat einen individuellen Schlüssel, kann zusätzlich aber auch durch einen Hauptschlüssel geöffnet werden. Dies hat den Vorteil, dass der Aufwand für die Schlüsselverwaltung geringer ist. Es hat aber den Nachteil, dass solche Systeme teurer in der Anschaffung sind.

Die meisten Notebooks, aber auch viele andere Geräte, haben eine kleine Öffnung, welche mit einem Ketten- oder Schloss-Symbol gekennzeichnet ist ("Kensington-Lock"). Diese Öffnung (ca. 3 x 7 mm) befindet sich seitlich oder hinten am Gerät. Es gibt eine breite Palette von Kabelsicherungen und anderen Produkten, welche diese Öffnung für die Sicherung von Geräten nutzt.

Bei Kabelsicherungen muss dann eine Kabelschlinge um ein solides Objekt in der Nähe des Gerätes gelegt, das zugehörige Schloss durch die entstandene Lasche gezogen und abgeschlossen werden.

Für Geräte, die diese Öffnung nicht haben, oder wo diese nicht stark genug ist, gibt es Sicherungsprodukte, bei denen eine stabile Platte auf das Gerät geklebt wird. An dieser wird dann das Sicherungskabel befestigt.

Elektronische Sicherungen

Daneben gibt es elektronische Sicherungen, die beispielsweise einen akustischen Abschreckungsalarm am Gerät selber auslösen, der potentielle Diebe dazu bringen soll, dass Gerät liegen zu lassen. Weitere Sicherungseinrichtungen sind z. B. Warensicherungsanlagen (mit EAS-Antennen oder Sicherungsetiketten) oder auch Kamera- bzw. Videoüberwachungsanlagen.

Es ist zu beachten, dass diese Sicherungen üblicherweise keinen umfassenden Schutz bieten und in unterschiedlicher Qualität verfügbar sind. Allgemein schützen sie vor allem vor "Mitnahme" und weniger vor gezieltem Diebstahl. Ein guter Vergleich sind Fahrradschlösser, die eine ähnliche Nutzenbilanz haben.

Bei Neuanschaffung von IT-Geräten sollte trotzdem darauf geachtet werden, dass diese Ösen am Gehäuse besitzen, um sie an anderen Gegenständen befestigen zu können, und dass die Gehäuse abschließbar sind.

CON.7.M12 Sicheres Vernichten von schutzbedürftigen Materialien und Dokumenten [**Benutzer**]

Innerhalb der eigenen Institution gibt es in der Regel eingeübte Verfahren, wie alte oder unbrauchbare Datenträger und Dokumente zu entsorgen sind, allerdings ist dies auf Reisen so nicht möglich. Daher ist vor der Entsorgung ausgedienter Datenträger und Dokumente genau zu überlegen, ob diese schützenswerte Informationen enthalten könnten. Ist dies der Fall, müssen die Datenträger und Dokumente im Zweifelsfall wieder mit zum Herkunftsort bzw. zurück in die eigene Institution genommen werden. Vor Ort sollten möglichst wenig schutzwürdige Materialien oder Dokumente erzeugt werden.

Auch Akten- und Datenvernichter ("Shredder") in fremden Institutionen sollten mit Vorsicht betrachtet werden, da hier nicht unbedingt ersichtlich ist, wer die Entsorgung durchführt bzw. wie zuverlässig diese ist.

Weiterhin ist zu beachten, dass Experten unter Umständen auch von defekten Datenträgern wertvolle Informationen zurückgewinnen können. Solche Datenträger dürfen deshalb ebenfalls nicht einfach weggeworfen werden, wenn sich darauf noch schützenswerte Daten befinden könnten.

Werden Unternehmen im Ausland mit der Entsorgung von schützenswerten Betriebsmitteln beauftragt, sind diese daraufhin zu überprüfen, ob der Entsorgungsvorgang verlässlich ist.

Es sollten dem Reisenden Möglichkeiten zum sicheren Löschen auf Reisen oder sicherem Transport ins Unternehmen bereitgestellt werden. Dies kann z. B. in Form:

- der Bereitstellung von Equipment für die Reise,
- von Zusammenarbeit mit einem lokalen Dienstleistern,
- der Zusammenarbeit mit Kurieren,
- der Nutzung von institutionseigenen Filialen

ermöglicht werden.

Die Sicherheitsrichtlinie muss die Regelungen enthalten, wie Mitarbeiter unterwegs mit ausgedienten Datenträgern und Dokumenten umgehen sollen.

Generell sollten Datenträger bis zur Entsorgung bzw. Abholung vor unbefugten Zugriff gesichert und auf der gesamten Transportstrecke geschützt werden. Auch bei einer Entsorgung nach den entsprechenden Sicherheitsstufen sollten Datenträger zuvor sicher gelöscht werden.

Eine DIN-gerechte Entsorgung von physischen Datenträgern ist allerdings im Ausland nur schwer möglich. Daher wird empfohlen, Dokumente und Datenträger wieder mit in die eigene Institution zu nehmen und dort nach einem geregelten Verfahren zu entsorgen.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Informationssicherheit auf Auslandsreisen".

CON.7.M13 Mitnahme von Daten und Datenträgern [Benutzer, IT-Betrieb]

Die Daten auf IT-Systemen, die außerhalb der eigenen Liegenschaften eingesetzt werden, wie Notebooks, Mobiltelefone, Tablets, mobile Festplatten, Austauschsticks und weitere, müssen ausreichend durch Sicherheitsmaßnahmen geschützt werden. Vor allem sollte die Mitnahme von Datenträgern und IT-Komponenten auf Auslandsreisen klar geregelt werden. Dazu gehören folgende Regeln:

- Die IT-Systeme dürfen nicht als Fluggepäck aufgegeben werden, sondern sind direkt vom Reisenden (als Handgepäck) mitzuführen.
- IT-Systeme müssen stets sicher aufbewahrt werden. Bei Dienstreisen sollten sie nicht unbeaufsichtigt gelassen werden. Insbesondere sollten sie nicht in Fahrzeugen zurückgelassen werden.
- Die Absicherung des Zugriffs auf die IT-Systeme ist mit den vorgeschriebenen Sicherheitsmaßnahmen umzusetzen, z. B. durch PINs oder Passwörter.
- IT-Systeme oder Datenträger, die schützenswerte Daten enthalten, sollten möglichst komplett verschlüsselt werden. Wenn IT-Systeme eine einfach nutzbare Verschlüsselung ermöglichen, ist es empfehlenswert, dass diese Funktionen auch genutzt werden, wenn lediglich weniger schützenswerte Daten auf den IT-Systemen gespeichert sind. Die kryptographischen Schlüssel sollten getrennt vom verschlüsselten Gerät aufbewahrt werden.
- Es kann sinnvoll sein, für Auswärtseinsätze dedizierte mobile IT-Systeme zu nutzen. Die Verwaltung, Wartung und Weitergabe solcher extern eingesetzten IT-Systeme sollte geregelt werden. Hierzu können beispielsweise Geräte-Pools eingerichtet werden.
- Es sollte protokolliert werden, wann und von wem welche IT-Komponenten außer Haus eingesetzt werden und in welchem Land diese sich befinden.

Vor Reiseantritt sollte zunächst geprüft werden, welche internen Daten nicht unbedingt auf dem IT-System gebraucht werden. Ist es nicht notwendig, diese Daten auf dem Gerät zu belassen, sollten diese sicher gelöscht werden (siehe CON.7.M9 Sicherer Umgang mit mobilen Datenträgern). Ergibt sich allerdings die Notwendigkeit, schützenswerte Daten mit auf Reisen zu nehmen, sollte dies nur in verschlüsselter Form erfolgen.

Außerhalb der organisationseigenen Liegenschaften sind die Mitarbeiter für den Schutz der ihnen anvertrauten IT verantwortlich. Darauf und auf die zu ergreifenden Vorsichtsmaßnahmen sind sie hinzuweisen.

Dabei sollte schriftlich geregelt sein, welche mobilen Datenträger auf Auslandsreisen mitgenommen werden dürfen und welche Sicherheitsmaßnahmen dabei zu berücksichtigen sind (z. B. Schutz vor Schadsoftware, Verschlüsselung geschäftskritischer Daten, Aufbewahrung mobiler Datenträger). Mitarbeiter sollten diese Regelungen vor Reiseantritt kennen und beachten .

Es sollte festgelegt werden,

- welche IT-Systeme bzw. Datenträger außer Haus mitgenommen werden dürfen,
- wer IT-Systeme bzw. Datenträger außer Haus mitnehmen darf,
- welche grundlegenden Sicherheitsmaßnahmen dabei beachtet werden müssen (Virenschutz, Verschlüsselung schützenswerter Daten, Aufbewahrung, etc.).

Die Art und der Umfang der anzuwendenden Sicherheitsmaßnahmen für extern eingesetzte IT-Systeme hängen einerseits vom Schutzbedarf der darauf gespeicherten IT-Anwendungen und Daten und andererseits von der Sicherheit der Einsatz- bzw. Aufbewahrungsorte ab.

Aufbewahrung tragbarer IT-Systeme und schützenswerter Informationen

Die Benutzer von tragbaren IT-Systemen sind vor Auslandsreisen besonders darauf hinzuweisen, diese geeignet aufzubewahren. Benutzer mobiler IT-Systeme müssen darauf achten, dass sie die Geräte auch außerhalb der Institution sicher aufbewahren. Gleiches gilt auch für schützenswerte Informationen. Folglich werden Sicherheitshinweise gegeben, die bei der mobilen Nutzung zu beachten sind:

- Tragbare IT-Systeme sollten nicht unbeobachtet bzw. ungeschützt aufbewahrt werden. Auch beim Verlassen fremder Büroräumlichkeiten sollte darauf geachtet werden, dass die mitgebrachten IT-Systeme und Datenträger nicht ungesichert herumliegen. Deshalb sollte entweder der Raum verschlossen oder die IT-Systeme und Datenträger mitgenommen werden. Bei Verlassen des Raums sollte das Gerät ausgeschaltet oder die Zugriffssperre aktiviert werden, um einen unbefugten Zugriff zu unterbinden. Überall dort, wo andere Maßnahmen wie geeignete Zutrittskontrolle nicht umgesetzt werden können, sollten Diebstahl-Sicherungen eingesetzt werden.
- Auch in Hotelräumen sollten tragbare IT-Systeme nicht ungesichert zurückgelassen werden. Das Gerät kann z. B. im hotelzimmereigenen Safe eingeschlossen werden, sodass eine erste Hemmschwelle für den Diebstahl oder Missbrauch mobiler IT-Systeme errichtet wird. Hochschutzbedürftige Informationen sollten allerdings auch nicht in einem hoteleigenen Safe aufbewahrt werden.
- Schützenswerte Informationen, die nicht unbedingt benötigt werden, sollten auf Reisen nicht mitgeführt werden. Ist dies allerdings doch notwendig, sollten Informationen im Handgepäck mitgeführt werden. Das Handgepäck darf nie unbeaufsichtigt bleiben.
- Wichtige Hinweise und allgemeine Handlungsanweisungen zur geeigneten Aufbewahrung und zum sicheren Transport tragbarer IT-Systeme sollten neben der Aufnahme in die Sicherheitsrichtlinie für die Benutzer separat auf einem Merkblatt zusammengefasst werden.

CON.7.M14 Kryptografisch abgesicherte E-Mail-Kommunikation [Benutzer, IT-Betrieb]

E-Mails sollten von den Mitarbeitern entsprechend den internen Vorgaben der Institution kryptographisch abgesichert werden.

Bei der E-Mail-Kommunikation im Ausland sollten Benutzer ihre E-Mails verschlüsseln, wenn diese vertrauliche Informationen enthalten, damit diese im Rahmen der Ende-zu-Ende-Verschlüsselung inhaltlich nur dem Sender und Empfänger bekannt sind. E-Mails sollten so verschlüsselt werden, dass sie nicht auf dem Weg zwischen Sender und Empfänger manipuliert werden können. E-Mails ohne vertrauliche Informationen sollten zumindest signiert werden, um die Authentizität der Kommunikationspartner sicherzustellen.

Benutzer sollten nicht über öffentliche IT-Systeme auf ihre Mails zugreifen, da hier die Zugangsdaten oder sogar Inhalte der E-Mails in unberechtigte Hände gelangen können. Zu solchen öffentlichen IT-Systemen gehören z. B. Surfstationen in Hotels oder Rechner in Internetcafés. Diese sind nicht vertrauenswürdig.

Umsetzungshinweise und Empfehlungen zur kryptographische Absicherung der E-Mail Kommunikation ist im Baustein APP1.4 Groupware enthalten.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

CON.7.M15 Abstrahlsicherheit tragbarer IT-Systeme [IT-Betrieb] (C)

Es sollte vor Beginn der Reise festgelegt werden, welchen Schutzbedarf die einzelnen Informationen haben, die auf mobilen Datenträgern bzw. Clients im Ausland verarbeitet werden. Informationstragende oder auch bloßstellende Abstrahlung dieser Datenträger und Clients kann von anderen empfangen bzw. abgefangen werden, sodass Informationen rekonstruiert und die Vertraulichkeit dieser Daten in Frage gestellt werden können. Die Institution sollte hier prüfen, ob ein solcher Schutzbedarf für vertrauliche Informationen vorliegt, der abstrahlarme bzw. -sichere Datenträger und Clients erfordert.

Hersteller von PC-Bildschirmen werben häufig mit dem Begriff "abstrahlarm" nach MPR II, TCO oder SSI. Diese Richtlinien berücksichtigen jedoch ausschließlich mögliche gesundheitsschädliche Auswirkungen der Gerätestrahlung. Die Messverfahren und Grenzwerte für die Strahlung sind daher für den Nachweis bloßstellender Abstrahlung ungeeignet und ermöglichen wie auch Messungen zur elektromagnetischen Verträglichkeit (EMV) keine Bewertung der Sicherheit gegen unberechtigtes Mitlesen der Daten.

Daneben werden aber auch speziell abstrahlgeschützte IT-Systeme angeboten. Ein detailliertes Prüfkonzept des BSI dient zur abgestuften Prüfung von IT-Geräten bzw. -Systemen. Grundgedanke dieses Konzeptes ist es, den Umfang der Schutzmaßnahmen so gut wie möglich an die vom Anwender angenommene Bedrohungslage anzupassen, um so bei minimiertem Kostenaufwand ein Optimum an Abstrahlsicherheit zu erzielen. So kann z. B. in vielen Fällen ein nach dem Zonenmodell (siehe BSI Konzept zum Schutz staatlicher Verschlusssachen) geprüftes und für den Einsatz in den Zonen 1-3 zugelassenes Gerät (sog. "Zone 1-Gerät") bereits einen hinreichenden Schutz gegen unberechtigtes Abhören vertraulicher Daten infolge bloßstellender Abstrahlung bieten.

Als Beispiel sei erwähnt, dass bei Tastaturen durch die elektromagnetische Abstrahlung der Tastaturmatrix und des Verbindungskabels eine Abhörgefährdung besteht. Dies gilt auch für kabellose Tastaturen. Die Abhörgefährdung ist aber bei kabelgebundenen Tastaturen im Allgemeinen wesentlich geringer als die Abhörgefahr durch den Einsatz von Funkkommunikationsstrecken bei kabellosen Eingabegeräten. Für Systeme mit proprietären Sicherheitsmaßnahmen, die kein Sicherheitszertifikat aufweisen, ist der Sicherheitswert nicht einschätzbar. Der Benutzer geht hierbei das Risiko ein, dass die nicht evaluierte Lösung des Herstellers nur eine minimale Sicherheit bietet, die aber bei weitem nicht ausreicht, um seine Daten effektiv zu schützen.

Bei hohem oder sehr hohem Schutzbedarf in Bezug auf die Vertraulichkeit sollte deshalb geprüft werden, ob ein Hersteller abstrahlgeschützte Geräte gemäß dieser sog. "TEMPEST"-Kriterien in seinem Lieferprogramm anbietet.

Dies kann durch eine Rückfrage beim Hersteller, beim BSI bzw. durch Einsicht in die offizielle Produktübersicht BSI TL 03305, welche auf der Internetseite des BSI unter dem Stichwort Publikationen verfügbar ist, geklärt werden. Dabei gehört zu der Aussage, dass für ein Gerät eine TEMPEST-Zulassung vorliegt, immer auch die Aussage des Zulassungsgrades (z. B. zugelassen für den Einsatz in den Zonen 1-3 gemäß Zonenmodell).

CON.7.M16 Integritätsschutz durch Check-Summen oder digitale Signaturen (I)

Check-Summen werden im Rahmen der Datenübertragung oder auch Datensicherung verwendet, um die Integrität der Daten zu bewahren. Bei Check-Summen (Prüfsummen, Hash) handelt es sich um einen Wert, mit dem die Integrität von Daten überprüft werden kann. Vor z. B. dem Versenden von Daten sollte auf der Senderseite die Check-Summe von gespeicherten bzw. zu übertragenen Daten über ein entsprechendes Programm berechnet werden. Auf der Empfängerseite sollte anhand des gleichen Verfahrens die Check-Summe aus den empfangenen Daten errechnet und beide Check-Summen verglichen werden. Ein Abgleich beider Check-Summen lässt auf die Korrektheit oder auch Manipulation der übertragenen Daten schließen.

Besser noch sollten digitale Signaturen verwendet werden, um die Integrität von schützenswerten Informationen zu bewahren. Bei digitalen Signaturen handelt es sich um ein asymmetrisches Kryptoverfahren, bei dem z. B. eine E-Mail oder eine Datei mit einem Wert versehen wird, der als digitale Signatur bekannt ist. Diese Signatur kann die Integrität eines Dokumentes über eine Check-Summe und einen Zeitstempel für einen definierten Zeitpunkt sicherstellen. Mithilfe eines passend zugeordneten Verifikationsschlüssels kann der Empfänger dieser Nachricht die Integrität dieser feststellen.

Soll das mobile IT-System über Mechanismen zur **Integritätsprüfung** verfügen, sind folgende Anforderungen sinnvoll:

- Es sollten Verfahren zur Integritätsprüfung eingesetzt werden, die absichtliche Manipulationen am IT-System bzw. den darauf gespeicherten Daten sowie ein unbefugtes Einspielen von Programmen zuverlässig aufdecken können.
- Bei der Datenübertragung müssen Mechanismen eingesetzt werden, mit denen absichtliche Manipulationen an den Meta- und den Nutzdaten erkannt werden können. Daneben darf die bloße Kenntnis der eingesetzten Algorithmen ohne spezielle Zusatzkenntnisse nicht ausreichen, um unerkannte Manipulationen an den oben genannten Daten vornehmen zu können.

CON.7.M17 Verwendung dedizierter Reise-Hardware [IT-Betrieb] (CIA)

Zur Verhinderung des unberechtigten Abflusses von schützenswerter Informationen der Institution auf Auslandsreisen (z. B. bei der Einreise oder der Ausreise) sollten den Mitarbeitern vorkonfigurierte Reise-Notebooks zur Verfügung gestellt werden. Diese Reise-Notebooks sollten auf Basis des Minimalprinzips nur die Funktionen und Informationen zur Verfügung stellen, die zur Fortführung der Geschäftstätigkeit unbedingt erforderlich sind.

CON.7.M18 Eingeschränkte Berechtigungen auf Auslandsreisen [Fachverantwortliche, IT-Betrieb] (CI)

Vor Reiseantritt sollte die Institution prüfen, welche Berechtigungen der Mitarbeiter wirklich braucht, um seinem Alltagsgeschäft im Ausland nachgehen zu können. Dabei sollte geprüft werden, ob Zugriffsrechte, auf z. B. interne Laufwerke der Institution, für die Reisedauer dem Mitarbeiter entzogen werden können, um einen unbefugten Zugriff auf diese zu verhindern. Der Benutzer hat dann nur auf jene Laufwerke Zugriff, die zur Ausübung seiner Tätigkeit essentiell sind.

Bei Auslandsaufenthalten ist darauf zu achten, dass Benutzerumgebung und Startprozedur für den Benutzer und an seine Aufgabe angepasst sind. Sind Editor-Programme oder Compiler nicht für die Aufgabenerfüllung des Benutzers erforderlich, ist die Nutzung im Ausland zu unterbinden. Die Änderung oder der Abbruch von Startskripten durch den Benutzer ist zu verhindern. Es ist eine Regelung bzgl. der Nutzerumgebung temporärer Benutzerkonten bei Auslandsreisen zu treffen. Bei Auslandsreisen sind vorhandene Sicherheitsmaßnahmen und -merkmale des eingesetzten IT-Betriebssystems wie die Benutzerkontensteuerung (UAC) zu aktivieren, um die Einschränkung der Benutzerumgebung durchzusetzen. Der Zugriff von Auslandsreisenden auf das interne Netz ist auf das erforderliche Maß einzuschränken.

3 Weiterführende Informationen

3.1 Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Informationssicherheit auf Auslandsreisen" finden sich unter anderem in folgenden Veröffentlichungen:

[27001A7] ISO/IEC 27001:2013

Information technology - Security techniques - Information security management systems - Requirements, Insebsondere Annex A, A.7 Human resource security, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/SC 27, Oktober 2013

[ISFCF2] The Standard of Good Practice for Information Security

Area CF2 Human Resource Security, Information Security Forum (ISF), June 2018

[NIST80053] Security and Privacy Controls for Federal Information Systems and Organizations

NIST Special Publication 800-53, Revision 4, April 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf , zuletzt abgerufen am 30.08.2018

[TR03305] Technische Leitlinie BSI TL 03305 für staatliche VS zugelassene abstrahlgeprüfte Hardware

Bundesamt für Sicherheit in der Informationstechnik (BSI), Mai 2017, https://www.bsi.bund.de/DE/Publikationen/TL03305/TL03305_node.html , zuletzt abgerufen am 31.08.2018

[VPN] Empfehlungen zu VPNs

Weitere Empfehlungen des BSI zum sicheren Aufbau und Betrieb von VPNs finden sich hier: https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-VPN/vpn_node.html , zuletzt abgerufen am 31.08.2018

Umsetzungshinweise für die Bausteinschicht OPS

OPS.1.1: Kern-IT-Betrieb / Kernaufgaben

Umsetzungshinweise zum Baustein OPS.1.1.2 Ordnungsgemäße IT-Administration

1 Beschreibung

1.1 Einleitung

Die in diesem Dokument beschriebenen Umsetzungshinweise geben Hinweise und Hilfestellung, wie die Anforderungen des Bausteins *OPS.1.1.2 Ordnungsgemäße IT-Administration* geeignet umgesetzt werden können. Sie stellen Vorschläge dar, die den typischen Gegebenheiten in einem Informationsverbund gerecht werden. Sie schließen nicht aus, dass die Anforderungen des Bausteins auch auf anderen, für einen individuellen Informationsverbund möglicherweise besser geeigneten Wegen erreicht werden können.

1.2 Lebenszyklus

Der Baustein *OPS.1.1.2 Ordnungsgemäße IT-Administration* beschreibt IT-Prozesse. Von daher beschäftigt er sich hauptsächlich mit der Lebenszyklusphase *Umsetzung*, nur einzelne Aspekte reichen in andere Lebenszyklusphasen hinein.

Planung und Konzeption

Um einen ordnungsgemäßen IT-Administrationsprozess zu etablieren, sind verschiedene Vorüberlegungen erforderlich. Aufgaben und Befugnisse im IT-Betrieb müssen für die Beteiligten klar ersichtlich sein, wichtige Grundregeln sollten in einer Richtlinie fixiert sein (siehe hierzu *OPS.1.1.2.M7 Regelung der IT-Administrationstätigkeit*). Wegen der umfassenden Berechtigungen sind Administrationstätigkeiten besonders sensibel. Dies ist durch entsprechende Vorgaben für die Einstellung von Personal (siehe hierzu *OPS.1.1.2.M3 Geregelte Einstellung von IT-Administratoren*) und für die Freisetzung (siehe hierzu *OPS.1.1.2.M4 Beendigung der Tätigkeit als IT-Administrator*) zu berücksichtigen.

Sofern für die IT-Umgebung Hochverfügbarkeitsanforderungen bestehen, muss sichergestellt werden, dass die eingesetzten Komponenten, Architekturen und Prozesse diesen Anforderungen gerecht werden (siehe hierzu *OPS.1.1.2.M19 Berücksichtigung von Hochverfügbarkeitsanforderungen*).

Beschaffung

Beschaffungsprozesse werden von diesem Baustein nicht berührt.

Umsetzung

Bei der Umsetzung eines ordnungsgemäßen Administrationsprozesses müssen verschiedene Sicherheitsvorgaben berücksichtigt werden. Zunächst müssen geeignete Personen zur Wahrnehmung der festgelegten Administrationsrollen ausgewählt werden (siehe hierzu *OPS.1.1.2.M1 Personalauswahl für administrative Tätigkeiten*). Für diese Personen müssen entsprechende Administrationskonten eingerichtet werden (siehe hierzu *OPS.1.1.2.M5 Administrationszugänge*), wobei der administrative Zugang zu IT-Systemen und Komponenten geeignet geschützt werden sollte (siehe hierzu *OPS.1.1.2.M6 Schutz administrativer Zugänge*). Bei erhöhtem Schutzbedarf sollte dies auch eine netzseitige Abschirmung administrativer Zugänge und Oberflächen umfassen (siehe hierzu *OPS.1.1.2.M16 Zugangsbeschränkungen für administrative Zugänge*).

Administrative Zugriffe erfolgen nicht nur auf Systemebene, sondern häufig auch innerhalb von Fachanwendungen. Auch solche administrativen Aufgaben müssen im Betrieb geeignet abgebildet werden (siehe hierzu *OPS.1.1.2.M8 Administration von Fachanwendungen*). Wenn die Größe der Organisation es erlaubt, oder erhöhte Anforderungen an die Integrität es erfordern, sollten verschiedene administrative Aufgaben personell voneinander getrennt werden (siehe hierzu *OPS.1.1.2.M15 Aufteilung von IT-Administrationstätigkeiten*). Die für den IT-Betrieb vorhandenen Personalressourcen müssen ausreichen, um einen ordnungsgemäßen Systembetrieb auch bei Zwischenfällen oder Personalausfällen aufrecht zu erhalten (siehe hierzu *OPS.1.1.2.M9 Ressourcenplanung*).

Bei erhöhtem Schutzbedarf kann es zusätzlich erforderlich werden, administrative Tätigkeiten durchgängig zu protokollieren (siehe hierzu *OPS.1.1.2.M18 Durchgängige Protokollierung administrativer Tätigkeiten*) und/oder durchgängig im Vier-Augen-Prinzip durchzuführen (siehe hierzu *OPS.1.1.2.M17 IT-Administration im Vier-Augen-Prinzip*).

Betrieb

Im laufenden Betrieb ist insbesondere sicherzustellen, dass administrative Tätigkeiten geeignet dokumentiert werden (siehe hierzu *OPS.1.1.2.M11 Dokumentation von IT-Administrationstätigkeiten*). Damit das eingesetzte Personal mit Entwicklungen Schritt hält, die die Sicherheit ihres Informationsverbunds betreffen, sind geeignete Maßnahmen zur fortlaufenden Qualifizierung und Information erforderlich (siehe hierzu *OPS.1.1.2.M10 Fortbildung und Information*).

Aussonderung

Dieser Baustein enthält keine Anforderungen an die Aussonderung.

Notfallvorsorge

Damit auch in Notfallsituationen die Durchführung einer ordnungsgemäßen IT-Administration möglich bleibt, müssen geeignete Vorkehrungen getroffen werden (siehe hierzu *OPS.1.1.2.M2 Vertretungsregelungen und Notfallvorsorge*).

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Ordnungsgemäße IT-Administration" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

OPS.1.1.2.M1 Personalauswahl für administrative Tätigkeiten [Leiter Personal]

IT-Administratoren müssen über die erforderliche berufliche Qualifikation verfügen, um die ihnen übertragenen Aufgaben ordnungsgemäß bewältigen zu können. Für Administratoren bedeutet dies im Regelfall eine IT-bezogene Berufsausbildung , ein entsprechendes Studium oder eine langjährige Berufspraxis im IT-Bereich. Ergänzend können interne Schulungen oder Weiterbildungen die Qualifizierung der entsprechenden Mitarbeiter sicherstellen. Beispielsweise können so im Bedarfsfall zusätzliche Kenntnisse vermittelt werden, die für die jeweilige Aufgabe benötigt werden.

Mitarbeiter, die eine administrative Rolle haben, dürfen nicht gleichzeitig eine kontrollierende Rolle (z.B. Revision) übernehmen. Außerdem ist die Rolle Administration auch nicht mit allen anderen Rollen in einer Institution vereinbar, da es hier zu Interessenkonflikten kommen kann.

Für die Übernahme von Administrationsaufgaben muss gewährleistet sein, dass jedem Administrator und ebenso den Vertretern für eine sorgfältige Aufgabenerfüllung auch die hierfür erforderliche Zeit zur Verfügung steht. Hierbei muss auch berücksichtigt werden, dass Aus- und Fortbildungsmaßnahmen erforderlich sind.

Um zu ermitteln, welche Spezialkenntnisse in der IT-Administration erforderlich sind, und wie diese abgedeckt werden können, empfiehlt es sich, zunächst eine Übersicht der eingesetzten Plattformen , Produkte und Techniken zu erstellen. Dabei ist zu unterscheiden, welche Fertigkeiten von jedem einzelnen IT-Administrator beherrscht werden müssen, und welche vom IT-Administrationsteam insgesamt abzudecken sind. In einer Matrix kann dann ermittelt werden, bei welchen Personen die entsprechenden Kenntnisse vorhanden sind, und wie diese erworben wurden (Studium, Ausbildung, berufliche Praxis oder Schulung). Findet sich kein Kandidat mit allen geforderten Qualifikationen, so kann geprüft werden, ob vorhandene Lücken im Rahmen von Qualifizierungsmaßnahmen geschlossen werden können.

Bei den erforderlichen Qualifikationen sind auch Sprachkenntnisse zu berücksichtigen: So ist es zur Vermeidung von Missverständnissen erforderlich, dass IT-Administratoren die Sprache beherrschen, die von den Anwendern ihrer Systeme gesprochen wird, damit sie deren Anforderungen oder Problembeschreibungen verstehen und bearbeiten können. In multinationalen Institutionen kann dafür ersatzweise auch eine vereinbarte Konzernsprache, in der Regel Englisch, zum Einsatz kommen.

Eine gute Lesefähigkeit der englischen Sprache inklusive läufiger Fachtermini ist für IT-Administratoren auch deshalb von Bedeutung, weil Informationen aus Systemdokumentation, Anleitungen oder Fachforen häufig nur in englischer Sprache verfügbar sind.

Werden administrative Aufgaben an Dritte übertragen (z. B. externe Dienstleister oder freie Mitarbeiter), so müssen die erforderlichen Qualifikationen bei der Auswahl der Auftragnehmer und der Vergabe des Auftrags ebenfalls berücksichtigt werden. Dazu sollten entsprechende Vereinbarungen getroffen werden, welche Mindestqualifikationen das eingesetzte Personal erfüllen muss und welche laufenden Qualifizierungsmaßnahmen erfolgen sollen.

IT-Administratoren müssen über eine geeignete Persönlichkeit verfügen, um die ihnen übertragenen Aufgaben zuverlässig und sorgfältig zu erledigen. Bei der Besetzung von Stellen durch internes Personal gibt hierzu die bisherige Führung der betroffenen Personen gute Hinweise. Hierzu sollten entsprechende Informationen von den bisherigen Vorgesetzten eingeholt werden. Bei externen Kandidaten gibt die Überprüfung von Arbeitszeugnissen und weiteren Bewerbungsunterlagen wichtige Einblicke in den beruflichen Werdegang und kann Hinweise auf die generelle Eignung zur jeweiligen Tätigkeit und die Zuverlässigkeit im Allgemeinen geben. Im Rahmen der vereinbarten Probezeit muss überprüft werden, ob die Personen tatsächlich für die ihnen anvertrauten Aufgaben geeignet sind.

Für alle Mitarbeiter in der IT-Administration sollte im Rahmen des gesetzlich Erlaubten eine Prüfung des persönlichen Hintergrunds erfolgen, z. B. durch die Einholung eines persönlichen Führungszeugnisses.

Auch bei der Übertragung von administrativen Aufgaben an Dritte ist die Zuverlässigkeit des eingesetzten Personals sicherzustellen. Dazu muss vereinbart werden, ob die Prüfung durch den Auftragnehmer erfolgt und geeignet nachgewiesen wird, oder ob dem Auftraggeber entsprechende Befugnisse zur Überprüfung eingeräumt werden. Weiterhin ist festzulegen, wie verfahren wird, wenn der Auftraggeber den Einsatz bestimmter Personen ablehnt, wenn Hinweise auf persönliche oder fachliche Defizite dies erforderlich machen.

OPS.1.1.2.M2 Vertretungsregelungen und Notfallvorsorge

Für alle administrativen Aufgaben und Verantwortlichkeiten müssen ausreichende Vertretungsregelungen getroffen werden, die sicherstellen, dass die Aufgaben ordnungsgemäß wahrgenommen werden können, auch wenn der verantwortliche Mitarbeiter ausfällt. Im Falle des Ausfalls eines IT-Administrators sollten Regelungen existieren, die die ordnungsgemäße Wahrnehmung der administrativen Aufgaben gewährleisten. Es sollten für alle Anwendungen und Systeme neben dem Hauptverantwortlichen weitere Personen benannt werden, die für Wartung und Administration fachlich geeignet und mit den jeweiligen Systemen vertraut bzw. geeignet dafür geschult sind. Die Namen und Kontaktmöglichkeiten dieser Mitarbeiter sollten schriftlich festgehalten werden. Ein geeignetes Verfahren muss sicherstellen, dass die Vertreter vom Ausfall eines IT-Administrators Kenntnis erhalten und anstehende Aufgaben übernehmen.

In Notfallsituationen kann zur Umsetzung von Sofortmaßnahmen ein kurzfristiger Zugriff auf Systeme und Anwendungen erforderlich werden, ohne dass ein befugter IT-Administrator verfügbar ist. Für diesen Fall sollten administrative Notfallzugänge eingerichtet werden. Die Zugangsdaten für diese Administrationskennungen sollten derart aufbewahrt werden, dass nur dem befugten Personenkreis ein Zugriff möglich ist. Zudem sollten sie im Bedarfsfall schnell bereitgestellt werden können.

Passwörter sollten möglichst nur dann hinterlegt werden, wenn es keine andere (technische) Lösung gibt. Dabei ist immer zu beachten, dass die Hinterlegung von Passwörtern einen falschen Signalcharakter für den sicheren Umgang mit Passwörtern vermittelt. Passwörter sollten aber immer dann sicher hinterlegt werden, wenn diese die einzige Möglichkeit sind, auf IT-Systeme Zugriff zu nehmen. Dies ist häufig bei Administrator-Zugängen der Fall.

Eine Möglichkeit ist die Aufbewahrung von Authentikationsmitteln in einem nur der Leitungsebene oder einem Notfallteam zugänglichen Schutzschrank. Die Ausgabe der Zugangsdaten sollte dokumentiert werden. Durch die Hinterlegung der Zugangsdaten oder Zugangsmittel in verschlossenen Umschlägen kann erreicht werden, dass ihr Einsatz erkennbar ist und anschließend z. B. eine Änderung der Kennwörter und Hinterlegung in einem neuen Kuvert erfolgt. Es sollte regelmäßig überprüft werden, dass aktuelle Passwörter und Authentikationsmittel hinterlegt sind.

OPS.1.1.2.M3 Geregelte Einstellung von IT-Administratoren [Leiter Personal]

Wenn Personen in der Institution administrative Aufgaben übernehmen, müssen ihre Aufgaben und Zuständigkeiten schriftlich festgelegt werden, z. B. in Form einer Stellenbeschreibung mit Aufgaben und Kompetenzen.

Sind geeignete interne oder externe Mitarbeiter ausgewählt, die die entsprechenden Voraussetzungen erfüllen (siehe *OPS.1.1.2.M1 Personalauswahl für administrative Tätigkeiten*), so müssen sie nach einem geregelten Verfahren in ihre Tätigkeit eingeführt werden. Dabei sind mindestens die folgenden Aspekte zu berücksichtigen:

- Die Nachweise über die Erfüllung der fachlichen und persönlichen Voraussetzungen sind systematisch abzulegen (z. B. in einer Personalakte).
- Eventuell vorhandene Qualifikationslücken sind vor Aufnahme der damit verbundenen Aufgaben durch geeignete Schulungsmaßnahmen zu schließen.
- Verpflichtungen und Belehrungen sind durchzuführen (in der Regel mindestens eine Verpflichtung auf das Datengeheimnis nach § 5 BDSG).
- Sicherheitsrichtlinien und Sicherheitsbestimmungen der Institutionen sowie die Aufbau- und Ablauforganisation im ISMS sind zu vermitteln.
- Meldewege und Ansprechpartner für Sicherheitsvorfälle sind bekannt zu machen.
- Die Struktur und die eingesetzten Verfahren für die Dokumentation sind zu erläutern.
- Personenbezogene Administrationskonten sind im erforderlichen Umfang einzurichten. Die Zugangsmittel (Kennwörter, Smartcards, Token...) sind zu initialisieren und sicher zu übergeben.
- Die IT-Administratoren sind in die von ihnen zu betreuenden Systeme und Netze einzuweisen.

Um eine vollständige Umsetzung dieser und eventueller weiterer, für die jeweilige Institution relevanter Punkte sicherzustellen, empfiehlt sich die Gestaltung von Checklisten oder Laufzetteln, die von den neuen IT-Administratoren abzuarbeiten sind und gleichzeitig die ordnungsgemäße Durchführung aller Aufgaben dokumentieren.

OPS.1.1.2.M4 Beendigung der Tätigkeit als IT-Administrator [Leiter Personal]

Wenn interne oder externe Mitarbeiter von einer Tätigkeit in der IT-Administration entbunden werden, muss ebenfalls sichergestellt werden, dass alle Unterlagen, Arbeitsmaterialien und Befugnisse wieder entzogen werden. Dies umfasst z. B.:

- Deaktivierung/Sperrung von Administrations- und Benutzerkonten
- Änderung von Kennwörtern nicht-personenbezogener administrativer Zugänge, deren Kennwörter dem ausscheidenden Mitarbeiter bekannt sind.
- Änderung der Kennwörter für WLAN-Zugänge
- Sperrung von VPN- oder Remote-Zugängen
- Sperrung von Benutzer- und Gerätezertifikaten, deren zugehörige Schlüssel unter der Gewalt des Mitarbeiters stehen oder standen
- Sperrung von Zugängen zu externen Diensten (z. B. Cloud-Anwendungen)
- Abgabe von Zutrittskarten oder Authentisierungsmitteln (Smartcards, Token)
- Rückgabe von mobilen IT-Geräten
- Prüfung und Anpassung von Alarmierungsplänen und Vertretungsregelungen
- Information betroffener Stellen über das Ausscheiden des Mitarbeiters (Mitarbeiter, Wachschutz, Pforte, Dienstleister, Lieferanten, Domainverwalter).

Die hier aufgeführten Punkte stellen Beispiele dar, die für die jeweils eigene Institution zu prüfen und nach Bedarf um weitere Punkte zu ergänzen sind.

Auch für die Freisetzung von IT-Administratoren empfiehlt sich der Einsatz entsprechender Checklisten oder Laufzettel, um die vollständige Abarbeitung der erforderlichen Schritte sicherzustellen und zu dokumentieren.

OPS.1.1.2.M5 Administrationskennungen

Für den administrativen Zugang zu IT-Systemen und Anwendungen müssen personenbezogene Administrationskennungen eingerichtet und verwendet werden, soweit dies technisch möglich ist. Die Nutzung einer zentralen Administrationskennung durch mehrere Personen führt dazu, dass Vorgänge nicht der ausführenden Person zugeordnet werden können. Daher muss für jede administrativ tätige Person eine zusätzliche administrative Kennung zur Verfügung gestellt werden.

Sofern der Einsatz übergreifender, nicht personenbezogener administrativer Kennungen im Einzelfall unumgänglich ist, sollte sichergestellt werden, dass die Verwendung der Kennung nachvollziehbar dokumentiert wird. Dies kann z. B. auf Unix-Systemen erreicht werden, indem zunächst eine Anmeldung mit einer persönlichen Kennung erfolgt und von dort mit dem Kommando "su" auf die übergreifende Kennung (z. B. "root") gewechselt wird. Denkbar wäre ein Nachweis auch durch die Nutzung sogenannter Sprungserver, auf denen aus einer personenbezogenen Sitzung heraus administrative Zugänge verwendet werden. Ist eine technische Umsetzung aufgrund besonderer Umstände überhaupt nicht möglich, sollten von den IT-Administratoren ersatzweise Aufzeichnungen über die Verwendung übergreifender Administrationskennungen geführt werden.

Die Rechte der Administrationszugänge sind immer den jeweiligen Erfordernissen anzupassen. Für einen Mitarbeiter, der ausschließlich die Datenbank administriert, sind beispielsweise keine Systemverwalter-Rechte oder Zugang zur Konfiguration des Mailservers notwendig. Gegebenenfalls davon abgeleitete Rechte, wie zum Beispiel die Möglichkeit, den Datenbank-Dienst auf Betriebssystemebene zu starten und zu beenden, müssen im Bedarfsfall ebenfalls vergeben werden.

Für Routinetätigkeiten muss eine persönliche, unprivilegierte Kennung benutzt werden. Dies umfasst alle nicht-administrativen Tätigkeiten, wie zum Beispiel Recherchetätigkeiten oder E-Mail-Kommunikation. So wird sichergestellt, dass einerseits keine unbeabsichtigten administrativen Änderungen am Informationsverbund stattfinden, andererseits aber auch Angriffe über externe Kommunikationsschnittstellen (E-Mail, WWW) nicht direkt auf Zugänge mit administrativen Berechtigungen wirken können.

Beispiel: Beim versehentlichen Ausführen eines als E-Mail-Anhang eingeschleusten Verschlüsselungstrojaners unter einer administrativen Kennung kann die Schadsoftware in kurzer Zeit sämtliche Dokumente in den Dateiablagen im Netz verschlüsseln. Erfolgt dasselbe Szenario unter Nutzung einer eingeschränkten Benutzerkennung, so ist der Schaden beschränkt auf die Dateien, die unter dieser Kennung im Schreibzugriff zugänglich sind.

OPS.1.1.2.M6 Schutz administrativer Kennungen

Der Zugang zu Administrationskennungen muss durch geeignete Authentisierungsmechanismen angemessen geschützt sein. Für Administrationskennungen sollte eine Zwei-Faktor-Authentisierung verwendet werden, bei der in der Regel zusätzlich zum Passwort ein weiterer Faktor hinzukommt, z. B.

- Hardware-Token mit dynamisch generierten Codes,
- mobile Geräte, an die dynamisch erzeugte Anmeldecodes gesendet werden,
- kryptographische Zertifikate, die an ein bestimmtes Gerät oder eine bestimmte Hardware (Chipkarte/Token) gebunden sind,
- biometrische Authentisierungsverfahren, sofern sie eine ausreichende Zuverlässigkeit und Sicherheit bieten.

Bei erhöhtem Schutzbedarf muss eine Zwei-Faktor-Authentisierung verwendet werden.

Auf diese Weise wird verhindert, dass ein potenzieller Angreifer alleine durch das Ausspähen von Passwörtern Zugriff auf geschützte Systeme bekommt, da ein weiterer Faktor, z. B. der Besitz einer Hardware oder entsprechende biometrische Eigenschaften, für eine Anmeldung erforderlich ist.

Einen etwas schwächeren Schutz bieten kryptographische Zertifikate, die in Software abgelegt und durch ein Passwort geschützt sind. Die Verwendung solcher Zertifikate kann z. B. beim Einsatz von SSH konfiguriert werden. Die Ablage der Zertifikate sollte so erfolgen, dass ein unbefugter Zugriff ausgeschlossen wird. Gegenüber hardwaregebundenen Zertifikaten besteht hierbei die grundsätzliche Gefahr, dass das Zertifikat von einem Angreifer kopiert und das Zugangspasswort ausgespäht oder erraten wird, dennoch bietet dieses Verfahren einen deutlichen Sicherheitsgewinn gegenüber Passwörtern alleine.

Bei der Verwendung von Benutzernamen und Passwörtern muss eine Passwortrichtlinie mit entsprechend hohen Anforderungen an die Komplexität von Passwörtern Anwendung finden. Da lange und komplexe Kennwörter nur schwierig zu merken sind, können Passwortverwaltungs-Programme zum Einsatz kommen, die Passwörter in einer verschlüsselten Datenbank ablegen. Diese Datenbank muss ihrerseits mit einem starken Passwort geschützt sein.

Passwörter für selten genutzte, privilegierte Zugänge (z. B. hinterlegte Notfallnutzer oder technische Nutzer von Diensten oder Datenbanken), bei denen eine Anmeldung durch IT-Administratoren nur im Ausnahmefall erfolgen muss, sollten deutlich länger gewählt werden, als es die Mindestvorgaben für Benutzerpasswörter in der Institution erfordern, um die Robustheit gegen Angriffe zu erhöhen.

Für Administrationszugriffe müssen sichere Protokolle verwendet werden, die die Kommunikation verschlüsseln, sofern nicht die lokale Konsole verwendet wird. Bei Unix-Derivaten sollte beispielsweise SSH und bei Windows RDP verwendet werden. Der Zugriff auf Web-Oberflächen muss mittels TLS abgesichert sein.

Jeder Anmeldevorgang über Administrationskennung muss protokolliert werden. Die Protokollierung muss idealerweise derart erfolgen, dass der angemeldete Benutzer keine Möglichkeit hat, das Protokoll zu verändern. Dies kann zum Beispiel realisiert werden, in dem die Protokollierung über ein Protokoll wie z. B. syslog auf einem separaten Protokollierungssystem erfolgt. Dabei ist sicherzustellen, dass das betroffene System und das Protokollierungssystem über eine einheitlich synchronisierte Systemzeit verfügen, um die Rekonstruktion von Vorgängen anhand der Protokolldaten zu erleichtern.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Ordnungsgemäße IT-Administration".

OPS.1.1.2.M7 Regelung der IT-Administrationstätigkeit [Leiter Personal]

Mitarbeiter mit IT-Administrationsaufgaben benötigen für ihre Arbeit umfangreiche Zugriffsmöglichkeiten auf Systeme, Anwendungen und Datenbestände. Administrative Zugriffe unterliegen oft gerade nicht der Berechtigungssteuerung, weil z. B. bei der Fehleranalyse umfassende Zugriffsmöglichkeiten erforderlich sind, oder weil die Systeme und Anwendungen eine Rechteeinschränkungen für Administratoren gar nicht vorsehen. Aber nicht alles, was die Mitarbeiter mit ihren Berechtigungen tun können, dürfen sie auch tun – sonst wäre ein ordnungsgemäßer und nachvollziehbarer IT-Betrieb nicht mehr gegeben. Für Zugriffe auf personenbezogene Daten oder Telekommunikationsinhalte gelten zudem gesetzliche Beschränkungen, die auch in der IT-Administration umgesetzt werden müssen.

Die Institution sollte daher Regelungen für die IT-Administration treffen und diese verbindlich in einer Arbeitsanweisung oder Richtlinie festschreiben. Dabei sollten folgende Inhalte berücksichtigt werden:

- Die Organisation des IT-Betriebs sollte beschrieben werden. Dies umfasst insbesondere die Aufgabenteilung in der IT-Administration inklusive entsprechender Vertretungsregelungen. Für jede IT-Komponente oder Anwendung muss klar nachvollziehbar sein, wer die administrative Verantwortung trägt. In größeren Institutionen kann auch eine Abgrenzung der Verantwortung für Planung, Beschaffung und Einführung, Betrieb und Weiterentwicklung sowie Aussonderung sinnvoll sein.
- Die Rolle Administration ist nicht mit allen anderen Rollen in einer Institution vereinbar. Beispielsweise muss beim Einsatz von Protokollierung auf die Rollentrennung von Administration und Revision geachtet werden. In Bereichen mit erhöhten Sicherheitsanforderungen können weitere Rollenausschlüsse erforderlich sein (siehe OPS.1.1.2.M14).
- Bei größeren Institutionen mit einer Vielzahl verschiedener IT-Systeme und Teilnetzen muss außerdem sichergestellt sein, dass die Aufgaben zwischen den verschiedenen Administratoren so verteilt sind, dass es zu keinen Zuständigkeitsproblemen kommt, also weder zu Überschneidungen noch zu Lücken in der Aufgabenverteilung. Darüber hinaus sollte die Kommunikation zwischen den verschiedenen Administratoren möglichst reibungslos ablaufen. Hierzu können z. B. regelmäßige Administratoren-Treffen durchgeführt werden, bei denen typische Probleme und Lösungsmöglichkeiten bei der täglichen Arbeit thematisiert werden.
- Regeln für den Umgang mit administrativen Zugängen sollten festgelegt werden (siehe OPS.1.1.2.M4).
- Befugnisse und Pflichten der Administratoren sollten beschrieben sein. Dazu gehört insbesondere auch ein Verbot des Zugriffs auf schützenswerte Datenbestände (z. B. E-Mail-Postfächer, Protokolldaten), wenn für den Zugriff keine betriebliche Notwendigkeit besteht.
- Für Änderungen am Informationsverbund sollten Antrags- und Freigabeverfahren etabliert werden. IT-Administratoren dürfen keine Änderungen vornehmen, für die nicht ein Auftrag und eine Freigabe vorliegen, oder die zur unmittelbaren Gefahrenabwehr erforderlich sind.
- Dokumentationspflichten der IT-Administratoren sollten beschrieben werden. Dies schließt die Form der Dokumentation, ihren Ablageort und Verpflichtungen zu einer angemessenen Aktualitätsprüfung ein.
- Die Pflichten und Befugnisse der IT-Administratoren im Rahmen der Aufklärung und Abwehr von Sicherheitsvorfällen sollten geregelt sein.

Die Richtlinie oder Arbeitsanweisung sollte von einer dazu befugten Führungsebene in Kraft gesetzt und allen IT-Administratoren zur Kenntnis gebracht werden. Sie muss in der jeweils aktuellen Fassung an einem definierten Ablageort für alle betroffenen Mitarbeiter zugänglich sein. In geeigneten Abständen sollte eine Prüfung und Anpassung sowie Bestätigung der Regelungen erfolgen.

OPS.1.1.2.M8 Administration von Fachanwendungen [IT-Betrieb]

Häufig nehmen Mitarbeiter in Fachbereichen einer Institution auch administrative Aufgaben für einzelne in Fachanwendungen wahr. Diese können sich mit den administrativen Aufgaben der Administratoren des IT-Betriebs überschneiden. Um eine gegenseitige Beeinträchtigung sowie Unklarheiten über die Verantwortungsbereiche zu vermeiden, sollten die spezifischen Aufgaben der Anwendungsadministratoren und Systemadministratoren schriftlich dokumentiert werden. Zudem sollten feste Ansprechpartner und Kommunikationsschnittstellen definiert werden, um den fachlichen Austausch zu erleichtern.

Sind administrative Eingriffe in den Anwendungsbetrieb notwendig, sollten die Fachadministratoren des jeweiligen Fachbereiches vorher über die anstehende Wartung und damit verbundene Beeinträchtigungen oder Änderungen informiert werden. Dies kann zum Beispiel bei Versionswechseln oder Wartungsfenstern der Fall sein. Zudem sollte eine Abstimmung mit dem Fachbereich angestrebt werden, um den Zeitpunkt des Wartungsfensters möglichst günstig zu legen und Anforderungen der Anwender zu berücksichtigen.

Die Anforderungen dieses Bausteins sind auch für die Anwendungsadministratoren umzusetzen, soweit dies innerhalb der Anwendungen möglich ist. So sollten administrative Aufgaben nur mit dafür vorgesehenen, personalisierten und besonders berechtigten Administrationskonten durchgeführt werden. Der Zugang zu Administrationsoberflächen sollte geeignet geschützt werden. Für den Zugriff auf Datenbestände (wie z. B. Anwendungsprotokolle) mit administrativen Rechten sollten geeignete Regelungen festgeschrieben werden. Geeignete Dokumentationsvorgaben sollten vereinbart werden.

OPS.1.1.2.M9 Ausreichende Ressourcen für den IT-Betrieb

Für alle anfallenden administrativen Tätigkeiten sollten ausreichende Sach- und Personalressourcen bereitgestellt werden, um diese ordnungsgemäß zu bewältigen. Diese sollten sowohl die anfallenden Routineaufgaben, als auch unvorhersehbare Tätigkeiten berücksichtigen. Insbesondere für die Behandlung und Aufklärung sicherheitsrelevanter Ereignisse sollten geeignete Reserven bereitstehen, um derartige Vorfälle zeitnah zu bearbeiten. Eine Aufrechterhaltung eines ordnungsgemäßen IT-Betriebs muss auch gewährleistet sein, wenn IT-Administratoren durch Urlaube, Krankheiten oder Fortbildungen nicht verfügbar sind. Entsprechend ausgebildete Personen sowie die notwendige technische Ausstattung sollten daher in der Ressourcenplanung berücksichtigt werden.

Fehlende Personalressourcen führen im Regelfall dazu, dass Dokumentationstätigkeiten entfallen und die Fehlerquote steigt.

In regelmäßigen Zyklen, beispielsweise jährlich, sollte die Ressourcenplanung einer Überprüfung unterzogen werden. Die Erfassung tatsächlich verwendeter Ressourcen und eine Analyse aller Faktoren hilft dabei, die Planung den aktuellen Erfordernissen anzupassen. Dabei sollte auch die Entwicklung der Bedrohungslage berücksichtigt werden, z. B. durch die Einbeziehung entsprechender Studien von Sicherheitsunternehmen oder Lagebildern von Stellen wie dem Bundesamt für Sicherheit in der Informationstechnik.

Im Zuge der Ressourcenplanung sollten auch für den IT-Betrieb erforderliche Sachmittel berücksichtigt werden. Dazu gehören beispielsweise ausreichend Krypto-Token, um sichere Authentikation von Administratoren bzw. einfache Verschlüsselung vertraulicher Daten zu ermöglichen.

OPS.1.1.2.M10 Fortbildung und Information [Leiter Personal]

Administratoren sollten kontinuierlich ihren Kenntnisstand entsprechend dem technischen Fortschritt erweitern. Daher sollte es ihnen ermöglicht werden, an passenden Fort- und Weiterbildungsmaßnahmen teilzunehmen. Diese sollten in einem Schulungsplan für das gesamte IT-Administrationsteam festgehalten werden. Ziel ist, das Wissen IT-Administratoren zum einen fachlich auf dem aktuellen Stand der Technik zu halten und zum anderen über neue Entwicklungen zu informieren, die für die Institution aktuell oder zukünftig von Bedeutung sein können. Auch sollte innerhalb des Teams abgestimmt werden, dass relevante Qualifikationen jeweils von mehreren Mitarbeitern abgedeckt werden, so dass Vertretungen möglich sind.

Den IT-Administratoren sollten geeignete Möglichkeiten geschaffen werden, um sich über Neuerungen bei den von ihnen verwalteten Lösungen zu informieren. Viele Anbieter versenden Newsletter oder Benachrichtigungen bei Sicherheitslücken und Produktupdates oder veranstalten Anwenderforen, in denen sie über Neuigkeiten informieren. Bei größeren Neuerungen sollten geeignete Schulungen erfolgen oder Möglichkeiten zu Recherchen und zum Literaturstudium bestehen.

Administratoren sollten sich regelmäßig über die Sicherheit der von ihnen betreuten Systeme, Dienste und Protokolle informieren, vor allem über aktuelle Gefährdungen, bekannt gewordene Schwachstellen und erforderliche Sicherheitsmaßnahmen. Informationsquellen zu diesem Thema sind beispielsweise:

- Das Bundesamt für Sicherheit in der Informationstechnik (BSI) (siehe http://www.bsi.bund.de/)
- Hersteller bzw. Distributoren von Programmen und Betriebssystemen. Diese informieren oft registrierte Kunden über bekannt gewordene Sicherheitslücken ihrer Systeme und stellen korrigierte Varianten des Systems oder Patches zur Behebung der Sicherheitslücken zur Verfügung.
- Computer Emergency Response Teams (CERTs). Dies sind Computer-Notfallteams, die als zentrale Anlaufstelle für präventive und reaktive Maßnahmen in bezug auf sicherheitsrelevante Vorfälle in Computersystemen dienen. CERTs informieren in sogenannten Advisories über aktuelle Schwachstellen in Hard- und Softwareprodukten und geben Empfehlungen zu deren Behebung. Verschiedene Organisationen oder Verbände unterhalten eigene CERTs.
- CERT-Bund, Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn, Telefon: 0228 99-9582-222, Fax: 022899-9582-5427, E-Mail: certbund@bsi.bund.de, WWW: https://www.bsi.bund.de/certbund/
- DFN-CERT, Zentrum für sichere Netzdienste GmbH, DFN-CERT, DFNCERT Services GmbH, Sachsenstraße 5, D-20097 Hamburg, Telefon: 040-808077-555, Fax: -556, E-Mail: info@dfn-cert.de, WWW: http://www.dfn-cert.de.
- An verschiedenen Hochschulen existieren CERTs, die auch Informationen öffentlich zur Verfügung stellen. Ein Beispiel ist das RUS-CERT der Universität Stuttgart (siehe http://cert.uni-stuttgart.de).
- Hersteller- und systemspezifische sowie sicherheitsspezifische Diskussionsgruppen oder Mailinglisten. In solchen Foren werden Hinweise auf existierende oder vermutete Sicherheitslücken oder Fehler in diversen Betriebssystemen und sonstigen Softwareprodukten diskutiert. Besonders aktuell sind meist die englischsprachigen Mailinglisten wie Bugtraq, von denen es an vielen Stellen öffentlich zugängliche Archive gibt, beispielsweise unter http://www.securityfocus.com.
- Manche IT-Fachzeitschriften veröffentlichen ebenfalls regelmäßig Beiträge mit einer Übersicht über neue Sicherheitslücken in verschiedenen Produkten.

Idealerweise sollten sich die Administratoren und Sicherheitsbeauftragte bei mindestens zwei verschiedenen Stellen über Sicherheitslücken informieren. Dabei ist es empfehlenswert, neben den Informationen des Herstellers auch eine "unabhängige" Informationsquelle zu benutzen.

Die Administratoren sollten jedoch in jedem Fall auch produktspezifische Informationsquellen des Herstellers nutzen, um beispielsweise darüber Bescheid zu wissen, ob für ein bestimmtes Produkt beim Bekanntwerden von Sicherheitslücken überhaupt Patches oder Updates bereitgestellt werden. Bei Produkten, für die der Hersteller keine Sicherheitspatches mehr zur Verfügung stellt, muss rechtzeitig geprüft werden, ob ein Einsatz unter diesen Umständen noch zu verantworten ist und durch welche zusätzlichen Maßnahmen ein Schutz der betroffenen Systeme trotzdem gewährleistet werden kann.

OPS.1.1.2.M11 Dokumentation von IT-Administrationstätigkeiten [IT-Betrieb]

Änderungen, die an Systemen oder Fachanwendungen vorgenommen wurden, sollten in geeigneter Form dokumentiert werden. Eine nachvollziehbare Dokumentation ist notwendig, um jederzeit einen Überblick über die IT-Systeme des Informationsverbunds zu haben und einen reibungslosen Betriebsablauf gewährleisten zu können. Dieses muss auch für Vertreter möglich sein, falls ein Administrator unvorhergesehen ausfällt. Eine nachvollziehbare Dokumentation ist auch Voraussetzung, um Prüfungen des Systems (z. B. auf problematische Einstellungen, Konsistenz bei Änderungen) durchführen zu können. Daher sollten die Veränderungen, die Administratoren am System vornehmen, dokumentiert werden, nach Möglichkeit automatisiert. Dieses gilt insbesondere für Änderungen an Systemverzeichnissen und -dateien. Vorhandene Protokollierungsmechanismen von Systemen und Anwendungen sollten dabei in einem geeigneten Umfang aktiviert werden.

Für alle Änderungen sollte außerdem dokumentiert werden, wer die Änderung beauftragt hat, wer sie durchführt und was damit bezweckt werden soll. Hierfür können entsprechende systembezogene Dokumente (Systemlogbücher) eingesetzt werden, aber auch zentrale Ticket-Systeme, in denen unter anderem der ausführende Mitarbeiter, der Anlass, der Zeitpunkt und die Beschreibung der Änderungen selbst erfasst werden. Ist das Ticket-System an eine CMDB (Configuration Management Database) angebunden, lassen sich so alle Änderungen direkt Systemen, Mitarbeitern und Kategorien zuordnen und nachverfolgen.

OPS.1.1.2.M12 Regelungen für Wartungs- und Reparaturarbeiten [IT-Betrieb]

Um die IT vor Störungen zu bewahren, müssen regelmäßig Wartungsarbeiten durchgeführt werden. Die rechtzeitige Einleitung von Wartungsarbeiten und die Überprüfung ihrer Durchführung sollte von einer zentralen Stelle aus wahrgenommen werden (z. B. Beschaffungsstelle). Die Wartungsarbeiten sollten von vertrauenswürdigen Personen oder Firmen ausgeführt werden, falls sie nicht von eigenem Personal durchgeführt werden können. Die Hinweise des Herstellers müssen dabei unbedingt beachtet werden. Bei regelmäßigen Wartungsarbeiten durch Externe kann der Abschluss eines Wartungsvertrages vorteilhaft sein.

Für jedes IT-System sollte dokumentiert werden, wann es gewartet wurde und welche Fehler dabei behoben wurden(z. B. Gerätepass oder Geräte- bzw. Konfigurationsmanagementsystem). Es empfiehlt sich außerdem, ein Informationssystem für Wartungs- und Reparaturarbeiten einzurichten. Mit einem solchen System können anstehende Arbeiten geplant und durchgeführte Arbeiten dokumentiert sowie der erfolgreiche Verlauf kontrolliert werden.

Außerdem sollte darin dokumentiert sein, wer für die Wartung oder Reparatur von Geräten verantwortlich ist.

Regelmäßige Reinigung von IT-Geräten

Alle Arten von IT-Geräten sollten regelmäßig gereinigt werden. Die hierfür empfehlenswerten Intervalle hängen von der Art des Gerätes bzw. der Einsatzumgebung ab. Mindestens einmal pro Jahr sollte aber eine Reinigung erfolgen, nicht nur weil es unangenehm ist, mit verschmutzten Geräten zu arbeiten, sondern auch weil Verschmutzungen deren Funktionsfähigkeit beeinträchtigen können.

Beispiele: Tastaturen sollten spätestens dann gesäubert werden, wenn sie klebrig werden oder einzelne Tasten klemmen. Ein Arbeitsplatz-PC sollte gelegentlich (z. B. einmal jährlich) auch innen von Staub befreit werden, sofern die Herstellerangaben nicht eine andere Vorgehensweise vorschlagen. Bei Druckern kann bei nachlässiger Reinigung die Druckqualität leiden oder Komponenten in der Funktion eingeschränkt oder sogar beschädigt werden. Typische Problempunkte sind Druckerwalzen, Druckköpfe und Tonerstaub-Ansammlungen.

Zu viel Staub in IT-Systemen kann zu einem Hitzestau führen. Durch Verunreinigungen auf Platinen (besonders wirkungsvoll sind Kombinationen aus Staub und Teer- und Nikotinablagerungen) können Kriechströme verursacht werden.

Ablagerungen sollten daher regelmäßig vorsichtig entfernt werden. Insbesondere sollte für eine wirkungsvolle Lüftung aller IT-Systeme gesorgt werden. Alle Belüfter und Lüftungskomponenten müssen von störenden Verunreinigungen frei gehalten werden.

Bei der Reinigung von IT-Geräten sind unbedingt die Vorgaben des Herstellers zu beachten, sowohl bei der Vorgehensweise und Werkzeug-Auswahl als auch bei den Mindest-Wartungsintervallen.

Wartungs- und Reparaturarbeiten im Hause

Für Wartungs- und Reparaturarbeiten im Hause, vor allem wenn sie durch Externe durchgeführt werden, sind Regelungen über deren Beaufsichtigung zu treffen: während der Arbeiten sollte eine fachkundige Kraft die Arbeiten soweit beaufsichtigen, dass sie beurteilen kann, ob während der Arbeit unautorisierte Handlungen vollzogen werden. Weiterhin ist zu überprüfen, ob der Wartungsauftrag im vereinbarten Umfang ausgeführt wurde.

Als Maßnahmen vor und nach Wartungs- und Reparaturarbeiten sind einzuplanen:

- Wartungs- und Reparaturarbeiten sind gegenüber den betroffenen Mitarbeitern rechtzeitig anzukündigen.
- Wartungstechniker müssen sich auf Verlangen ausweisen.
- Der Zugriff auf Daten durch den Wartungstechniker ist soweit wie möglich zu vermeiden. Falls erforderlich, sind Speichermedien vorher auszubauen oder zu löschen (nach einer kompletten Datensicherung), insbesondere wenn die Arbeiten extern durchgeführt werden müssen. Falls das Löschen nicht möglich ist (z. B. aufgrund eines Defektes), sind die Arbeiten auch extern zu beobachten bzw. es sind besondere vertragliche Vereinbarungen zu treffen und vertrauenswürdige Firmen auszuwählen.
- Die dem Wartungstechniker eingeräumten Zutritts-, Zugangs- und Zugriffsrechte sind auf das notwendige Minimum zu beschränken und nach den Arbeiten zu widerrufen bzw. zu löschen.
- Nach der Durchführung von Wartungs- oder Reparaturarbeiten sind, je nach "Eindringtiefe" des Wartungspersonals, Passwortänderungen erforderlich. Im IT-Bereich sollte eine Überprüfung auf Schadsoftware durchgeführt werden.
- Die durchgeführten Wartungsarbeiten sind zu dokumentieren (Umfang, Ergebnisse, Zeitpunkt, Firmenname sowie eventuell Name des Wartungstechnikers).
- Beauftragte Firmen sollten schriftlich zusichern, dass sie einschlägige Sicherheitsvorschriften und Richtlinien (z. B. VdS 2008 Feuergefährliche Arbeiten, Richtlinien für den Brandschutz) beachten. Dies gilt für alle Tätigkeiten, bei denen eine direkte oder indirekte Gefahr für Gebäude oder Menschen entstehen können. Letztlich kommt es darauf an, dass das vor Ort eingesetzte Personal mit diesen Regeln vertraut ist.
- Im Anschluss an die Wartungs- oder Reparaturarbeiten ist die ordnungsgemäße Funktion der gewarteten Anlage zu überprüfen. Insbesondere die Rücknahme der für Testzwecke vorgenommenen Eingriffe ist zu kontrollieren.

Externe Wartungs- und Reparaturarbeiten

Werden IT-Systeme zur Wartung oder Reparatur außer Haus gegeben, sind alle sensitiven Daten, die sich auf Datenträgern befinden, vorher physikalisch zu löschen. Ist dies nicht möglich, weil aufgrund eines Defekts nicht mehr auf die Datenträger zugegriffen werden kann, sind die mit der Reparatur beauftragten Unternehmen auf die Einhaltung der erforderlichen Informationssicherheitsmaßnahmen zu verpflichten. Mit diesen sind vertragliche Regelungen über die Geheimhaltung von Daten zu treffen (Vertraulichkeitsvereinbarungen, siehe auch ORP.1 Organisation). Insbesondere ist festzulegen, dass Daten, die im Rahmen der Wartung extern gespeichert wurden, nach Abschluss der Arbeiten sorgfältig gelöscht werden. Ebenso sind die Pflichten und Kompetenzen des externen Wartungspersonals sorgfältig festzulegen.

Bei der Durchführung externer Wartungsarbeiten muss protokolliert werden, welche IT-Systeme oder Komponenten wann an wen zur Reparatur gegeben wurden, wer dies veranlasst hat, was der Wartungs- bzw. Reparaturauftrag umfasst, zu welchem Zeitpunkt die Reparatur abgeschlossen sein sollte und wann das Gerät wieder zurückgebracht wurde. Um dies nachhalten zu können, ist eine Kennzeichnung der IT-Systeme oder Komponenten erforderlich, aus der zum einem hervorgeht, welcher Organisation diese gehören, und zum anderen eine eindeutige Zuordnung innerhalb der Organisation möglich ist.

Beim Versand oder Transport der zu reparierenden Komponenten sollte darauf geachtet werden, dass Beschädigungen und Diebstahl vorgebeugt wird. Befinden sich auf den IT-Systemen noch sensitive Informationen, müssen sie entsprechend geschützt transportiert werden, also z. B. in verschlossenen Behältnissen oder durch Kuriere. Weiterhin müssen Nachweise über den Versand (Reparaturauftrag, Begleitzettel, Versandscheine) und den Eingang beim Empfänger (Empfangsbestätigung) geführt und archiviert werden.

Bei IT-Systemen, die durch Passwörter geschützt sind, müssen je nach Umfang der Reparaturarbeiten und der Art der Passwortabsicherung, alle oder einige Passwörter entweder bekannt gegeben oder auf festgelegte Einstellungen wie "REPARATUR" gesetzt werden, damit die Wartungstechniker auf die Geräte zugreifen können.

Nach der Rückgabe der IT-Systeme oder Komponenten sind diese auf Vollständigkeit zu überprüfen. Alle Passwörter sind zu ändern. Datenträger sind nach der Rückgabe mittels eines aktuellen Viren-Suchprogramms auf Computer-Viren zu überprüfen. Alle Daten oder Programme, die sich auf dem reparierten Gerät befinden, sind auf Integrität zu überprüfen.

Regelungen für die Fernwartung können OPS.2.4 Fernwartung entnommen werden.

OPS.1.1.2.M13 Absicherung von Fernwartung [IT-Betrieb, Informationssicherheitsbeauftragter (ISB)]

Die Fernwartung von IT-Systemen birgt besondere Sicherheitsrisiken. Bei der Fernwartung ist zu unterscheiden, ob internes oder externes Wartungspersonal auf die IT-Systeme zugreift. Damit Administratoren IT-Benutzern schnell helfen können, ohne dass sie sich zum Aufstellungsort der jeweiligen IT-Systeme begeben müssen, werden bei der IT-Betreuung häufig Fernwartungszugänge genutzt. Aus Sicherheitsgründen ist es sinnvoll, auf externe Fernwartung zu verzichten. Ist dies nicht möglich, so sind zusätzliche Sicherungsmaßnahmen unumgänglich.

Das zu wartende IT-System muss die folgenden Sicherheitsfunktionen realisieren:

- Der Aufbau der Verbindung für eine Fernwartung sollte immer vom lokalen IT-System initiiert werden. Dies kann durch Anruf des zu wartenden IT-Systems bei der Fernwartungsstelle oder über einen automatischen Rückruf (Callback) realisiert werden.
- Der Benutzer des IT-Systems muss dem Fernzugriff explizit zustimmen, z. B. über eine entsprechende Bestätigung am System. Er sollte alle Tätigkeiten während des Fernzugriffs beobachten.
- Das externe Wartungspersonal muss sich zu Beginn der Wartung authentisieren. Werden dabei Passwörter unverschlüsselt übertragen, sollten Einmalpasswörter benutzt werden.
- Die Durchführung einer Fernwartung muss protokolliert werden. Dabei ist zumindest Anfang und Ende der Fernwartung sowie die Beteiligten festzuhalten. Wenn auf dem gewarteten IT-System niemand die Fernzugriffe beobachten kann, müssen alle Tätigkeiten bei der Durchführung der Fernwartung auf dem zu wartenden IT-System protokolliert werden.

Darüber hinaus können am zu wartenden IT-System noch weitere Funktionalitäten implementiert werden:

- Verhängen einer Zeitsperre bei fehlerhaften Zugangsversuchen
- Sperren der Fernwartung im Normalbetrieb und explizite Freigabe für eine genau definierte Zeitspanne
- Einschränkung der Rechte des Wartungspersonals: Das Wartungspersonal sollte nicht die vollen Administrator-Rechte besitzen. Es sollte eine abgestufte Rechteverwaltung realisiert werden. Dabei ist auch eine Aufteilung der Administrationstätigkeiten zu prüfen (siehe OPS.1.1.2.M15 Aufteilung von Administrationstätigkeiten). Das Wartungspersonal sollte nur auf die Daten und Verzeichnisse Zugriff haben, die aktuell von der Wartung betroffen sind.
- Auf dem IT-System sollte für das Wartungspersonal eine eigene Benutzer-Kennung existieren. Es ist sinnvoll, auf externe Fernwartung zu verzichten. Ist dies nicht möglich, so sind zusätzlich zu den oben genannten Sicherheitsmaßnahmen folgende Punkte zu beachten:

- Bei einer Fernwartung über externe Kommunikationsverbindungen müssen die Zugänge und die Verbindungen abgesichert werden. Das Fernwartungspersonal muss sich authentisieren und die übertragenen Daten müssen verschlüsselt werden. Beispielsweise kann die Anbindung per VPN oder exklusiv genutzte Verbindungen realisiert werden.
- Wenn dies technisch möglich ist, sollten alle Tätigkeiten während der Administration von Dritten durch eigene IT-Experten beobachtet werden. Beispielsweise können bei der Fernadministration eines Clients über eine graphische Benutzeroberfläche oft alle Ein- und Ausgaben am zu wartenden IT-System angezeigt und aufgezeichnet werden (siehe OPS.1.1.2.M18 Durchgängige Protokollierung administrativer Tätigkeiten). Auch wenn Fernwartung durch Dritte genutzt wird, weil intern das Know-how oder die Kapazität nicht verfügbar sind, darf das externe Wartungspersonal nicht unbeaufsichtigt gelassen werden. Bei Unklarheiten über die Vorgänge sollte der lokale IT-Experte sofort nachfragen. Es muss jederzeit die Möglichkeit geben, die Fernwartung lokal abzubrechen.
- Werden während der Wartung Daten oder Programme auf dem lokalen IT-System angelegt, so muss dies deutlich erkennbar und nachvollziehbar sein, also z. B. darf dies nur in besonders markierten Verzeichnissen oder unter bestimmten Benutzer-Kennungen erfolgen.
- Alle Remote-Administrationsvorgänge müssen aufgezeichnet werden. Dabei ist zumindest Anfang und Ende der Fernwartung sowie die Beteiligten festzuhalten. Wenn auf dem gewarteten IT-System niemand die Fernzugriffe beobachten kann, müssen alle Tätigkeiten bei der Durchführung der Fernwartung auf dem zu wartenden IT-System protokolliert werden.

Mit externem Wartungspersonal sollten vertragliche Regelungen über die Geheimhaltung von Daten getroffen werden (Vertraulichkeitsvereinbarungen, siehe auch ORP.1 Organisation). Insbesondere ist festzulegen, dass Daten, die im Rahmen der Wartung extern gespeichert wurden, nach Abschluss der Arbeiten sorgfältig gelöscht werden. Ebenso sind die Pflichten und Kompetenzen des externen Wartungspersonals sorgfältig festzulegen.

Weiteres zu diesem Thema findet sich in OPS.2.4 Fernwartung.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

OPS.1.1.2.M14 Sicherheitsüberprüfung von Administratoren (CIA)

Die Möglichkeiten, die Vertrauenswürdigkeit von neuem oder externem Personal überprüfen zu lassen, sind in Deutschland, aber auch in vielen anderen Ländern, rechtlich sehr eingeschränkt. Dazu kommt, dass die Ergebnisse meist wenig aussagekräftig sind, wie z. B. bei polizeilichen Führungszeugnissen. Grundsätzlich sollte aber vor der Übernahme von neuen oder externen Mitarbeitern in Projekte überprüft werden, ob

- diese hinreichende Referenzen haben, z. B. aus anderen, ähnlichen Projekten, und
- der vorgelegte Lebenslauf des Bewerbers aussagekräftig und vollständig ist.

Darüber hinaus kann es sinnvoll sein, sich akademische und berufliche Qualifikationen bestätigen zu lassen, beispielsweise durch Nachfragen an der Universität oder früheren Arbeitgebern oder Kunden. Auch die Identität des Bewerbers sollte verifiziert werden, z. B. durch Vorlage von Ausweispapieren.

Wenn externes Personal intern eingesetzt wird oder im Rahmen von Projekten, Kooperationen oder Outsourcing-Vorhaben auf interne Anwendungen und Daten zugreifen kann, sollten vergleichbare Überprüfungen wie für eigene Mitarbeiter durchgeführt werden. Bei der Vertragsgestaltung mit externen Dienstleistern sollte vertraglich festgehalten werden, welche Seite solche Überprüfungen durchzuführen hat und in welcher Tiefe diese erfolgen.

OPS.1.1.2.M15 Aufteilung von Administrationstätigkeiten (CI)

Viele Betriebssysteme, Anwendungen und IT-Komponenten bieten die Möglichkeit, die Administrationsrolle aufzuteilen und Administrationstätigkeiten an verschiedene Benutzer zu verteilen. Wenn es Administrationsrollen für Spezialaufgaben gibt, sollte davon Gebrauch gemacht werden. Insbesondere, wenn in großen Systemen mehrere Personen mit Administrationsaufgaben betraut werden müssen, kann das Risiko der übergroßen Machtbefugnis der Administratorrollen durch eine entsprechende Aufgabenteilung vermindert werden, so dass Administratoren nicht unkontrolliert unautorisierte oder unbeabsichtigte Veränderungen am System vornehmen können.

Auch wenn Administrationstätigkeiten aufgeteilt werden, legen viele Systeme trotzdem automatisch einen Administrator-Account an, der keinen Beschränkungen unterliegt (je nach System "root", "superuser" oder "Supervisor". Der Zugang hierzu sollte möglichst restriktiv gehandhabt werden. Wenn möglich, sollte er durch eine Mehr-Faktor-Authentisierung geschützt sein.

Bestehen erhöhte Anforderungen an einen Schutz vor Manipulationen, die durch oder unter Mitwirkung von IT-Administratoren vorgenommen werden, so sollten in größeren Institutionen verschiedene Administrationsrollen definiert werden, die jeweils durch unterschiedliche Personen besetzt werden. Die Aufteilung richtet sich dabei am besten nach den Angriffsszenarien, gegen die ein Schutz erreicht werden soll. Denkbar sind z. B. die folgenden Aufteilungen, die auch miteinander kombiniert werden können.

Dabei ist zu beachten, dass eine feinere Aufteilung bedeutet, dass mehr Personal bereitstehen muss, um alle relevanten Tätigkeiten durchgängig abzudecken – auch im Urlaubs- und Krankheitsfall.

Bei knappen Personalressourcen kann die Aufteilung von Administrationstätigkeiten auch auf besonders schutzbedürftige Systeme und Anwendungen begrenzt werden.

OPS.1.1.2.M16 Zugangsbeschränkungen für administrative Zugänge (CIA)

Der Schutz von administrativen Zugängen zu IT-Systemen und Komponenten lässt sich noch deutlich erhöhen, wenn der Zugang nicht nur durch einen Authentisierungsmechanismus für die Administratoren geschützt wird (siehe OPS.1.1.2.M5), sondern zusätzlich auch netzseitig beschränkt wird. Administrative Zugänge und Oberflächen sind dann nur aus einem Netzsegment heraus erreichbar, das abgetrennt ist von den Netzen, in denen das System seine Dienste anbietet.

So können z. B. SSH-Zugänge oder Web-Oberflächen für die Administration an eine separate Netzwerkkarte gebunden werden, die in ein separiertes Administrationsnetz eingebunden ist. Ein Anwender, der das System über eine andere Netzwerkkarte und ein anderes Netz anspricht, kann diese Zugänge dann gar nicht erst aufrufen. Dabei ist zu beachten, dass sich eine Segmentierung des Netzes in verschiedene Schutzzonen dann auch im Administrationsnetz spiegeln muss – sonst besteht die Gefahr, dass ein Angreifer nach der erfolgreichen Übernahme eines Systems das Administrationsnetz missbraucht, um Sicherheitsgateways zu umgehen. Beispiel für den Schutz der administrativen Zugänge durch ein abgesetztes Administrationsnetz

In das Administrationsnetz können dann ausgewählte Client-Systeme eingebunden werden, von denen aus die administrativen Zugänge der Systeme erreicht werden können. Noch besser ist die Einrichtung eines Sprungservers, auf dem sich die IT-Administratoren anmelden müssen, um von dort aus in das Administrationsnetz zu gelangen. So können alle administrativen Zugänge gesteuert, protokolliert und gegebenenfalls aufgezeichnet werden.

Insbesondere bei Firewall- und DMZ-Systemen ist darauf zu achten, dass administrative Oberflächen auf keinen Fall über Außenverbindungen erreichbar sind.

OPS.1.1.2.M17 IT-Administration im Vier-Augen-Prinzip (CI)

Bei besonders kritischen Systemen oder bei bestimmten kritischen Aktivitäten kann es wünschenswert sein, dass die administrativen Tätigkeiten grundsätzlich im Vier-Augen-Prinzip durchgeführt werden. Dabei führt dann jeweils ein Administrator die Arbeiten durch, während ein anderer Administrator zugegen ist und die Tätigkeiten beobachtet.

Diese Anforderung kann durch eine organisatorische Vorgabe (z. B. eine Arbeitsanweisung) umgesetzt werden. Idealerweise wird sie durch technische Maßnahmen unterstützt, z. B. durch die Aufteilung des administrativen Passworts in zwei Hälften, die jeweils nur einem Administrator bekannt sind. Dadurch kann die Anmeldung mit administrativen Rechten nur erfolgen, wenn beide Administratoren zugegen sind.

In einigen Fällen bieten Systeme auch integrierte Funktionen für die Umsetzung eines Vier-Augen-Prinzips, z. B. für die Einrichtung und Freischaltung von Firewallregeln auf einem Sicherheitsgateway.

Die Umsetzung eines Vier-Augen-Prinzips erfordert entsprechend mehr Personal und kann die Verfügbarkeit von Administratoren im Notfall verzögern. Sie ist daher sorgfältig abzuwägen und wird im Regelfall bei sehr hohen Sicherheitsanforderungen umgesetzt (z. B. für die Schlüsselserver von qualifizierten Vertrauensdiensten).

OPS.1.1.2.M18 Durchgängige Protokollierung administrativer Tätigkeiten (CI)

Administrative Tätigkeiten sollten möglichst protokolliert werden. Auf Systemen mit hohen Sicherheitsanforderungen sollten sie durchgängig protokolliert werden.

Dabei sollte nicht nur die Anmeldung am System (siehe OPS.1.1.2.M5 Administrationskennungen), sondern alle vom Administrator abgesetzten Befehle oder aufgerufenen Funktionen protokolliert werden. Weil die Protokollierung dabei vom Administrator nicht abgeschaltet oder umgangen werden können soll, erfolgt sie idealerweise nicht auf dem administrierten System selbst, sondern in einer Umgebung, die nicht unter der Kontrolle der durchführenden Administratoren steht.

Dies kann realisiert werden, in dem der administrative Zugang zu IT-Systemen und Komponenten netzseitig nur über die Nutzung eines Sprungservers möglich ist, auf dem eine vollständige Protokollierung der ausgeführten Tätigkeiten erfolgt. Für dieses Einsatzszenario sind am Markt auch fertige Lösungen verfügbar, die sowohl konsolenbasierte Zugriffe als auch Zugriffe über grafische Oberflächen aufzeichnen können. Für konsolenbasierte Zugriffe existieren auch verschiedene freie Lösungen.

Um den Schutzzweck zu erreichen, dürfen die aufgezeichneten Protokolle von den durchführenden Administratoren selbst nicht verändert oder gelöscht werden können . Die protokollierten Daten sollten in regelmäßigen Abständen durch einen unabhängigen Dritten (z. B. Revisor) ausgewertet werden.

OPS.1.1.2.M19 Berücksichtigung von Hochverfügbarkeitsanforderungen (A)

Bestehen in der zu administrierenden IT-Umgebung Hochverfügbarkeitsanforderungen, so müssen geeignete Konzepte und Maßnahmen realisiert werden, um diese Anforderungen zu erfüllen. Dies erfordert im Regelfall eine übergreifende Herangehensweise. Das BSI hat in seinem Hochverfügbarkeits-Kompendium ("HV-Kompendium") eine geeignete Methodik sowie zahlreiche Hilfestellungen bei der Analyse, Planung und Realisierung von hochverfügbaren IT-Umgebungen zusammengetragen. Das Kompendium ist auf der Webseite des BSI kostenfrei abrufbar und gliedert sich in mehrere Bände und Abschnitte:

Die Hochverfügbarkeitsplanung sollte mit den zugrundeliegenden Methoden, Annahmen und Ergebnissen dokumentiert werden. Die Verantwortung für die Erstellung und Fortschreibung des Hochverfügbarkeitskonzepts muss einer geeigneten Stelle in der Institution übertragen werden, z. B. einem IT-Architekten.

Hochverfügbarkeitsplanung und Sicherheitsmanagement müssen ineinander greifen. So müssen die HV-Anforderungen bei der Schutzbedarfsfeststellung im Informationssicherheitsprozess im Hinblick auf das Schutzziel Verfügbarkeit berücksichtigt werden. Umgekehrt müssen Erkenntnisse aus Sicherheitsvorfällen, die dieses Schutzziel betreffen, zurückfließen in die HV-Planung.

Die Realisierung von Hochverfügbarkeitsanforderungen sollte auch im Rahmen von Audits und Revisionen mit berücksichtigt werden. Dies kann z. B. die Durchführung von Lasttests oder von Tests der vorgesehenen Hochverfügbarkeitsmaßnahmen (z. B. Schwenk von Rechenzentren) umfassen.

3 Weiterführende Informationen

3.1 Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Ordnungsgemäße IT-Administration" finden sich unter anderem in folgenden Veröffentlichungen:

[27001A12] ISO/IEC 27001:2013

Information technology - Security techniques - Information security management systems - Requirements, insbesondere Annex A, A.12 Operations security, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/SC 27, Oktober 2013

[HVK] Hochverfügbarkeitskompendium

Bundesamt für Sicherheit in der Informationstechnik (BSI), 2013, https://www.bsi.bund.de/DE/Themen/Sicherheitsberatung/Hochverfuegbarkeit/HVKompendium/hvkompendium_node.html , zuletzt abgerufen am 24.08.2018

[ISFSY] The Standard of Good Practice for Information Security

Area SY System Management, Information Security Forum (ISF), June 2018

[NIST80053] Security and Privacy Controls for Federal Information Systems and Organizations

NIST Special Publication 800-53, Revision 4, April 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf , zuletzt abgerufen am 30.08.2018

Umsetzungshinweise zum Baustein OPS.1.1.3 Patch- und Änderungsmanagement

1 Beschreibung

1.1 Einleitung

Aufgabe des Änderungsmanagements ist es, verändernde Eingriffe in Anwendungen, Infrastruktur, Dokumentationen, Prozesse und Verfahren steuer- und kontrollierbar zu gestalten. Ein fehlendes oder vernachlässigtes Patch- und Änderungsmanagement führt schnell zu Sicherheitslücken in den einzelnen Komponenten und damit zu möglichen Angriffspunkten.

Vor allem im Bereich der Informationstechnologie stehen viele Behörden und Unternehmen aufgrund der immer schneller fortschreitenden Entwicklung und der steigenden Anforderungen der Benutzer vor der Herausforderung, die notwendigen Neuerungen an den Komponenten ihrer Systemlandschaft korrekt und zeitnah zu übernehmen. Erfahrungen in Behörden und Unternehmen zeigen, dass Sicherheitslücken oder Störungen häufig auf fehlerhafte oder nicht erfolgte Änderungen zurückzuführen sind.

In diesem Dokument wird aufgezeigt, wie ein funktionierendes Patch- und Änderungsmanagement in einer Institution aufgebaut werden kann. Auch wird beschrieben, wie der entsprechende Prozess kontrolliert und optimiert werden kann, damit Störungen im Betrieb vermieden sowie Sicherheitslücken minimiert und zeitnah beseitigt werden können. Die Beschreibungen konzentrieren sich dabei auf den IT-Betrieb, können aber auch sinngemäß in anderen Geschäftsprozessen umgesetzt werden. Der Begriff Änderungsmanagement bezeichnet in diesem Baustein die Aufgabe, Änderungen zu planen und zu steuern. Das Patchmanagement stellt einen Teilbereich des Änderungsmanagements dar, der auf die Aktualisierung von Software zielt und in jedem Fall anzuwenden ist.

1.2 Lebenszyklus

Um ein effektives System einzurichten, mit dem Änderungen behandelt werden können, sind eine Reihe von Schritten zu durchlaufen.

Planung und Konzeption

Über das Patch- und Änderungsmanagement sollten alle Änderungen an Hard- und Softwareständen sowie deren Konfigurationen gesteuert und kontrolliert werden. Um alle Änderungen erfassen und bewerten zu können, sollten alle innerhalb des Patch- und Änderungsmanagements erfassten IT-Systeme diesem unterstellt sein (siehe OPS.1.1.3.M2 *Festlegung der Verantwortlichkeiten für das Änderungsmanagement*). Änderungen an der Konfiguration und dem Zustand der Systeme sind damit nur noch über das Änderungsmanagement möglich. Das erfordert von der Leitung der Institution, die entsprechende Verantwortung zu delegieren. Die organisatorische Umsetzung des Patch- und Änderungsmanagements stellt eine Querschnittsfunktion durch verschiedene Abteilungen einer Institution dar. Insbesondere sind der IT-Betrieb, das Informationssicherheitsmanagement und die Fachabteilungen einzubinden.

Ein einzelner Änderungsvorgang beginnt mit einer Änderungsanforderung. Diese sollte zunächst erfasst und durch den Änderungsmanager kontrolliert werden. Zu dieser Änderung sollten Relevanz, Dringlichkeit, geplante Durchführung (Termin, Ablauf) sowie mögliche Risiken und Probleme zusammengestellt und erfasst werden (siehe OPS.1.1.3.M4 *Planung des Änderungsmanagementprozesses* und OPS.1.1.3.M5 *Umgang mit Änderungsanforderungen*).

Das Patch- und Änderungsmanagement kann durch technische Hilfsmittel, beispielsweise zum automatischen Verteilen von Software, sinnvoll unterstützt werden. Werden für die Umsetzung des Patch- und Änderungsmanagements spezielle Tools eingesetzt, so muss sichergestellt werden, dass ein Konzept für deren Einsatz erstellt wird (siehe OPS.1.1.3.M8 *Sicherer Einsatz von Änderungsmanagement-Werkzeugen*).

Beschaffung

Es gibt unterschiedliche Produkte, die den Patch- und Änderungsmanagementprozess unterstützen. Um aus diesen Produkten eine geeignete Auswahl zu treffen, müssen vor der Beschaffung die Anforderungen an diese Werkzeuge, zum Beispiel, welche Plattformen unterstützt werden müssen, festgelegt werden (siehe OPS.1.1.3.M8 *Sicherer Einsatz von Änderungsmanagement-Werkzeugen*).

Umsetzung

Bei der Umsetzung sollten alle vom Patch- und Änderungsmanagement betreuten IT-Systeme diesem einzeln oder gruppenweise unterstellt werden. Des Weiteren müssen Änderungen an diesen Systemen an einer zentralen Stelle dokumentiert werden (siehe OPS.1.1.3.M11 *Kontinuierliche Dokumentation der Informationsverarbeitung*).

Betrieb

Je nach Größe und Komplexität eines Patches oder einer durchzuführenden Änderung wird empfohlen, in einem Durchführungsplan Tests, Kontroll- und Abbruchpunkte sowie Prioritäten für die Verteilung zu definieren. Dabei muss sichergestellt werden, dass das angestrebte Sicherheitsniveau während und nach der Änderung erhalten bleibt. Die Freigabe und Durchführung von Änderungen sollten abgestimmt und dabei Ressourcen und Interessen von Fachbereichen und IT-Betrieb berücksichtigt werden (siehe OPS.1.1.3.M7 *Integration des Änderungsmanagements in die Geschäftsprozesse* und OPS.1.1.3.M6 *Abstimmung von Änderungsanforderungen*).

Zur Qualitätssicherung und um Fehler erkennen beziehungsweise zukünftigen Fehlern vorbeugen zu können, sollte jeder Patch und jede Änderung, nachdem sie aufgespielt wurde, bewertet werden (siehe OPS.1.1.3.M13 *Erfolgsmessung von Änderungsanforderungen*).

Änderungen, insbesondere Softwareaktualisierungen, können manuell, aber auch mithilfe von geeigneten Tools durchgeführt werden. Bei Einsatz dieser Werkzeuge ist darauf zu achten, dass diese gegen Missbrauch besonders gesichert sind, und nicht zu einer Gefährdung der Gesamtsicherheit führen, da sie häufig mit Systemadministrator-Berechtigungen arbeiten. Die Tools bieten die Möglichkeit, an vielen Systemen gleichzeitig Änderungen durchzuführen. Dadurch multiplizieren sich aber auch die Auswirkungen von Fehlern, sodass sehr sorgfältig getestet werden sollte, bevor die Änderung durchgeführt wird (siehe OPS.1.1.3.M12 *Skalierbarkeit beim Änderungsmanagement*). Zu berücksichtigen ist ebenfalls, dass umzustellende Systeme zeitweise oder permanent abgeschaltet bzw. nicht erreichbar sein könnten. Dies betrifft vor allem mobile Geräte wie zum Beispiel Laptops und Smartphones (siehe OPS.1.1.3.M14 *Synchronisierung innerhalb des Änderungsmanagements*). Außerdem muss während des gesamten Patch- und Änderungsmanagementprozesses die Integrität und Authentizität der verwendeten Software technisch sichergestellt werden (OPS.1.1.3.M10 *Sicherstellung der Integrität und Authentizität von Softwarepaketen*).

Die Autoupdate-Mechanismen verwendeter Software müssen, unabhängig von ihrem Einsatzgrad innerhalb des Patch- und Änderungsprozesses, betrachtet werden (siehe OPS.1.1.3.M3 *Konfiguration von Autoupdate-Mechanismen*).

Notfallvorsorge

Für die Notfallvorsorge müssen die einzelnen Notfallpläne der Anwendungen und IT-Systeme, die vom Patch- und Änderungsmanagement verwaltet werden, berücksichtigt werden (siehe DER.4 *Notfallmanagement*). Da das Patch- und Änderungsmanagement zur technischen Umsetzung von Sicherheit in der Institution beiträgt, sollten geeignete technische Redundanz- und Ersatzsysteme bereitgestellt werden, um einem nicht kompensierbaren Ausfall entgegenzuwirken. Des Weiteren sind Vertreterregelungen von besonderer Bedeutung, um den Entscheidungs- und Freigabeprozess aufrecht zu erhalten.

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Patch- und Änderungsmanagement" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

OPS.1.1.3.M1 Konzept für das Patch- und Änderungsmanagement [Administrator, Fachverantwortliche]

Bei der Komplexität heutiger IT-Systeme können bereits kleine Änderungen an laufenden Systemen zu Sicherheitsproblemen führen, z. B. durch unerwartetes Systemverhalten oder Systemausfälle.

In Bezug auf Informationssicherheit ist es Aufgabe des Änderungsmanagements, neue Sicherheitsanforderungen zu erkennen, die sich aus Änderungen an IT-Systemen ergeben. Sind signifikante Hardware- oder Software-Änderungen an einem IT-System geplant, so ist zu untersuchen, wie sich diese auf die Sicherheit des Gesamtsystems auswirken. Änderungen an einem IT-System dürfen nicht dazu führen, dass einzelne Sicherheitsmaßnahmen ineffizienter werden und so die Gesamtsicherheit gefährdet ist.

Daher sollte es Richtlinien für die Durchführung von Änderungen an IT-Komponenten, Software oder Konfigurationsdaten geben. Alle Änderungen an IT-Komponenten, Software oder Konfigurationsdaten sollten geplant, getestet, genehmigt und dokumentiert werden. Es ist dafür zu sorgen, dass auf alle sicherheitsrelevanten Änderungen angemessen reagiert wird. Dazu gehören zum Beispiel:

- Änderungen an IT-Systemen (neue Applikationen, neue Hardware, neue Netzverbindungen, Modifikationen an der eingesetzten Software, Einspielen von Sicherheitspatches, Aufrüstung der Hardware usw.),
- Änderungen in der Aufgabenstellung oder in der Wichtigkeit der Aufgabe für die Institution,
- Änderungen in der Benutzerstruktur (neue, etwa externe oder anonyme, Benutzergruppen),
- räumliche Änderungen, z. B. nach einem Umzug.

Bevor Änderungen genehmigt und umgesetzt werden, ist zu prüfen und zu testen, ob das Sicherheitsniveau während und nach der Änderung erhalten bleibt. Wenn Risiken, insbesondere für die Verfügbarkeit, nicht auszuschließen sind, muss eine Rückfall-Lösung geplant werden, die auch Kriterien vorgibt, wann sie angewendet werden soll.

Alle Änderungen und die dazugehörigen Entscheidungsgrundlagen sind zu dokumentieren. Das gilt sowohl in der Betriebs- als auch in einer Testumgebung.

Wichtig für das Patch- und Änderungsmanagement ist auch ein Berechtigungskonzept:

- Nur diejenigen, die Änderungen durchführen dürfen, sollten Zugriffsberechtigungen auf die dafür relevanten Systembereiche haben.
- Es sollte Mechanismen geben, die sicherstellen, dass alle wesentlichen Änderungen vorher abgestimmt wurden.

Hinweis: Bei der Durchführung von Änderungen sollte immer beachtet werden, dass Änderungen eines IT-Systems oder seiner Einsatzbedingungen

- Änderungen in der Umsetzung einzelner Sicherheitsmaßnahmen,
- die Erstellung eines neuen Sicherheitskonzepts oder sogar
- die Überarbeitung der organisationsweiten Leitlinie zur Informationssicherheit

erforderlich machen können. Bei größeren Änderungen sollte daher das Informationssicherheitsmanagement einbezogen werden.

OPS.1.1.3.M2 Festlegung der Verantwortlichkeiten [Leiter IT]

Beim Aufbau des Patch- und Änderungsmanagements müssen eine Reihe von Verantwortlichkeiten geregelt werden. Dabei ist sicherzustellen, dass für jeden Aufgaben- und Organisationsbereich exakt definiert ist, welche Verantwortlichkeiten im Patch- und Änderungsprozess ein Mitarbeiter besitzt und wie die Koordination zwischen den einzelnen Bereichen abzulaufen hat.

Teilweise ist es üblich, dass die Mitarbeiter verschiedener Bereiche einer Institution unterschiedliche Verantwortlichkeiten bezüglich der Durchführung von Änderungen besitzen. So kann beispielsweise ein Bereich für Betriebssysteme zuständig sein und ein anderer Bereich die darauf installierten Dienste (z. B. E-Mail-Server, Fachanwendung etc.) betreuen. Das kann dann dazu führen, dass unterschiedliche Bereiche beispielsweise für das Patchen eines Gesamtsystems verantwortlich sein können. In solchen Fällen ist es besonders wichtig, die Zuständigkeiten genau festzulegen.

Die so aufgeteilten Verantwortlichkeiten sollten sich auch im Berechtigungskonzept wieder finden.

Für die effiziente und effektive Koordination und Bewertung der Änderungen sollte in der Institution ein dedizierter Änderungsmanager (Change Manager) benannt sein. Er filtert, akzeptiert und klassifiziert sämtliche Änderungsanforderungen. Er ist zudem dafür verantwortlich, die notwendigen Änderungen zu autorisieren sowie sie zu planen, zu koordinieren und durchzuführen.

Es ist unbedingt erforderlich, dass Änderungen koordiniert ablaufen. Kein Mitarbeiter darf Änderungen auf eigene Faust durchführen. Auch alle Mitarbeiter des IT-Betriebs müssen relevante Änderungen grundsätzlich mit dem Änderungsmanagement absprechen. Damit wird sichergestellt, dass etwaige Änderungen sich nicht gegenseitig behindern oder gar zu einem Systemausfall führen.

Bei einer Institution mindestens mittlerer Größe oder mit komplexen IT-Infrastrukturen sollte der Änderungsmanager bei seiner Arbeit durch ein Change Advisory Board (CAB) unterstützt werden. Es hat sich bewährt, neben den mit der technischen Umsetzung von Änderungsaufgaben betrauten Personen auch eine Person aus jeder Fachabteilung als Mitglied in das CAB zu berufen. Das CAB wird regelmäßig zu bestimmten Zeiten einberufen, um Änderungen zu beurteilen und dem Änderungsmanager zu helfen, diese einzuschätzen, zu priorisieren und zu autorisieren. In der Regel werden dem CAB nur schwerwiegende Änderungen vorgelegt. Zu diesem Zweck kann das CAB hinsichtlich seiner Mitglieder unterschiedlich zusammengesetzt sein. Das komplette CAB könnte beispielsweise alle drei Monate zusammenkommen und über kritische Änderungsanforderungen diskutieren.

Für unkritische regelmäßige Änderungen können die Absprachen direkt zwischen dem Änderungsmanager und den verantwortlichen Administratoren bzw. dem Test-Team erfolgen.

Damit das CAB seine Aufgaben angemessen erfüllen kann, müssen seine Mitglieder in der Lage sein, zu beurteilen, wie sich Änderungen sowohl technisch als auch aus Sicht der Geschäftsziele und -prozesse auswirken können.

OPS.1.1.3.M3 Konfiguration von Autoupdate-Mechanismen [Administrator]

Viele Produkte verfügen über automatische Update-Mechanismen (Autoupdate), die die Anwender darüber informieren, wenn Patches oder Updates vorhanden sind. Häufig bieten diese auch die Option, die Updates sofort über das Internet herunterzuladen und zu installieren. In der Regel enthalten heute alle Betriebssysteme und verfügbaren Standardsoftwarepakete solche Mechanismen. Die Funktionsweise des Update-Mechanismus ist je nach Version, Installationsmodus und Hersteller unterschiedlich ausgeprägt.

Üblicherweise suchen IT-Produkte mit Autoupdate bei jedem Start des Systems bzw. der Software oder zeitlich gesteuert auf einem öffentlichen Updateserver nach neuen Versionen oder Softwarepaketen. Die Produkte bieten verschiedene Möglichkeiten, den Autoupdate-Mechanismus zu konfigurieren. Wenn neue IT-Komponenten in Betrieb genommen werden, sollte immer auch überprüft werden, ob und welche Update-Mechanismen diese haben und wie diese konfiguriert werden können. Dabei sollte auch kontrolliert werden, welche Daten vom Autoupdate-Mechanismus zum Hersteller übertragen werden. Es sollte zunächst grundsätzlich geklärt werden, wie mit diesen Mechanismen umgegangen wird. Danach sollte festgelegt werden, wie die Update-Funktionen konkret in den verschiedenen Produkten konfiguriert werden. Die folgenden Abschnitte geben einen Überblick über die verschiedenen Varianten dieser Mechanismen.

Nicht in jeder Software lässt sich die Update-Funktion vollständig deaktivieren. Falls die Institution die unkontrollierte Kommunikation von IT-Komponenten mit der Außenwelt unterbinden will, müssen hierfür Paketfilter eingesetzt werden.

Wird keine Abfrage eines öffentlichen Update-Servers gewünscht, lassen sich viele Softwareprodukte auf andere Internet-Adressen als die des Herstellers, beispielsweise interne, umlenken.

Einige Hersteller bieten Software für den Eigenbetrieb von Update-Servern oder Update-Spiegelservern an, dabei wird der Update-Server in der Institution lokal installiert (z. B. Windows Server Update Services WSUS). Der Update-Server kommuniziert dann direkt mit dem Hersteller und lädt die gewünschten Aktualisierungen. Der Vorteil dieser Lösung ist, dass die von der Aktualisierung betroffenen IT-Systeme einer Institution nicht selber mit dem Update-Server des Herstellers kommunizieren müssen, sondern nur mit dem lokal installierten System. Dadurch kann der Datenverkehr nach außen auf ein Mindestmaß reduziert werden. Bei vielen Produkten für Update-Server lassen sich die gewünschten Einstellungen komfortabel über eine grafische Benutzeroberfläche (GUI) vornehmen. Allerdings gibt es auch Produkte, bei denen die notwendigen Einstellungen, um lokale Update-Server zu verwenden oder die Abfrage von einem öffentlichen Update-Server zu unterbinden, verborgen oder nur per Paketfilter bzw. Firewall zu unterbinden sind.

Falls öffentliche Update-Server genutzt werden sollen, so ist zunächst die Authentizität des Update-Servers zu prüfen (siehe OPS.1.1.3.M10 *Sicherstellung der Integrität und Authentizität von Softwarepaketen*). Außerdem sollte untersucht werden, ob sich Update-Abfrageaktionen mithilfe von Zeitintervallen oder Ereignissen einstellen lassen. Die Einstellungen müssen dann entsprechend der festgelegten Änderungsstrategie vorgenommen werden.

Es sollte geprüft werden, wie die Kommunikation mit Update-Servern auf das geringst mögliche Maß beschränkt werden kann. Außerdem muss entschieden werden, ob die direkte Kommunikation mit dem Hersteller als einzige Alternative oder parallel zur internen Kommunikation (Parallelkonfiguration) betrieben werden soll.

Eine Parallelkonfiguration ist häufig sinnvoll für mobile Nutzer, die nicht immer innerhalb des Behörden- oder Unternehmensnetzes kommunizieren. Bei mobilen IT-Systemen kann es beispielsweise wichtiger sein, unterwegs einen aktuellen Patch einzuspielen, wenn dieser eine gefährliche Sicherheitslücke schließt, als auf die Freigabe vom Änderungsmanagement zu warten. Stattdessen kann der Änderungsmanager aber auch festlegen, dass sämtliche Software-Änderungen ausschließlich durch die interne freigegebene Softwareverteilung erfolgen.

Bei Autoupdate-Mechanismen ist auch noch zu beachten, ob die Änderungen vom Hersteller nur auf ein internes IT-System geladen werden und die Installation danach dem Benutzer überlassen wird, oder ob diese, nachdem sie heruntergeladen sind, sofort automatisch installiert werden.

Außerdem muss festgelegt werden, wie mit eventuell benötigten Neustarts von IT-Systemen nach der Installation von Änderungen umgegangen wird, also ob diese direkt erfolgen oder z. B. erst, wenn das System das nächste Mal heruntergefahren wird.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Patch- und Änderungsmanagement".

OPS.1.1.3.M4 Planung des Änderungsmanagementprozesses [Änderungsmanager]

Jede Institution sollte für das Änderungsmanagement einen klar definierten Prozess einrichten und die Zuständigkeiten für die verschiedenen Aufgaben regeln (siehe OPS.1.1.3.M2 *Festlegung der Verantwortlichkeiten*). Alle Änderungen von Hard- und Softwareständen sowie Konfigurationen sollten über den Prozess des Patch- und Änderungsmanagements gesteuert und kontrolliert werden. Um alle Änderungen erfassen und bewerten zu können, sollten alle vom Änderungsmanagement betreuten IT-Systeme dem Änderungsmanager unterstellt sein. Änderungen an Konfiguration und Zustand der Systeme sollten damit nur noch über das Änderungsmanagement möglich sein.

Der Änderungsmanagementprozess kann, angelehnt an die IT Infrastructure Library (ITIL), wie folgt schematisch dargestellt werden:

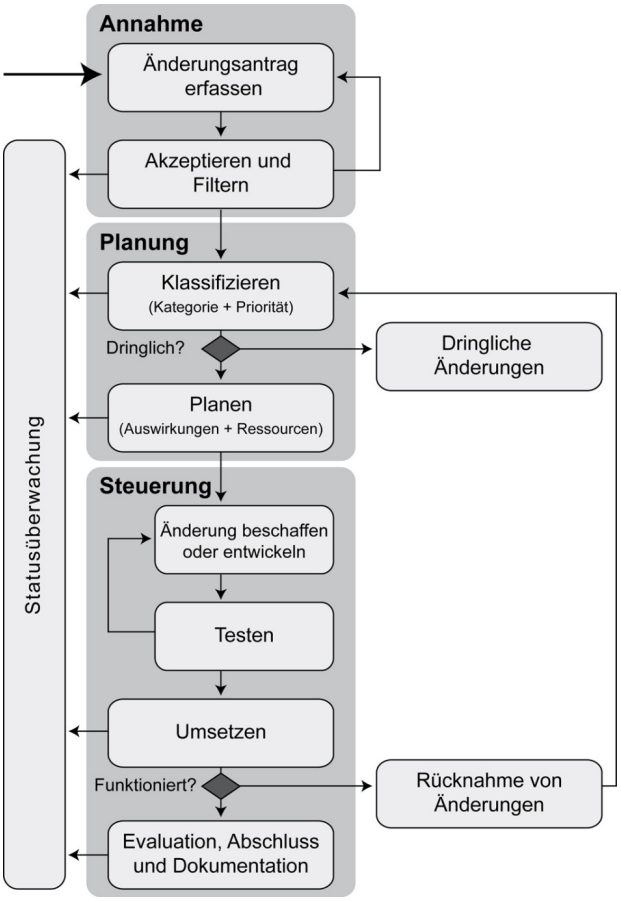


Abbildung: Überblick über den Patch- und Änderungsmanagementprozess

Koordination

Wenn eine Änderungsanforderung (Request for Change, RfC) (siehe OPS.1.1.3.M5 *Umgang mit Änderungsanforderungen*) eingereicht und akzeptiert wurde, muss sie zunächst klassifiziert, also kategorisiert und priorisiert werden, bevor mit der eigentlichen Umsetzungsplanung und -koordination begonnen wird. Im Anschluss sollten folgende Punkte berücksichtigt werden, bevor die Änderung eingespielt wird.

- Beschaffung oder Entwicklung der Änderungen
  Viele Hersteller bieten an, die nötigen Informationen über neue Hard- oder Software oder über aufgetretene Fehler und deren Behebung im Abonnement per E-Mail zu erhalten.
  Aktualisierungen und Patches werden in der Regel auf Internet-Servern zum Download bereitgestellt. Teilweise sind diese Quellen nur in Verbindung mit gültiger Registrierung oder mit Support-Verträgen zugänglich. Häufig bietet die installierte Software oder das installierte Betriebssystem dem Benutzer die Möglichkeit, Software-Änderungen direkt mittels der jeweiligen Anwendung oder dem jeweiligen System zu laden.
  Einige Hersteller stellen ihren Kunden spezielle Applikationen zur Verfügung, um die Produkte zu verwalten und zu aktualisieren. Zusätzlich gibt es auch immer mehr Anwendungen, die, wenn der Benutzer und die Sicherheitseinstellungen es zulassen, selbsttätig über das Internet bei ihren Herstellern nach Aktualisierungen suchen und den Anwender informieren. Aus Sicherheitssicht gibt es jedoch auch Nachteile, wenn Änderungen automatisiert eingespielt werden. So können fehlerhafte Updates, die automatisch eingespielt werden, zu Ausfällen und Fehlfunktionen führen. Daher sollte genau überlegt werden, ob solche Mechanismen in Anspruch genommen werden sollen.
  Eine interne Softwareentwicklung könnte eine weitere Möglichkeit sein, Software-Änderungen zu beziehen, falls aufgetretene Sicherheitslücken oder andere Anforderungen diese erforderlich machen. Allerdings muss dafür nicht nur das nötige Fachwissen vorhanden sein. Auch die Schnittstellen oder der Quellcode müssen offen liegen.
- Testen
  Nachdem eine Änderung eingespielt wurde, muss die Funktionalität der Systeme durch einen Test ermittelt werden. Dafür ist bei jeder Änderung, wenn möglich, eine repräsentative Auswahl an typischen Anwendungsszenarien mit der Fachabteilung festzulegen und zu testen. Die Ergebnisse sind zu dokumentieren und mit den erwarteten Ergebnissen zu vergleichen, um eventuelle Probleme festzustellen. Außerdem müssen alle Protokolldateien, die während des Tests angelegt werden, auf Hinweise von Fehlfunktionen untersucht werden.
- Integration in die Softwareverteilung, Test der Integration
  Oft müssen spezifische Paket- oder Dateiformate, in denen die Hersteller ihre Aktualisierungen zur Verfügung stellen, angepasst werden, damit diese in einem System zur automatischen Softwareverteilung benutzt werden können. Das gilt insbesondere dann, wenn während oder nach der Installation noch aktive Komponenten, wie beispielsweise Shell-Skripte ausgeführt werden müssen. Diese Anpassungen sind auf einem Testsystem auf ihre Wirksamkeit zu prüfen, bevor die Änderungen verteilt werden.

Umsetzung

Die vom Änderungsmanager bestimmten Mitarbeiter werden beauftragt, die Änderung umzusetzen. Das Änderungsmanagement überwacht dies. Bei Änderungen, die nur ungenügend getestet werden können, ist es in manchen Fällen sinnvoll, diese zunächst nur bei einer kleinen Benutzergruppe einzuspielen. Danach werden die Ergebnisse evaluiert, bevor die Änderung auf allen Systemen umgesetzt wird. Ist das aufgrund der Gegebenheiten nicht möglich oder sinnvoll, beispielsweise weil vergleichbare Änderungen schon häufig ohne Probleme durchgeführt wurden, oder weil miteinander inkompatible Softwarestände eine Teil-Verteilung unmöglich machen, kann auch eine Komplett-Verteilung durchgeführt werden.

Evaluation

Durchgeführte Änderungen sollten anschließend evaluiert werden. Danach wird das Ergebnis vom Änderungsmanagement bzw. vom CAB (Change Advisory Board) anhand der folgenden Aspekte bewertet:

- Hat die Änderung bzw. der Patch das angestrebte Ziel erreicht?
- Sind die Auftraggeber und die Benutzer mit dem Ergebnis zufrieden?
- Sind Seiteneffekte (zum Beispiel Störungen bei nicht von der Änderung betroffenen Anwendungen) aufgetreten?
- Wurden die veranschlagten Kosten, der geplante Aufwand und der Zeitplan eingehalten?

Wurde die Änderung erfolgreich durchgeführt, kann die Änderungsanforderung (Request for Change) bzw. der Änderungsdatensatz geschlossen werden. Ist die Änderung fehlgeschlagen, muss entschieden werden, ob die durchgeführten Änderungen angepasst werden müssen. In machen Fällen empfiehlt es sich, die Änderung rückgängig zu machen und eine neue oder abgeänderte Änderungsanforderung auszuarbeiten. Bei einer fehlgeschlagenen Änderung kann es auch sinnvoll sein, die Ursachen zu untersuchen und davon ausgehend IT-Systeme oder Prozesse anzupassen. So können ähnliche Probleme zukünftig vermieden werden.

Je nach Art und Umfang kann es sinnvoll sein, die Änderung sofort zu evaluieren. Andererseits kann es auch vorteilhaft sein, einige Tage oder Wochen abzuwarten, bis abzusehen ist, wie sich die Änderung auswirkt und ob das Ziel erreicht wurde. Durchgeführte Änderungen sind erst dann erfolgreich abgeschlossen, wenn sie positiv evaluiert und dokumentiert wurden. Damit dies nicht vergessen wird, sollte sich der Änderungsmanager über eine automatisierte Wiedervorlage daran erinnern lassen.

Rücknahme von Änderungen

Ob es notwendig ist, Hard- oder Software-Änderungen zurückzuziehen, ergibt sich direkt aus der Evaluation. Waren die Änderungen nicht erfolgreich oder hat sich die Situation sogar verschlechtert, sollten sie zurückgenommen werden, wenn es technisch möglich und wirtschaftlich vertretbar ist.

Das kann häufig durch die benutzte Patch- und Änderungsmanagementsoftware technisch unterstützt werden. Falls nicht, müssen die Änderungen manuell rückgängig gemacht werden.

Abschluss und Dokumentation

Es empfiehlt sich, alle Änderungsanforderungen, Hard- und Software-Änderungen, Testdurchführungen und -ergebnisse in einer Datenbank zu dokumentieren, unabhängig davon, ob sie erfolgreich waren oder nicht, (siehe OPS.1.1.3.M11 *Kontinuierliche Dokumentation der Informationsverarbeitung*).

In vielen Institutionen ist es inzwischen Routine, Betriebssysteme und Anwendungen regelmäßig mit den verfügbaren Software-Updates zur Behebung von Schwachstellen und dem Schutz vor Schadsoftware zu versorgen. Oft wird jedoch vergessen, dass dieses Verfahren auch für Hardware notwendig ist. In vielen IT-Geräten werden kompakte Betriebssysteme eingesetzt, die oft auf die jeweilige Hardware zugeschnitten sind. Dazu gehören beispielsweise Router, Switches, Netzdrucker und Smartphones. Daher muss sichergestellt sein, dass auch solche Geräte ins Patch- und Änderungsmanagement einbezogen und mit sicherheitsrelevanten Updates versorgt werden.

OPS.1.1.3.M5 Umgang mit Änderungsanforderungen [Änderungsmanager]

Die Anträge für Änderungen sollten nach einem festgelegten Ablauf eingereicht und bearbeitet werden.

Änderungsanforderungen einreichen und erfassen

Zunächst müssen alle Änderungsanforderungen (Requests for Change, RfCs) erfasst werden. Damit alle notwendigen Informationen vorliegen, empfiehlt es sich, den Antragstellern ein Formular zur Verfügung zu stellen (siehe Muster einer Änderungsanforderung aus den Hilfsmitteln zum IT-Grundschutz).

Dieser Antrag dient auch dazu, die Änderung abzustimmen (siehe auch OPS.1.1.3.M6 Abstimmung von Änderungsanforderungen). Wenn beispielsweise eine Änderung beantragt wurde, um ein bestehendes Problem zu lösen, sollte auch eine entsprechende Referenz auf das Problem, meist eine Erfassungsnummer in einer Datenbank, mit dokumentiert werden.

Nicht jeder Änderungsantrag wird innerhalb des Änderungsprozesses als normale Änderung behandelt. Einige routinemäßige Änderungen, die klar umschrieben sind, standardisiert durchgeführt werden und dennoch eine Änderung betreffen, können wie eine Serviceanfrage behandelt werden. Eine Serviceanfrage wäre zum Beispiel, ein Passwort zurückzusetzen und, bezogen auf das Änderungsmanagement, ein Login-Banner eines Dienstes zu verändern (der Text, mit dem sich der Dienst bei einem Verbindungsaufbau über die Netzschnittstelle meldet).

Änderungsanforderungen filtern und akzeptieren

Nachdem eine Änderungsanforderung erfasst wurde, wird sie durch den Änderungsmanager (Change Manager) kontrolliert. Dabei sollen nicht durchführbare, unnötige oder doppelte Änderungsanforderungen ermittelt werden. Solche Anträge sollten mit einer Begründung abgelehnt werden. So ist es für den Antragsteller möglich, seine Änderungsanforderung zu überdenken und umzuformulieren.

Wenn eine Änderungsanforderung akzeptiert wurde, werden die Informationen in einen Änderungsdatensatz aufgenommen, um die Änderung durchzuführen. Der Datensatz kann in einem Software-Werkzeug, auf Papier oder auch in einer selbst erstellten Datenbank erfasst werden. Im weiteren Verlauf werden dem Änderungsdatensatz noch die nachstehenden Informationen hinzugefügt:

- ermittelte Priorität und Kategorie,
- Beurteilung der Auswirkungen und erforderliche Ressourcen,
- Empfehlungen des Änderungsmanagers bzw. des Änderungsberatungsausschusses (Change Advisory Board, CAB),
- Datum und Uhrzeit der Autorisierung,
- geplantes Datum für die Umsetzung der Änderung,
- aktuelles Datum und aktuelle Uhrzeit der Änderung,Datum der Auswertung,
- Begründung für eine eventuelle Ablehnung des Vorschlags bzw. des Antrags und
- Ablaufplan und Auswertungsdaten.

- Testergebnisse und aufgetretene Probleme,

Änderungsanforderungen klassifizieren (Priorität und Kategorie)

Nachdem eine Änderungsanforderung akzeptiert worden ist, muss sie priorisiert und kategorisiert werden:

- Die Priorität beschreibt, wie wichtig eine Änderung ist und leitet sich von der Dringlichkeit und den Auswirkungen ab. Wenn ein Fehler korrigiert werden soll, der schon einmal im Rahmen des Änderungsmanagements eingestuft worden ist, wird die Priorität unter Umständen bereits mit übergeben. Dabei sollte sie jedoch immer noch einmal vom Änderungsmanager überprüft und falls erforderlich korrigiert werden. Gleiches gilt für Sicherheitspatches oder Updates, die von der Informationssicherheit beantragt werden. Die endgültige Priorität wird jedoch innerhalb des Änderungsmanagements unter Berücksichtigung anderer gerade anstehender Änderungsanforderungen festgelegt.
- Die Kategorie bestimmt der Änderungsmanager. Grundlage sind dabei die zu erwartenden Auswirkungen und die benötigten Ressourcen. höchste Priorität:
- normale Priorität:
  Eine Änderung mit normaler Priorität hat keine besondere Dringlichkeit oder größere Auswirkung, darf aber nicht auf einen späteren Zeitpunkt verschoben werden. Im CAB erhält diese Änderung bei der Zuteilung von Ressourcen normale Priorität.
- niedrige Priorität:
  Eine Änderung mit niedriger Priorität ist erwünscht, hat jedoch Zeit, bis sich eine passende Gelegenheit ergibt (z. B. eine Folgeversion oder eine geplante Wartung).

Die aus Priorität und Kategorie zusammengesetzte Klassifizierung legt fest, wie die Änderungsanforderung weiter bearbeitet wird und beschreibt somit, wie bedeutend die geplante Änderung ist.

Prioritäten werden vom Änderungsmanager für eine Änderung vergeben und sind in unterschiedliche Stufen eingeteilt, wobei das Sicherheitsmanagement ein Einspruchsrecht gegen zu niedrige bzw. falsche Priorisierung erhalten sollte. Es können beispielsweise die folgenden Prioritätsstufen vom Änderungsmanagement vergeben werden:

- hohe Priorität:
  Diese Priorität beschreibt z. B. eine Änderung aufgrund einer schwerwiegenden Störung oder hängt mit anderen dringenden Aktivitäten zusammen. Diese Änderung erhält bei der nächsten Sitzung des CAB oberste Priorität bei der Zuordnung von Ressourcen für Test- und Durchführung.

Kategorien werden in der Regel vom Änderungsmanagement zugewiesen, wobei auch hier das Sicherheitsmanagement ein Einspruchsrecht gegen eine zu niedrige Kategorisierung erhalten sollte. Mithilfe von Kategorien soll einschätzbar sein, wie sich die Änderung auswirkt und wie die Institution durch den Änderungsprozess belastet wird. Beispielsweise können nachstehende Kategorien vergeben werden:

- geringfügige Folgen:
  Eine Änderung dieser Kategorie erfordert wenig Aufwand. Der Änderungsmanager kann diese Art von Änderungen genehmigen, ohne dass er sie dem CAB vorlegen muss.
- erhebliche Folgen:
  In diese Kategorie fallen Änderungen, die einen erheblichen Aufwand erfordern und sich weitreichend auf die IT-Dienste auswirken. Solche Änderungen werden im CAB besprochen, um den erforderlichen Aufwand zu definieren und das Risiko zu minimieren. Im Vorfeld der Sitzung wird zunächst die notwendige Dokumentation an die Mitglieder des CAB sowie falls erforderlich auch an einige IT-Spezialisten und Entwickler verschickt.
- weitreichende Folgen:
  Eine Änderung dieser Kategorie erfordert einen hohen Aufwand. Für eine solche Änderung benötigt der Änderungsmanager zunächst die Autorisierung durch das Sicherheitsmanagement-Team. Anschließend muss die Änderung dem CAB noch zur Beurteilung und weiteren Planung vorgelegt werden.

Planung

Die am Änderungsmanagementprozess beteiligten Mitarbeiter planen die Umsetzung für alle angenommenen Änderungen. Bei Bedarf geschieht dies zusammen mit dem CAB. An dieser Stelle des Änderungsmanagementprozesses ist es wichtig, die dazu benötigten technischen und personellen Ressourcen zu berücksichtigen und abzuschätzen, wie sich die Durchführung der Änderung auf den Betrieb auswirkt. Die folgenden Aspekte sollten mindestens berücksichtigt werden:

- benötigte technische und personelle Ressourcen und deren KostenNotfallpläne für die Reaktion auf unerwünschte Effekte durch die Änderung,Zuverlässigkeit und Wiederherstellbarkeit der betroffenen IT-Dienste,
  - technische Genehmigungen, weil beispielsweise zusätzliche IT-Systeme beschafft werden müssen.
  - geschäftliche Genehmigungen, weil beispielsweise die Aktualisierung Auswirkungen auf Zulieferer hat.
- Anzahl und Verfügbarkeit der benötigten IT-Spezialisten,
- gewünschte zeitliche Umsetzung einer Änderung,
- Konsequenzen für die Nutzung der IT-Dienste und daraus resultierende Anpassungen an Service-Level-Vereinbarungen,
- eventuelle Konflikte mit anderen Änderungen.

OPS.1.1.3.M6 Abstimmung von Änderungsanforderungen [Änderungsmanager]

Ob ein Änderungsmanagementprozess erfolgreich ist, hängt von einer effektiven Kommunikation ab, da die einzelnen Prozessschritte, wie sie in OPS.1.1.3.M4 *Planung des Änderungsmanagementprozesses* und OPS.1.1.3.M5 *Umgang mit Änderungsanforderungen* festgelegt wurden, oft nur weiter durchgeführt werden können, nachdem die verantwortlichen Rollen reagiert haben.

In den Abstimmungsprozess für eine Hard- oder Softwareänderung sind außer dem Change Advisory Board (CAB) eventuell weitere Zielgruppen einzubeziehen. Welche das sind, hängt von der Größe und der Struktur der Institution ab. Typischerweise sollten der Antragsteller einer Hard- oder Softwareänderung, der IT-Helpdesk und der von den Auswirkungen der Änderung betroffene Endbenutzer bzw. ein Vertreter des Fachbereiches einbezogen werden.

Den Geschäftsprozess-Verantwortlichen muss das Antragsverfahren für Hard- oder Softwareänderungen bekannt sein. Sie müssen auch erfahren, welchen Prozess der Antrag durchläuft und welche Informationen im Verlauf des Antragsverfahrens bereit gestellt werden. Ein wesentlicher Aspekt ist die inhaltliche Qualität des Änderungsantrages (RfCs). Die notwendigen Angaben werden häufig als Formular oder über eine Eingabemaske in einer speziellen Anwendung erfasst. Welche Informationen benötigt werden und wie das Formular aufgebaut wird, sollte daher besonderes sorgfältig mit den möglichen Zielgruppen abgestimmt und festgelegt werden.

Ferner muss durch den Änderungsmanagementprozess sichergestellt werden, dass sich bei schwerwiegenden Änderungen alle Fachverantwortlichen zum Antragsinhalt äußern können, um eine aus Sicht einer Zielgruppe unerwünschte Änderung zu verhindern.

Auf der anderen Seite darf das Antragsverfahren nicht zu lange dauern. Es muss außerdem möglich sein, wichtige Änderungen beschleunigt zu behandeln. Dabei muss es unter Umständen definiert erlaubt sein, den regulären Änderungsmanagementprozess abzukürzen.

OPS.1.1.3.M7 Integration des Änderungsmanagements in die Geschäftsprozesse [Änderungsmanager]

Je nach Art der durchgeführten Änderungen kann es notwendig sein, dass eine Anwendung oder ein IT-System neu gestartet werden muss und dadurch über einen kurzen Zeitraum ausfällt. Darüber hinaus können auch sorgfältig durchgeführte Tests nicht immer vermeiden, dass es zu Schwierigkeiten bei der betroffenen Anwendung kommt oder ein System durch die Verteilung von Hard- oder Software-Änderungen ganz ausfällt.

Aus diesem Grund ist, unabhängig von durchgeführten Tests, auch die aktuelle Situation der betroffenen Geschäftsprozesse zu berücksichtigen. Es kann z. B. durchaus sinnvoll sein, eine Hard- oder Software-Änderung ein paar Tage später durchzuführen, obwohl das betroffene System zum aktuellen Zeitpunkt als sicherheitskritisch eingestuft wird. Eventuell werden durch das System wichtige Dienstleistungen erbracht, auf die die Institution angewiesen ist. Die Leitungsebene könnte das Risiko einer Unterbrechung von Geschäftsprozessen durch das Patch- und Änderungsmanagement höher bewerten als das Risiko durch eine noch nicht geschlossene Schwachstelle.

Um Hard- und Software-Änderungen zu verteilen, ist es daher notwendig, alle Beteiligten bezüglich der kommenden Änderungen und der zu erwartenden Ausfallzeiten zu benachrichtigen. Zu den einzelnen Parteien gehören alle Fachabteilungen, die das System benötigen. Insbesondere Fachabteilungen, deren Aufgabenerfüllung von den betroffenen Anwendungen und IT-Systemen abhängig ist, müssen in die Priorisierung von Änderungen und in die Terminfindung einbezogen werden.

Es muss mindestens eine Eskalationsebene über dem Änderungsmanager und dem CAB existieren,die notfalls über die Priorisierung entscheidet (siehe OPS.1.1.3.M5 *Umgang mit Änderungsanforderungen*). Diese Eskalationsebene muss aus der Leitungsebene der Institution gewählt werden.

OPS.1.1.3.M8 Sicherer Einsatz von Werkzeugen für das Patch- und Änderungsmanagement [Leiter IT]

Ein Werkzeug für das Patch- und Änderungsmanagement spielt als zentrale Instanz zur Umsetzung des Änderungsmanagementprozesses und zur Softwareverteilung für den sicheren und ordnungsgemäßen Betrieb der Institution eine wesentliche Rolle.

Geeignete Auswahl von Werkzeugen

Der Änderungsmanagementprozess kann mit verschiedenen Produkten oder Produktkombinationen unterstützt werden. Es kann vielfältige Gründe geben, Änderungen mithilfe eines geeigneten Werkzeugs umzusetzen. Häufig sind heterogene IT-Infrastrukturen und die effektivere Ausnutzung von Ressourcen bestimmend.

Bevor ein Werkzeug für das Patch- und Änderungsmanagement beschafft wird, sollten die Anforderungen und Rahmenbedingungen ermittelt werden, um ein für die jeweilige Institution geeignetes Produkt zu finden. Das Vorgehen für die Evaluation eines Werkzeugs ist stets ähnlich und orientiert sich an der gültigen Änderungsstrategie der Institution, unabhängig davon, ob ein Änderungsmanagement als Werkzeug für ein Betriebssystem, für die Produktpalette eines Herstellers oder für ein großes heterogenes IT-Szenario benötigt wird.

Nachfolgend sind die wichtigsten Ausstattungsmerkmale aufgeführt, die bei der Produktwahl beachtet werden sollten.

- Plattformunterstützung:
  Einerseits bezeichnet dieser Begriff, welche Plattformen bezüglich Umsetzung des Patch- und Änderungsprozesses unterstützt werden und andererseits, auf welcher Plattform das Werkzeug selbst lauffähig ist. Besonders der erste Aspekt sollte sehr detailliert betrachtet werden, da beispielsweise im Server-Client-Bereich die meisten Werkzeug-Hersteller Patches und Änderungsvorgänge bei Microsoft-Produkten unterstützen. Dies heißt jedoch nicht, dass auch die gesamte in der Institution vorhandene IT-Produktpalette von Desktop- und Server-Betriebssystem über Applikationsserver bis hin zu Einzelprodukten abgedeckt wird.
- Änderungsanalyse:
  Einige Hersteller konzentrieren sich auf die mit dem Verteilungsprozess verbundene Menge der Updates und ihre rasche Verteilung sowie auf das Reporting des "Auslieferungsstatus". Einige liefern mehr Informationen zu den Hintergründen bzw. Gründen eines Patches, teilweise mit Listen betroffener Dateien, genauer Beschreibung der Schwachstellen und eigenen Testberichten. Insbesondere für Sicherheitspatches, die in der Regel rasch verteilt werden sollten, liefern die Detailinformationen einen unverzichtbaren Hinweis für die interne Einstufung der Hard- oder Software-Änderung.
- Änderungsverifikation:
  Die meisten Hersteller liefern Hash-Summen, Fingerprints oder Signaturen mit den Änderungen, um deren Echtheit und Integrität zu bestätigen. Jedoch prüfen nur wenige Werkzeuge diese Nachweise. Deswegen besteht die Gefahr, dass unerwünschte Software massenhaft in der Institution verteilt wird und so ein erheblicher Schaden entsteht. Aus Sicherheitsgründen sollten daher keine Änderungswerkzeuge eingesetzt werden, bei denen diese Funktion fehlt.
- Änderungsstrategie:
  Das Werkzeug muss eine flexible Konfiguration ermöglichen, um möglichst viele Schritte der gewählten Änderungsstrategie zu automatisieren. Diese kann aufgrund unterschiedlicher Plattformen stark differieren. Die abgearbeiteten Schritte des Änderungsprozesses sollten vom Tool nachvollziehbar, je nach Bedarf sogar revisionssicher, dokumentiert werden. Spätere Änderungen im Prozess müssen in das Werkzeug einfließen können.
- Verteilung:
  Nicht jede Änderung sollte auf jedes System aufgespielt werden. Das Werkzeug sollte die Gruppierung von Systemen und Applikationen nach frei definierbaren Attributen wie z. B. Schutzbedarf, Standort und Organisationseinheit ermöglichen. Aus diesen Attributen können entsprechend den standardisierten Systemtypen in der Institution IT-Systemprofile werden.
- Rollback:
  Keine Software ist perfekt. Deshalb kann es trotz aller Tests notwendig sein, einen Änderungsprozess wieder umzukehren. Diesen Vorgang automatisieren zu können spart im Fehlerfall Zeit und Geld. Wenn sich fehlerhafte Änderungen nicht zeitnah und mit geringem Aufwand zurücknehmen lassen, kann das die Institution erheblich schädigen.
- Statusbewertung:Es muss möglich sein, die geänderte Hard- oder Software auf allen Systemen automatisch und korrekt zu verteilen. Es könnten, wie allgemein bei der Softwareverteilung, Probleme mit der Verbindung oder Verfügbarkeit eines Systems auftreten. So kann ein System zum Beispiel einen Patch aufgrund anderer Systemzustände ablehnen. Wichtig ist daher, dass das Änderungswerkzeug den Patch-Status aller Systeme erfasst. Je nach Strategie sollte das Werkzeug bei aufgetretenen Problemen den technischen Änderungsprozess bei den restlichen IT-Systemen fortsetzen oder bestimmte Systemgruppen überspringen oder den Prozess beenden.

Sicherheitsrichtlinie für den Einsatz von Änderungsmanagementwerkzeugen

Das Patch- und Änderungsmanagement muss mit einem angemessenen organisatorischen und technischen Aufwand betrieben werden. Dabei ist unter anderem der Schutzbedarf der Geschäftsprozesse und damit der Schutzbedarf der Daten und Systeme zu berücksichtigen. Dafür sollte eine spezifische Sicherheitsrichtlinie für das Änderungsmanagement erstellt werden. Diese muss mit dem Sicherheitskonzept der Institution und den daraus abgeleiteten Sicherheitsrichtlinien abgestimmt sein.

Aspekte, zu denen in dieser Sicherheitsrichtlinie Vorgaben formuliert werden müssen, sind:

Vorgaben für die Planung:

- Das Werkzeug muss über skalierbare Serverapplikationen verfügen. Dafür müssen bereits im Vorfeld Anforderungen formuliert werden, wie Replikation und Lastverteilung eingesetzt werden sollen und wie technische Redundanzen benutzt werden können.
- Für eine sichere Netzverbindung zu externen Bezugsquellen von Patches oder Änderungen, z. B. bei Herstellern, müssen geeignete Regelungen festgelegt werden. Beispielsweise könnte die Direktverbindung der Clients zu den Herstellern der eingesetzten Software durch entsprechende Regeln auf dem Sicherheitsgateway auf einen Proxy umgeleitet werden.
- Damit die Integrität und Authentizität von Änderungen zuverlässig überprüft werden können, müssen geeignete Konzepte und Komponenten festgelegt werden.
- Es müssen Anforderungen an die Dokumentation für Betrieb, Notfall und Wiederanlauf des Änderungsmanagement-Werkzeugs formuliert werden. Dazu gehört unter anderem, dass die Dokumentation immer aktuell sein muss. Des Weiteren sollte definiert werden, wo die Dokumentation aufbewahrt werden muss und wie viele Exemplare der Dokumentation vorhanden sein müssen.

Vorgaben für die Administration:

- Es ist erforderlich, ein Rechtekonzept für Mitarbeiter im Änderungsmanagement und auch für die Dienste, die von der Patch- und Änderungsmanagementsoftware verwendet werden, zu erstellen.
- Für die Administratoren ist festzulegen, wie Rechte vergeben werden, welche Rechte sie bekommen oder welche sie verteilen dürfen.Vorgaben für die Installation:

- Die Werkzeuge für das Patch- und Änderungsmanagement müssen sicher konfiguriert werden. Die jeweiligen konkreten Einstellungen hängen stark von den vorhandenen Anwendungen und IT-Systemen der Institution ab.

- Es muss festgelegt werden, wie die für das Patch- und Änderungsmanagement-Werkzeug relevanten IT-Ressourcen unter Berücksichtigung von Sicherheitsaspekten konfiguriert werden.
- Das Patch- und Änderungsmanagement-Werkzeug sollte angemessen im LAN separiert werden. Neue Änderungen und Patches sollten nicht im Produktivnetz getestet werden, sondern in einem separaten Testnetz.

Vorgaben für den sicheren Betrieb

- Für den Betrieb eines Patch- und Änderungsmanagement-Tools sind Vorgaben und Abläufe festzulegen, also beispielsweise, wer darauf zugreifen darf und wo Änderungen durchgeführt werden dürfen.
- Patches und Änderungen werden häufig über das Internet bezogen. Verbindungen in öffentliche oder weniger vertrauenswürdige Netze sind grundsätzlich über Sicherheitsgateways abzusichern.
- Das Patch- und Änderungsmanagement-Werkzeug selbst muss in den Prozess des Patch- und Änderungsmanagements mit eingegliedert werden. Dabei ist zu definieren, wie Hard- und Software-Änderungen für das Patch- und Änderungsmanagement-Werkzeug selbst zu behandeln sind.

Vorgaben für Protokollierung und Monitoring

- Es ist festzulegen, wie die vom Werkzeug gelieferten Daten überwacht, protokolliert und ausgewertet werden sollen.

Datensicherung

- Ein geeignetes Verfahren für die Datensicherung ist festzulegen. Bei der Datensicherung sollten mindestens folgende Komponenten in regelmäßigen Abständen gesichert werden:
  - Die Konfiguration bzw. die Einstellungen der für das Patch- und Änderungsmanagement benötigten Werkzeuge.
  - Die Datenbanken mit den aktuellen Konfigurationen der IT-Systeme.
  - Bei selbst übersetzter Software die genauen Compiler-Einstellungen.
  - Die installierten Patches und Änderungen.
  - Die letzten Wiederherstellungspunkte der IT-Systeme.
  - Eventuell vorhandene ältere Versionsstände, beispielsweise weil die neueste Version einer Software noch nicht ausreichend getestet wurde oder nicht auf allen Systemen lauffähig ist.
  - Eine Übersicht über die Vergleichsprüfsummen der Softwarepakete, diese sollte eventuell auf einem Write Once Read Many - Medium (WORM) gesichert werden.
  - Eine Übersicht über die Vergleichsprüfsummen der Softwarepakete, diese sollte eventuell auf einem Write Once Read Many - Medium (WORM) gesichert werden.
- Des Weiteren muss das Datensicherungskonzept für das Patch- und Änderungsmanagement-Werkzeug in das übergreifende Datensicherungskonzept der Institution eingebunden werden.

Störung und Notfallvorsorge

- Für die Notfallvorsorge müssen die einzelnen Notfallpläne der Anwendungen und IT-Systeme, die vom Patch- und Änderungsmanagement verwaltet werden, berücksichtigt werden.
- Abhängig von den Verfügbarkeitsanforderungen an das Patch- und Änderungsmanagement-Werkzeug sollte überlegt werden, für das Werkzeug einen separaten Notfallplan für den Fall unerwünschter Effekte bei und nach der Installation von Patches und Änderungen zu erstellen.

OPS.1.1.3.M9 Test- und Abnahmeverfahren für neue Hard- und Software [Leiter IT]

Bevor neue Hardware-Komponenten oder neue Software in der Produktivumgebung eingesetzt werden, müssen sie auf speziellen Testsystemen kontrolliert werden. Dabei ist zu prüfen, ob das Produkt lauffähig ist und ob es sich negativ auf die laufenden IT-Systeme auswirkt. Da vor erfolgreichen Tests Schadfunktionen nicht ausgeschlossen werden können und da bei Tests Fehler provoziert werden, sind immer vom Produktionsbetrieb isolierte Testsysteme zu verwenden. Generelle Verfahrensweisen für die Software-Abnahme und -Freigabe inklusive des Testens sind in APP.5.1 *Standard-Software* beschrieben. Erst nach bestandenem Test dürfen neue Komponenten auf Produktionssystemen installiert werden.

Software-Abnahme-Verfahren

Im Zuge eines Software-Abnahme-Verfahrens wird überprüft, ob die betrachtete Software die erforderliche Funktionalität zuverlässig bereitstellt und ob sie darüber hinaus keine unerwünschten Nebeneffekte hat. Mit der anschließenden Freigabe der Software durch die fachlich zuständige Stelle wird die Erlaubnis erteilt, die Software zu nutzen. Gleichzeitig übernimmt diese Stelle damit auch die Verantwortung für das IT-Verfahren, das durch die Software realisiert wird.

Bei der Software-Abnahme wird sinnvollerweise zwischen Software unterschieden, die selbst oder im Auftrag entwickelt wurde, und Standardsoftware, die lediglich für den speziellen Einsatzzweck angepasst wird.

Abnahme von selbst- oder im Auftrag entwickelter Software

Bevor der Auftrag zur Software-Entwicklung intern oder extern vergeben wird, muss die Anforderungsdefinition für die Software erstellt sein, aus der dann das Grob- und Feinkonzept für die Realisierung entwickelt wird. Anhand dieser Dokumente erstellt die fachlich zuständige Stelle einen Abnahmeplan.

Üblicherweise werden hierzu Testfälle und die erwarteten Ergebnisse für die Software erarbeitet. Anhand dieser Testfälle wird die Software getestet. Der Abgleich zwischen erwartetem und tatsächlich berechnetem Ergebnis wird als Indiz für die Korrektheit der Software benutzt.

Zur Entwicklung der Testfälle und zur Durchführung der Tests ist folgendes zu beachten:

- die Testfälle werden von der fachlich zuständigen Stelle entwickelt,
- für Testfälle werden keine Daten des Wirkbetriebs benutzt,
- Testdaten, insbesondere wenn dafür Wirkdaten kopiert werden, dürfen keine vertraulichen Informationen beinhalten. Personenbezogene Daten sind zu anonymisieren oder zu simulieren,
- der Test darf sich nicht auf den laufenden Betrieb auswirken. Nach Möglichkeit sollte ein logisch oder physisch isolierter Testrechner benutzt werden.

Eine Abnahme ist zu verweigern, wenn:

- schwerwiegende Fehler in der Software festgestellt werden,
- Testfälle auftreten, in denen die erwarteten Ergebnisse nicht mit den berechneten übereinstimmen,
- Benutzerhandbücher oder Bedienungsanleitungen nicht vorhanden oder von nicht ausreichender Qualität sind und
- die Software, unter anderem der Quellcode und die Abläufe, nicht oder nicht ausreichend dokumentiert ist.

Die Ergebnisse der Abnahme sind schriftlich festzuhalten. Die Dokumentation des Abnahmeergebnisses sollte umfassen:

- Bezeichnung und Versionsnummer der Software und eventuell des IT-Verfahrens,
- Beschreibung der Testumgebung,
- Testfälle und Testergebnisse und
- Abnahmeerklärung.

Abnahme von Standardsoftware

Wird Standardsoftware beschafft, so sollte auch diese abgenommen und freigegeben werden. In der Abnahme sollte überprüft werden, ob

- die Software frei von Computer-Viren ist,
- die Software kompatibel zu den anderen eingesetzten Produkten ist,
- die Software in der angestrebten Betriebsumgebung lauffähig ist und welche Parameter zu setzen sind,
- die Software komplett einschließlich der erforderlichen Handbücher ausgeliefert wurde und
- die geforderte Funktionalität erfüllt wird.

Freigabe-Verfahren

Wurde die Software abgenommen, muss sie danach für die Nutzung freigegeben werden. Dazu ist zunächst festzulegen, wer berechtigt ist, Software freizugeben. Die Freigabe der Software ist schriftlich festzulegen und geeignet zu hinterlegen.

Die Freigabeerklärung sollte umfassen:

- Bezeichnung und Versionsnummer der Software und falls erforderlich des IT-Verfahrens,
- Bestätigung, dass die Abnahme ordnungsgemäß vorgenommen wurde,
- Einschränkungen für die Nutzung (Parametereinstellung, Benutzerkreis,...),
- Freigabedatum, ab wann die Software eingesetzt werden darf und
- die eigentliche Freigabeerklärung.

Falls IT-technisch möglich, muss verhindert werden, dass Software nach der Freigabe unbemerkt verändert oder manipuliert werden kann, beispielsweise durch geeignete Verfahren zum Integritätsschutz. Andernfalls müssen geeignete organisatorische Regelungen festgelegt werden, um Änderungen an der Software zu verhindern bzw. zeitnah festzustellen.

Auch nach intensiven Abnahmetests kann es vorkommen, dass im laufenden Einsatz Fehler in der Software festgestellt werden. Für diesen Fall ist festzulegen, wie in einem solchen Fehlerfall verfahren werden soll (Ansprechpartner, Fehlerbeseitigungsablauf, Beteiligung der fachlich zuständigen Stelle, Wiederholung der Abnahme und Freigabe, Versionskontrolle).

OPS.1.1.3.M10 Sicherstellung der Integrität und Authentizität von Softwarepaketen [Administrator]

Software sollte grundsätzlich nur aus bekannten Quellen installiert werden, besonders dann, wenn sie nicht auf Datenträgern geliefert, sondern beispielsweise aus dem Internet heruntergeladen wurde. Das gilt besonders für Updates oder Patches. Die meisten Hersteller und Distributoren bieten zu diesem Zweck Prüfsummen an, mit denen sich zumindest die Integrität eines Paketes überprüfen lässt. Die Prüfsummen werden dabei meist auf den Webseiten der Hersteller veröffentlicht oder auch per E-Mail verschickt. Um die Integrität eines heruntergeladenen Programms oder einer Archivdatei zu verifizieren, wird dann die veröffentlichte Prüfsumme mit einer von einem entsprechenden Programm lokal erzeugten Prüfsumme verglichen.

Falls zu einem Softwarepaket Prüfsummen angeboten werden, so sollten diese überprüft werden, bevor das Paket installiert wird.

Die Authentizität kann mit Prüfsummen jedoch nicht überprüft werden. Daher werden in vielen Fällen für Programme oder Pakete digitale Signaturen angeboten. Die zur Überprüfung der Signatur benötigten öffentlichen Schlüssel sind wiederum meist auf den Webseiten des Herstellers oder von Public-Key-Servern verfügbar. Häufig werden die Prüfsummen mit einem der Programme PGP oder GnuPG erzeugt.

Ergibt die Prüfung, dass es sich um eine gültige Signatur des jeweiligen Herstellers handelt, so resultiert daraus ein deutlich höherer Grad an Vertrauenswürdigkeit für das Paket als lediglich durch das Vorhandensein einer Prüfsumme.

Manchmal führen selbst die eingebauten Software-Updatemechanismen des jeweiligen Betriebssystems oder der Anwendungssoftware keine Prüfsummenvergleiche durch. Wenn möglich, sollte allerdings bei jedem Softwarepaket ein Prüfsummencheck durchgeführt werden.

Ferner sind nicht alle Prüfsummenvergleiche ohne Mitwirkung der Benutzer durchführbar, da die hierfür erforderlichen Checksummen, Signaturen oder Zertifikate von den Herstellern nicht auf eine einheitliche Weise bereitgestellt werden. Daher ist häufig eine manuelle Verifikation auf den Herstellerseiten oder die Anpassung der URLs in der Änderungssoftware nötig.

Falls zu einem Softwarepaket digitale Signaturen verfügbar sind, sollten diese auf jeden Fall vor der Installation des Pakets überprüft werden.

Ein prinzipielles Problem bei der Verwendung digitaler Signaturen stellt die Verifikation der Authentizität des verwendeten Schlüssels selbst dar. Trägt der öffentliche Schlüssel keine Signatur einer bekannten vertrauenswürdigen Person oder Organisation (etwa eines Trustcenters), so bieten die mit dem entsprechenden privaten Schlüssel erzeugten Signaturen keine wirkliche Sicherheit, dass das Softwarepaket tatsächlich vom Entwickler, Hersteller oder Distributor stammt. Daher sollten die öffentlichen Schlüssel, sofern sie nicht zertifiziert sind, möglichst aus einer anderen Quelle als das Softwarepaket selbst bezogen werden, beispielsweise von einem anderen Spiegelserver, auf dem das Paket ebenfalls heruntergeladen werden kann, oder von einem Public-Key-Server.

Um Prüfsummen und digitale Signaturen zu überprüfen, müssen die entsprechenden Programme lokal vorhanden sein. Die Administratoren sollten über die Bedeutung und Aussagekraft von Prüfsummen und digitalen Signaturen informiert sein. Außerdem müssen die Administratoren genügend Zeit haben, die Prüfprogramme im Arbeitsalltag einzusetzen und sich mit der Bedienung vertraut zu machen.

Von einem Bezug von Patches und Änderungen per E-Mail ist aus verschiedenen Gründen abzuraten. Die Herkunft von E-Mails ist ohne Einsatz zusätzlicher Sicherheitsmechanismen schwer festzustellen und die Empfängeradressen in den Institutionen sind oft Verteilerlisten, deren Adresse leicht zu erraten ist. Patches und Änderungen können außerdem sehr umfangreich sein. Viele Unternehmen und Behörden haben die Größe von E-Mail-Anhängen beschränkt und verbieten unter Umständen zudem die Annahme ausführbarer Anhänge. Ferner werden durch die großen Datenmengen die E-Mail-Systeme unnötig belastet. Daher kann eine rechtzeitige Verfügbarkeit der Software-Änderungen, die besonders bei Sicherheitspatches kritisch sein kann, via E-Mail nicht ausreichend gewährleistet werden.

Des Weiteren bieten einige Hersteller an, Änderungen und Patches dem Kunden direkt auf Datenträgern zuzusenden. Auch in diesem Fall sollten die Änderungen möglichst anhand von Prüfsummen oder digitalen Signaturen verifiziert werden, denn Absender-Angaben auf Postsendungen und Hersteller-Logos auf CDs und DVDs lassen sich leicht fälschen.

Ein weiteres Hilfsmittel zur Prüfung der Echtheit der Aktualisierung können vom Hersteller veröffentlichte Nachrichten auf seiner Webseite, per Newsletter oder über ähnliche Kanäle sein. Einige Hersteller haben Zyklen und Zeitpunkte etabliert, zu denen in der Regel systematisch Informationen über Änderungen veröffentlicht werden.

OPS.1.1.3.M11 Kontinuierliche Dokumentation der Informationsverarbeitung [Leiter IT, Änderungsmanager]

Die Informationsverarbeitung muss kontinuierlich in allen Phasen, allen Anwendungen und allen Systemen dokumentiert werden, um einen ordnungsgemäßen IT-Betrieb gewährleisten zu können. Dazu gehören:

- eine aktuelle Dokumentation aller vorhandenen IT-Systeme und deren Konfiguration,
- die Dokumentation der auf den jeweiligen IT-Systemen eingerichteten Benutzer und deren Rechteprofile, dies umfasst auch eine Beschreibung und Begründung aller Einschränkungen bei der Nutzung von IT-Systemen,
- die neu hinzugekommenen Hard- und Softwarekomponenten müssen in der Systemdokumentation aufgeführt werden,
- die Dokumentation aller sicherheitsrelevanten Abläufe wie der Datensicherung oder der Vernichtung von Datenträgern,
- die Dokumentation der Wartungsmaßnahmen,
- eine Beschreibung aller gefundenen und behobenen Fehler.

Die Benennung der Systemverantwortlichen sollte ebenfalls schriftlich erfolgen und den Benutzern bekannt gegeben werden. Für Problemfälle sollte dokumentiert sein, wer helfen kann und wo Informationen zu finden sind.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

OPS.1.1.3.M12 Skalierbarkeit beim Änderungsmanagement (A)

Bei der Beschaffung eines Patch- und Änderungsmanagement-Werkzeugs gelten oft andere Anforderungen als im späteren Betrieb. Die IT-Landschaft wächst und zusätzliche IT-Systeme, die vom Patch- und Änderungsmanagement berücksichtigt werden müssen, kommen hinzu. Daher ist es wichtig, dass das Patch- und Änderungsmanagement-Werkzeug skaliert werden kann. Welche Skalierbarkeit bei der Einführung des Systems benötigt wird, muss bereits während der Planungsphase ermittelt werden.

Die Hauptfaktoren, welche die Skalierbarkeit beeinflussen, sind die geforderte Umsetzungsgeschwindigkeit mit der Hard- oder Software-Änderungen in der vorhandenen IT-Infrastruktur verteilt werden sollen sowie die Notwendigkeit, im Fehlerfall die IT-Systeme massiv parallel wiederherzustellen.

Für den Fall, dass fehlerhafte Hard- oder Software-Änderungen verteilt werden, müssen Unterbrechungspunkte definiert werden. Da diese Möglichkeit stark von der Umsetzungsgeschwindigkeit abhängt, muss festgelegt werden, wo, wie und zu welchem Zeitpunkt eine bewusste Unterbrechung der Verteilung möglich ist.

Um festzustellen, ob eine erwartete Umsetzungsgeschwindigkeit tatsächlich besteht, können zunächst Betriebswerte der IT-Infrastruktur wie Netzbandbreiten und Systemauslastung herangezogen werden. Die Umsetzungsgeschwindigkeit muss vor Inbetriebnahme des Systems jedoch sorgfältig getestet werden. Auf eventuelle auftretende Engpässe in der IT-Infrastruktur muss rasch durch Erweiterung oder Konfigurationsänderung reagiert werden.

Zu den ermittelten Werten ist ein vermutetes Wachstum der IT-Infrastruktur in der direkten Zeit nach der Inbetriebnahme hinzuzurechnen, um nicht sofort in eine weitere Skalierungs- und Umbauphase des Systems überzugehen. Weitere Erfahrungswerte aus dem Betrieb sollten gesammelt und dann als zusätzliche Anhaltspunkte für den weiteren Ausbau des Systems verwendet werden.

In der Praxis hat es sich bewährt, die Skalierbarkeit entsprechend der physischen und geografischen IT-Struktur der Institution umzusetzen. Wenn es die Änderungsstrategie der Institution erlaubt, können z. B. in den Niederlassungen der Institution Verteilersysteme eingesetzt werden, die die Software-Änderungen nur für die IT-Systeme des jeweiligen Standortes erhalten und verarbeiten.

Ist die Änderungsstrategie der Institution dagegen stark zentral orientiert oder werden die Patch- und Änderungsmanagement-Werkzeuge im Outsourcing betrieben, so ist es empfehlenswert, die Skalierung so zu wählen, dass pro Niederlassung dezidierte Systeme betrieben werden.

Werden Softwarewerkzeuge zur Unterstützung des Patch- und Änderungsmanagements eingesetzt, so ist darauf zu achten, dass diese den Anforderungen an die Skalierbarkeit genügen.

OPS.1.1.3.M13 Erfolgsmessung von Änderungsanforderungen (IA)

Managementprozesse wie das Patch- und Änderungsmanagement müssen stetig verbessert, optimiert und an die sich verändernden Bedingungen in der Institution angepasst werden. Die Art und Weise, wie die vorliegende Maßnahme in der Institution umgesetzt wird, zeigt auch den Reifegrad des Patch- und Änderungsmanagement-Prozesses.

Mit den im Vorfeld von Hardware-, Software- oder Konfigurationsänderungen durchgeführten Tests lässt sich vorwiegend überprüfen, ob die Änderungen im voraussichtlichen Einsatzfeld grundsätzlich funktionieren. Da Änderungen meistens eine Störung beheben sollen, ist es notwendig, von den Antragstellern der Änderungsanforderung nachträglich eine Auswertung über den Erfolg der Änderung einzuholen.

Dafür ist es unumgänglich, so genannte Nachtests durchzuführen. Als Voraussetzung dafür müssen Referenzsysteme als Qualitätssicherungssysteme ausgewählt werden. Außerdem muss sichergestellt werden, dass die Nachtests durch diejenigen Fachanwender, welche die Geschäftsprozesse der Institution kennen und eventuell vorhandene Fehler beurteilen können, durchgeführt werden.

Wurde die Änderung aus Sicherheitssicht nötig, müssen die Nachtests vom Änderungsmanager initiiert und von Fachanwendern durchgeführt werden.

Die Ergebnisse der Nachtests und Auswertungen werden im Rahmen des Patch- und Änderungsprozesses dokumentiert. Für den Änderungsmanager, das Change Advisory Board und das Sicherheitsmanagement sind somit Daten verfügbar, mit denen der Prozess verbessert werden kann.

OPS.1.1.3.M14 Synchronisierung innerhalb des Änderungsmanagements [Änderungsmanager] (CIA)

In den meisten Behörden und Unternehmen werden häufig Änderungen an der IT-Infrastruktur vorgenommen. Auf diese Änderungen muss der Änderungsmanagementprozess reagieren. Dabei muss gewährleistet werden, dass die jeweiligen Patches und Änderungen zeitnah und möglichst gleichzeitig auf alle betroffenen IT-Systeme aufgespielt werden.

Bei mobilen Endgeräten oder auch wenn das verwendete Netz überlastet ist, kann es vorkommen, dass IT-Systeme bei der Verteilung von Hard- oder Software-Änderungen nicht erreichbar sind. Für solche Fälle müssen geeignete Mechanismen etabliert werden, die sicherstellen, dass sich Systeme erst dann wieder am Netz anmelden können, wenn sie mit geeigneten Updates versorgt wurden. Es gibt verschiedene Werkzeuge, die vor einem Zugriff auf das Produktivnetz überprüfen, ob Sicherheitsprogramme und Sicherheitspatches auf dem aktuellen Stand sind, und bei Sicherheitsmängeln den Zugriff auf das interne Netz abweisen. In der Regel werden solche Tools dazu benutzt, den Softwarestand der Systeme zunächst festzustellen und dann die Software zur Aktualisierung zusammen zu stellen. Je nach Art des Änderungsprozesses können diese dann automatisch oder nach vorheriger Freigabe für diese Systeme verteilt und installiert werden. Änderungen, die einen Systemneustart erfordern, sollten als letztes installiert werden, oder erst beim Herunterfahren des IT-Systems. Je nach technischer Unterstützung und Umsetzung des Prozesses können die Aktualisierungen auch installiert werden und der danach nötige Neustart kann gesondert freigegeben werden.

3 Weiterführende Informationen

3.1 Wissenswertes

Grundbegriffe des Änderungsmanagements

Beim Änderungsmanagementprozess werden verschiedene Aktualisierungen und Verbesserungen in der Produktionsumgebung bereit gestellt, gesteuert und verwaltet. In diesem Bereich haben sich eine Vielzahl von Begriffen etabliert. Diese müssen den am Prozess beteiligten Personen bekannt sein.

Bei **Versionsbezeichnungen** sind sehr unterschiedliche Benennungen gebräuchlich. Das ist darauf zurückzuführen, dass für die Begriffsdefinition kein einheitlicher, verbindlicher, übergreifender Standard existiert. Während der Entwicklung durchlaufen die Produkte verschiedene **Stadien.** Aufgrund der nicht exakt definierten Begriffe empfiehlt es sich, innerhalb der Institution ein Glossar zu benutzen, um ein einheitliches Verständnis aller Fachausdrücke sicher zu stellen.

Die erste lauffähige Version eines Produkts wird oft **Alpha-Version** genannt. Die Alpha-Version dient meist der internen Verwendung, z. B. um zu demonstrieren, dass ein Softwareprojekt durchführbar ist. Sie enthält deshalb in der Regel bereits die wichtigsten Grundfunktionen.

Eine **Beta-Version** ist eine noch unfertige Produkt-Version, die vom Entwickler oft zu Test- und Vorverkaufszwecken veröffentlicht wird. Die wesentlichen Funktionen des Produktes sind bereits vorhanden, jedoch noch nicht ausreichend getestet. Beta-Versionen werden an sogenannte Beta-Tester verteilt, welche die Funktionalität und Nutzbarkeit des Produktes überprüfen und Fehler an die Entwickler melden. In der Software werden so typischerweise viele Programmierfehler gefunden.

Bei der Software-Entwicklung bezeichnet **Release Candidate** (**RC**) oder **Freigabekandidat** eine abschließende Testversion. In dieser Version sind alle Funktionen, welche die Endversion der Software enthalten soll, verfügbar. Diese Versionsart dient einem abschließenden System- oder Produkttest. Es werden nur dann weitere RCs veröffentlicht, wenn dabei gravierende Qualitätsprobleme ermittelt werden.

Die fertige und veröffentlichte Version einer Software wird als **Release** oder **Stable** bezeichnet und in der Regel zusätzlich mit einer Versionsnummer versehen. Da zu diesem Zeitpunkt auch mit der Herstellung der Medien begonnen wird, wird oft auch der Begriff **Ready to Manufacturing (RTM)** benutzt.

Viele Softwareentwickler, haben Mechanismen für den Umgang mit Softwarekorrekturen veröffentlicht. Dabei werden die nachfolgenden Begriffe nicht immer konsequent einheitlich verwendet. Sie geben jedoch insgesamt den notwendigen Überblick über die Begriffswelt in diesem Themengebiet.

Softwarekorrekturen werden veröffentlicht, um Fehler in bereits veröffentlichter Software zu beheben. Ein **Patch** ist ein generelles **Softwareupdate**, welches Fehlfunktionen in einer Software behebt. Zunächst ist ein solches **Update** nicht kritisch und nicht sicherheitsrelevant. Ist das Update relevant für die Sicherheit der Software, wird also eine Sicherheitslücke geschlossen, wird es oft **Sicherheitspatch** genannt. Für einen Sicherheitspatch wird oft ein **Schweregrad** angegeben. Dieser bezieht sich in der Regel darauf, für wie schwerwiegend der Hersteller die Sicherheitslücke hält, die der Sicherheitspatch behebt. Wird mit dem Update eine wesentliche Funktionalität der Software korrigiert, die aber nicht unbedingt sicherheitsrelevant ist, beispielsweise eine falsche Berechnung, so wird es oft als **kritisches Update** bezeichnet.

Eine andere Veröffentlichung der Hersteller, die sich jedoch nur auf spezielle Kundensituationen bezieht und oft nur bei gültigem Supportvertrag zur Verfügung gestellt oder erst aufgrund von Supportanfragen erstellt wird, hat die Bezeichnung **Hotfix**. Dabei kann es sich um ein einzelnes Paket aus einer oder mehreren Dateien handeln, um ein Problem in einem Produkt zu beheben.

Bei einem **Servicepack** dagegen handelt es sich um eine kumulative Sammlung von Hotfixes, Sicherheitspatches, kritischen Updates und Updates, die seit der Markteinführung des Produktes veröffentlicht wurden und der Allgemeinheit zur Verfügung gestellt werden.

Der Zeitraum bis zur Veröffentlichung von Servicepacks ist oft sehr lang ist. Für die Bereitstellung der Menge der zwischendurch verfügbaren Softwarekorrekturen kann außerdem eine Zusammenfassung sinnvoll sein. Daher veröffentlichen einige Hersteller zwischendurch sogenannte **Update Roll-Ups**. Das ist eine Sammlung von Sicherheitspatches, kritischen Updates, Updates und Hotfixes, die kumulativ oder für eine einzelne Produktkomponente, wie beispielsweise einen Webserver, angeboten werden.

Nach der Veröffentlichung von Servicepacks werden die dann verfügbaren Produktserien oft im Dezimalkommastellenbereich um eine Nummer erhöht. Das soll dokumentieren, dass die Softwareprodukte bereits alle bis zu diesem Zeitpunkt verfügbaren Korrekturen enthalten. Einige Hersteller bezeichnen dies auch als **Integriertes Service Pack**.

Aufgrund der verschiedenen Anforderungen von Kunden, sehen sich Hersteller oft gezwungen, neue Optionen (Features) in ihr Produkt zu integrieren. Diese Funktionserweiterungen werden in der Regel allen Kunden mit gültigen Vertragsbeziehungen zum Hersteller (Supportvertrag, Updatevertrag, Softwarepflegevertrag etc.) als **Featurepack** angeboten. Die neuen Features fließen gewöhnlich in die nächste Produktversion mit ein.

Zwei Arten der **Änderung** an IT-Komponenten sind in der betrieblichen Praxis üblich. **Standardisierte Änderungen** und **Änderungen**, die den Änderungsmanagementprozess durchlaufen müssen.

Standard-Änderungen sind Änderungen an Anwendungen und IT-Systemen, für die genaue Verfahrensanweisungen existieren und die vorab vom **Änderungsmanager** genehmigt wurden.

Die geschriebene Verfahrensanweisung muss gewährleisten, dass das mit der Änderung zusammenhängende Risiko vernachlässigt werden kann. Die Änderung kann ausgeführt werden, ohne noch einmal den Änderungsmanager kontaktieren zu müssen. Dadurch wird die Arbeitsmenge der mit dem Prozess beauftragten Personen wesentlich reduziert.

Einer der Beweggründe für Hard- oder Software-Änderungen sind Störungen. Eine **Störung** (**Incident**) ist eine Abweichung vom standardmäßigen Betrieb einer IT-Dienstleistung (**Service**), die tatsächlich oder potenziell die Service-Qualität mindert oder sogar den Service unterbricht.

Ist die Ursache für eine Störung nicht erkennbar, so liegt ein näher zu untersuchendes Problem vor. Mit dem Begriff **Problem** werden in ITIL eine oder mehrere gleichartige Störungen mit unbekannter Ursache bezeichnet. Wird die zugrunde liegende Ursache ermittelt und eine Möglichkeit gefunden, das Problem zu beheben oder zu umgehen, wird aus einem Problem ein bekannter Fehler (Known Error). Der Lösungsweg wird in einer Änderungsanforderung (Request for Change, RfC) dokumentiert und unter der Kontrolle des Änderungsmanagements (Change Managements) umgesetzt.

Zusätzlich zu der speziellen Begriffswelt des Änderungsmanagements (beispielsweise aus ITIL), sollten die damit betrauten Personen mit der Begriffswelt der Informationssicherheit vertraut sein.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Patch- und Änderungsmanagement" finden sich unter anderem in folgenden Veröffentlichungen:

[GSKHM] Hilfsmittel zur Nutzung der IT-Grundschutz-Kataloge

Bundesamt für Sicherheit in der Informationstechnik (BSI), https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Kataloge/Hilfsmittel/Bausteine/bausteine_node.html, zuletzt abgerufen am 05.10.2018

Umsetzungshinweise zum Baustein OPS.1.2.2 Archivierung

1 Beschreibung

1.1 Einleitung

Bei nahezu allen Geschäftsprozessen entstehen Daten, die geeignet archiviert oder über eine lange Zeit gespeichert werden müssen, um sie später wiederfinden und verwenden zu können. Kennzeichnend für die Archivierung (Langzeitspeicherung) ist die dauerhafte und unveränderbare Speicherung von elektronischen Dokumenten und anderen Daten. Die Aufbewahrungsfrist der jeweiligen Daten muss zum Archivierungszeitpunkt festgelegt werden. Eventuell müssen die Daten auch zeitlich unbegrenzt verfügbar sein.

Wenn in diesem Baustein der Begriff "Dokumente" benutzt wird, werden hiermit auch Daten inkludiert.

1.2 Lebenszyklus

In der Planungsphase müssen die Ziele definiert und ein Archivierungskonzept entwickelt werden (siehe OPS.1.2.2.M2 *Entwicklung eines Archivierungskonzepts*). Hierbei müssen die relevanten Anforderungen ermittelt werden (siehe OPS.1.2.2.M1 *Ermittlung von Einflussfaktoren für die elektronische Archivierung*), wobei auch abgeschätzt werden muss, wie sich die Anforderungen während der erwarteten Laufzeit des einzuführenden Archivsystems entwickeln werden.

Umsetzung

Bei der Einführung eines Archivsystems ist zunächst ein System auszuwählen, das den ermittelten Anforderungen genügt (siehe OPS.1.2.2.M17 *Auswahl eines geeigneten Archivsystems*). Darüber hinaus sind der Aufstellungsort des Systems sowie der Lagerungsort der Archivmedien festzulegen (siehe OPS.1.2.2.M3 *Geeignete Aufstellung von Archivsystemen und Lagerung von Archivmedien*).

Betrieb

Auch muss festgelegt werden, wie das Archivsystem zu benutzen ist, und die Administratoren und Benutzer müssen entsprechend geschult werden (siehe OPS.1.2.2.M10 *Erstellung einer Richtlinie für die Nutzung von Archivsystemen*).

Um die Ordnungsmäßigkeit langfristig sicherstellen zu können, sind nicht nur der Archivierungsprozess kontinuierlich zu überwachen (siehe OPS.1.2.2.M13 *Regelmäßige Revision der Archivierungsprozesse*) und zu dokumentieren., sondern auch die Informationserhaltung sowie, soweit erforderlich, die Beweiswerterhaltung zu gewährleisten. Daneben gilt es, die relevanten Standards und Normen einzuhalten. Darüber hinaus ist sicherzustellen, dass zu jedem Zeitpunkt genügend Speicherressourcen zur Archivierung verfügbar sind (siehe OPS.1.2.2.M12 *Überwachung der Speicherressourcen von Archivmedien*).

Migration

Die Migrationsphase wird häufig durch folgende Ereignisse ausgelöst:

- Bei Systemkomponenten oder Datenformaten hat ein Technologiewechsel stattgefunden. Daher sollten die Entwicklungen in diesem Bereich beobachtet werden (siehe OPS.1.2.2.M9 *Auswahl geeigneter Datenformate für die Archivierung von Dokumenten*).
- Systemkomponenten, insbesondere Datenträger, sind überaltert und müssen durch neue ersetzt werden (siehe OPS.1.2.2.M16 *Regelmäßige Erneuerung technischer Archivsystem-Komponenten*).
- Die Nutzungskriterien für das Archivsystem haben sich geändert (siehe OPS.1.2.2.M14 *Regelmäßige Beobachtung des Marktes für Archivsystemen*).
- Kryptografische Verfahren, Produkte bzw. Schlüssel müssen durch neue abgelöst werden (siehe OPS.1.2.2.M16 *Regelmäßige Aufbereitung von kryptographisch gesicherten Daten bei der Archivierung*).

Aussonderung

Bei der Außerbetriebnahme und Aussonderung von Archivsystemen und -medien sind verschiedene Maßnahmen zu ergreifen, damit weder wichtige Daten verloren gehen noch sensible Daten zurückbleiben. Entsprechende Sicherheitsempfehlungen finden sich in den Bausteinen CON.6 *Löschen und Vernichten* und OPS.1.2.7 *Verkauf/Aussonderung von IT*.

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Archivierung" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

OPS.1.2.2.M1 Ermittlung von Einflussfaktoren für die elektronische Archivierung [Informationssicherheitsbeauftragter (ISB)]

Bevor eine Entscheidung getroffen werden kann, welche Verfahren und Produkte für die elektronische Archivierung eingesetzt werden sollen, müssen die für den Anwendungsfall relevanten technischen, rechtlichen und organisatorischen Einflussfaktoren ermittelt und ins Archivierungskonzept übernommen werden.

Ermittlung der technischen Einflussfaktoren

Um die technischen Einflussfaktoren zu ermitteln, sollten die Eigentümer der zu archivierenden Dokumente befragt werden, also beispielsweise die Verantwortlichen der einzelnen IT-Systeme bzw. IT-Anwendungen und die Systemadministratoren. Die Ergebnisse sind nachvollziehbar im Archivierungskonzept (siehe OPS.1.2.2.M2 *Entwicklung eines Archivierungskonzepts*) zu dokumentieren.

Maßgebliche technische Einflussfaktoren für die elektronische Archivierung sind unter anderem:

- das zu erwartende Datenaufkommen,
- die Dateiformate der zu archivierenden Inhaltsdaten, Metadaten sowie Beweisdaten (z. B. beweisrelevante Daten, z. B. Signaturen, Siegel, Zeitstempel bzw. technische Beweisdaten (Evidence Records)),
- das Änderungsvolumen und die Versionierung,
- die Aufbewahrungsdauer und Löschvorgaben der Dokumente,
- die Zahl und Art der Zugriffe,
- die vorhandene IT-Einsatzumgebung sowie
- zu beachtende Normen und Standards.

Die angegebenen Einflussfaktoren sind nachfolgend detaillierter dargestellt:

Zu erwartendes Datenaufkommen

Ein wesentliches Auswahlkriterium für elektronische Archivsysteme ist die Größe der zu archivierenden Dateien und das in Zukunft zu erwartende Datenaufkommen. Dies kann typischerweise nur großzügig abgeschätzt werden. Die Dateigröße von Dokumenten hängt dabei auch sehr stark vom Dateiformat und dem Umfang der Rendition (siehe weiter unten) ab.

Dateiformate der zu speichernden Dokumente

Je nach Wahl des Archivsystems könnten in diesem grundsätzlich alle verwendeten Dateiformate abgelegt werden, z. B. die in Büroumgebungen üblichen Formate (DOCX, PDF, RTF, ASCII, ZIP, ODT etc.) oder auch Bild- und Tondateien (JPG, GIF, WAV, MPEG etc).

Um allerdings den Aufwand bei der Erhaltung der langzeitgespeicherten Dokumente wirtschaftlich sinnvoll zu gestalten, sollten die in die Langzeitspeicherung zu übernehmenden Dokumente in ein geeignetes Format überführt werden.

Für herkömmliche Textdokumente empfiehlt es sich, diese in den jeweils aktuellen und anforderungsgerechten Standard von PDF/A umzuwandeln. Für spezifische Formate, für die das nicht möglich oder sinnvoll ist, sollte geprüft werden, welche alternativen langzeitspeicherfähigen Formate infrage kommen. Um diese Dokumente zu erhalten, muss jedoch regelmäßig geprüft werden, ob sie noch lesbar sind. Ist das nicht der Fall bzw. zeichnet sich das ab, müssen sie in neuere Formate konvertiert werden.

Weitere langzeiterhaltende Maßnahmen sind in OPS.1.2.2.M9 *Auswahl geeigneter Datenformate für die Archivierung von Dokumenten* detailliert beschrieben.

Bei der elektronischen Archivierung haben sich in der Vergangenheit mehrere Dateiformate etabliert, die unterschiedlich für künftige Verwendungszwecke der Dokumente geeignet sind. Häufig kann oder soll jedoch der spätere Verwendungszweck nicht festgelegt werden. In so einem Fall ist aber nicht vorhersagbar, welches das beste Datenformat für die spätere Verwendung ist. Ebenso häufig bestehen bereits zum Zeitpunkt der Datenspeicherung konkurrierende Anforderungen an die Wahl des Dateiformates, die sich aus den unterschiedlichen Verwendungszwecken ergeben. Deshalb hat es sich, vor allem bei der Langzeitspeicherung, als vorteilhaft erwiesen, Dokumente in mehreren Dateiformaten gleichzeitig zu archivieren. Die Dokumente müssen dazu vorher konvertiert werden. Dieser Vorgang wird als Rendition bezeichnet. Bei der Rendition ist jedoch auf eine genaue Dokumentation der Verfahrensweise zu achten. Informationen über das Originalformat müssen mit archiviert werden. Außer den Inhaltsdaten müssen meistens begleitende Beschreibungs- und Beweisdaten mitgespeichert werden.

Das hierfür notwendige Archivinformationspaket (engl. Archival Information Packet - AIP) soll in einer selbsttragenden Form alle zur Erfüllung des Aufbewahrungszwecks notwendigen Informationen bis zum Ablauf der geltenden Aufbewahrungsfristen in einer möglichst hard- und softwareneutralen Form beinhalten. Dabei geht es primär um die Inhaltsdaten (die aufzubewahrenden Daten [1-n] selbst), beschrieben durch die notwendigen Metadaten (sowohl fachliche als auch technische Metadaten) und die zum Nachweis der Authentizität, Integrität sowie Vertraulichkeit notwendigen Daten. Es ist dabei entscheidend eine ausreichende Menge der Metadaten zu erfassen (Kontextsicherung), um den aufbewahrten Vorgang auch in der Zukunft vollständig rekonstruieren zu können.

Für die Meta- und Protokollinformationen hat sich XML als Format und z. B. XDOMEA als Standard für elektronische Akten und Vorgänge etabliert. Beispielsweise kann als XML-Schema für die Meta- und Protokolldaten dabei die jeweils aktuelle Spezifikation von XDOMEA verwendet werden. Als XML-Schema für das AIP zur Aufnahme der beschreibenden Informationen der aufzubewahrenden Dokumente selbst sowie der beweisrelevanten Daten und technischen Beweisdaten empfiehlt es sich die Vorgaben des BSI gemäß BSI TR-03125, siehe [TR-ESOR-F] zu verwenden. Damit ist ein Informationspaket für den Zeitraum der Langzeitspeicherung verfügbar, das alle notwendigen Informationen (Meta- und Primärinformationen) umfasst.

So wird beispielsweise eine Integration von XDOMEA in die Datenpaketstruktur XAIP als selbsttragendes Archivinformationspaket gemäß BSI TR-03125, siehe [TR-ESOR-F] und [TR-ESOR-XB] beschrieben.

Die Rendition von Dokumenten und anschließende Speicherung in mehreren Dateiformaten wirkt sich unmittelbar auf die für die Archivierung notwendige Speicherkapazität aus.

Änderungsvolumen und Versionstiefe

Bei der Archivierung von Daten und Dokumenten ist zu überlegen, welche Änderungen an den Daten im Lauf der Zeit auftreten werden, wie häufig das zu erwarten ist und wie damit zu verfahren ist. Wenn archivierte Daten geändert werden sollen, soll folgendermaßen vorgegangen werden:

- Die neue Version der Daten wird zusätzlich zur ursprünglichen Version archiviert (Versionierung), wobei unter Umständen nur eine maximale Anzahl von Versionen derselben Daten archiviert bleibt. Die Versionstiefe muss eventuell gegen Anforderungen an die Nachvollziehbarkeit geprüft werden.

Institutionsintern oder rechtlich kann eine Versionierung der Daten gefordert werden. Sofern eine Versionierung von Daten vorgenommen wird, muss das sowohl bei der Berechnung der notwendigen Speicherkapazität des Archivsystems als auch bei Aufbau und Struktur des Archivinformationspakets berücksichtigt werden.

Aufbewahrungsdauer der Daten und Dokumente

Für die Kalkulation der notwendigen Speicherkapazität des Archivsystems ist es unerlässlich abzuschätzen, wie lang die Aufbewahrungsdauer der archivierten Dokumente sein wird. Für die Aufbewahrungsdauer ergeben sich aufgrund rechtlicher oder institutionsinterner Vorgaben minimale, jedoch teilweise auch maximale Fristen, die zu beachten sind.

Die Aufbewahrungsdauer beeinflusst jedoch nicht nur die Speicherkapazität des Archivsystems, sondern auch die Auswahl des Speichermediums sowie dessen Entsorgung nach Ablauf der Aufbewahrungsdauer. Weiterhin wirkt sich die Aufbewahrungsdauer auch auf die Maßnahmen für die digitale Bestandserhaltung aus.

Zahl und Art der Zugriffe

Zugriffszahlen sowie die Art der Zugriffe auf das Archivsystem wirken sich auf die Konfiguration des Archivservers und die Auswahl der Speicherkomponenten aus. Als Einflussfaktoren sind daher zu ermitteln:

- Wie viele Zugriffe werden innerhalb eines vorgegebenen Zeitraums auf das Archivsystem erfolgen?
- Wie hoch ist der Anteil von Schreibzugriffen gegenüber Lesezugriffen?
- Welche Antwortzeiten werden verlangt?
- Erfolgen die Zugriffe direkt von Benutzer- bzw. Clientsystemen auf das Archivsystem?
- Muss das Archivsystem zwischen Zugriffen verschiedener Benutzer unterscheiden oder erfolgt dies durch übergeordnete Komponenten?
- Muss das Archivsystem mehrere, logisch oder physisch voneinander getrennte Archive verwalten (Mandantenfähigkeit)?

IT-Einsatzumgebung

Archivsysteme sind typischerweise in komplexere IT-Landschaften eingebettet. Hierdurch ergeben sich technische Anforderungen, z. B. hinsichtlich

- der Netzanbindung,
- der verwendbaren Netzprotokolle (deren Definition z. B. bekannt sein muss, wenn die Kommunikationsverbindung über Firewalls geführt wird),
- Kompatibilität zu anderen Programmen oder IT-Systemen,
- der Einbindung in Systemmanagement-Umgebungen sowohl zur Administration als auch zur Überwachung des Archivsystems,
- der Administrations- und Nutzungsschnittstellen sowie
- der Antwortzeiten des Archivsystems.

Zu beachtende Normen und Standards

Die im Bereich der Archivierung bestehenden Standards konzentrieren sich auf die Bereiche

- Datenformate und Kompressionsverfahren,
- Architektur,
- Funktionen und Prozesse,
- Schnittstellen zwischen dem Fachverfahren und dem Langzeitspeichersystem, z. B. Schnittstelle S.4 in BSI TR-03125 TR-ESOR, siehe [TR-ESOR-E]
- Speichermedien und deren Aufzeichnungsverfahren sowie
- einzubindende Fachverfahren.

Systemhersteller erhalten durch die Offenlegung von Schnittstellen, die im Rahmen der Standardisierung erfolgt, die Möglichkeit, eine Kompatibilität von Systemkomponenten, Schnittstellen und Datenformaten herzustellen. Deshalb kann durch die Berücksichtigung von Standards bei der Auswahl von Archivsystemen eine längerfristige Planungs- und Investitionssicherheit gewährleistet werden.

Für den Anwender verringern Standards die Abhängigkeit von einzelnen Herstellern, Systemlieferanten und Dienstleistern. Bei den langen Zeiträumen, über die Archivsysteme typischerweise eingesetzt werden, ist dies besonders wichtig, da nicht absehbar ist, wie sich Produktlinien langfristig entwickeln. So könnte sich z. B. bei Insolvenz eines Herstellers proprietärer Speicherkomponenten das Problem ergeben, dass das Archivierungssystem nicht mehr in der bisherigen Art durch Zukauf neuer Speichermedien und -komponenten erweitert werden kann. Behörden und Unternehmen mit hohem Archivierungsbedarf müssen dann typischerweise kurzfristig die Archivdaten migrieren. Bei Einsatz standardisierter Komponenten kann dagegen einfach ein anderer Lieferant für die betroffene Teilkomponente gewählt werden.

Hinsichtlich Standards ist allerdings zu beachten, dass auch diese mit der Zeit aufgrund neuer technologischer Entwicklungen an Relevanz verlieren und eventuell durch neue Standards ersetzt werden. Zudem besteht auch ein Wettbewerb zwischen unterschiedlichen Standardisierungsgremien und Herstellern, wodurch es auch konkurrierende Standards gibt. Insofern empfiehlt es sich auf anerkannte Standards unabhängiger Standardisierungsgremien wie z.B. ISO, ETSI/CEN, DIN oder BSI zu setzen.

Prinzipiell ist die Archivierung jedoch auch ohne Standards und mit proprietären Datei- und Speicherformaten möglich, sofern über den Archivierungszeitraum eine ausreichende Wartung und Systembetreuung durch Hersteller und eine Anpassung der Schnittstellen an sich verändernde Anforderungen sichergestellt wird. Es wird jedoch empfohlen, sich bei der Planung von Archivsystemen eng an geltenden Standards für Dateiformate und Schnittstellen zu orientieren.

Bereits bei der Planung eines Archivsystems sollte eine spätere Migration berücksichtigt werden, da sich bei der langfristigen Speicherung von Daten typischerweise zwischendurch die Technik oder die Anforderungen ändern. Daher sollten Schnittstellen, Dateiformate und Index-Datenbank besonders sorgfältig ausgewählt werden. Auch sollten alle Entscheidungen nachvollziehbar dokumentiert werden.

Weitere Empfehlungen enthält die BSI TR-03125 (siehe [TR-ESOR]) hinsichtlich des Einsatzes offener, interoperabler und standardisierter Datenformate BSI TR-03125 (siehe [TR-ESOR-F], insbesondere Kap. 3) und herstellerunabhängiger interoperabler Schnittstellen (siehe [TR-ESOR-E], insbesondere Kap. 3] entsprechend nationaler und internationaler Standards, insbesondere für die Schnittstellen zwischen dem Fachverfahren und dem Langzeitspeichersystem sowie weitere Harmonisierungen in Form einer Profilierung für Bundesbehörden (siehe BSI TR-03125 [TR-ESOR-B] und [TR-ESOR-XB]).

Ermittlung der rechtlichen Einflussfaktoren für die elektronische Archivierung

Für die Aufbewahrung bestimmter Informationen bestehen verschiedene rechtliche Vorgaben. Werden diese nicht eingehalten, kann das zivil- oder strafrechtliche Konsequenzen haben. Daher sollten sich die Verantwortlichen informieren, welche rechtlichen Vorgaben zu beachten sind. Hieraus ergeben sich Anforderungen, die im Archivierungskonzept berücksichtigt werden müssen. Das betrifft unter anderem

- die Mindestaufbewahrung aus rechtlichen Gründen,
- Höchstaufbewahrungsdauer aus Datenschutzgründen,
- Zugriffsrechte für Externe, z. B. Steuerbehörden oder Gerichte,
- Beweiswerterhaltung elektronischer Dokumente,Umgang mit ersetzend gescannten oder signierten Eingängen,
- Vorlage von Daten bei Prüfbehörden, Gerichten, Dritten,
- Auswertbarkeit oder Reproduzierbarkeit von Daten, z. B. im Forschungsumfeld,
- Anbietungspflicht gemäß Archivrecht gegenüber öffentlichen Archiven sowie
- Qualität von eingesetzten elektronischen Signatur- oder Siegel- oder Zeitstempel-Algorithmen bzw. Verfahren für technische Beweisdaten (engl. Evidence Records).

Die anzuwendenden rechtlichen Grundlagen sind im Einzelfall zu klären.

Im Folgenden werden einige Quellen genannt, die in Deutschland typischerweise zu berücksichtigen sind:

- Bürgerliches Gesetzbuch (BGB)
  Hier werden insbesondere Anforderungen an die Rechtsgültigkeit von Dokumenten im Zivilrecht gestellt. Das BGB definiert auch Verjährungsfristen, z. B. für Schadenersatz aus unerlaubter Handlung.
- Zivilprozessordnung (ZPO)
  Analog zum BGB wird durch die ZPO geregelt, welche Dokumente als Urkunde anerkannt werden müssen, beispielsweise aufgrund einer eigenhändigen Unterschrift oder einer qualifizierten elektronischen Signatur.
- Handelsgesetzbuch (HGB)
  Hier werden Anforderungen an die Ordnungsmäßigkeit und Revisionsfähigkeit der Geschäftstätigkeit gestellt. Dies umfasst auch bestimmte Aufbewahrungsfristen für Geschäftsdokumente.
- Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD).
- Fachvorschriften, z. B. Luftfahrt, Gesundheitswesen, Zulassungsrecht, Forschung, Atomrecht.
- Gesetz zur Durchführung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Durchführungsgesetz), siehe [EIDAS-DG].
- Vertrauensdienstegesetz (siehe [VDG]) als Artikel 1 des eIDAS-Durchführungsgesetzes (siehe [EIDAS-DG]).
- Verordnung (EU) Nr. 910/2014 des europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktion im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, siehe [EIDAS-VO].
- eIDAS-Durchführungsbeschlusses (EU) 2015/1506
- Verordnung (EU) 2016/679 des europäischen Parlaments und des vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

Weiterhin gibt es Gesetze und Vorschriften, die speziell für Behörden und in der Verwaltung zu beachten sind, beispielsweise:

- Verwaltungsverfahrengesetz (VwVfG)
  Definiert grundsätzliche Zulässigkeit der Übermittlung elektronischer Dokumente sowie den Einsatz von QES des Personalausweises/elektronischen Aufenthaltstitels bzw. De-Mail mit Absenderbestätigung als Ersatz der angeordneten Schriftform.
- Verwaltungsgerichtsordnung (VwGO)
  Grundsätzliche Zulässigkeit der Verwendung einer elektronischen Akte sowie die Übertragung der Dokumente in einer elektronischen Form im Bereich der Prozessakten.
- Bundesarchivgesetz und die entsprechen Landesarchivgesetze,
  Aussonderung digitaler Unterlagen und deren Archivierung im Bundesarchiv. Ein Leitfaden. Version 1.2. Bundesarchiv 2010

- E-Government-Gesetz vom 25. Juli 2013 (BGBl. I S. 2749)
  §§ 6 und 7 EGovG fordern die elektronische Aktenführung inkl. Scannen und Langzeitaufbewahrung nach dem "Stand der Technik", mit Verweis auf TR-ESOR und TR RESISCAN, Landesgesetze folgen.

Darüber hinaus gibt es weitere zahlreiche gesetzliche und institutionsinterne Regelungen (z. B. Vorschriften für Sozialversicherungsträger, Krankenhäuser, Pharmaindustrie, Militär oder Kreditwesen), die ermittelt werden müssen. Wesentliche Regelungskriterien sind üblicherweise die Aufbewahrungsdauer sowie der Vertraulichkeits- und Integritätsbedarf.

Für die öffentliche Verwaltung besteht darüber hinaus die gesetzliche Verpflichtung, auch in digitaler Form vorliegende Dokumente nach Ablauf der geltenden Aufbewahrungsfristen den zuständigen Archiven zur Übernahme anzubieten (Anbietungspflicht, siehe Archivgesetz Bund für Bundesbehörden sowie entsprechende Landesarchivgesetze).

Ermittlung der organisatorischen Einflussfaktoren für die elektronische Archivierung

Für die elektronische Archivierung gibt es eine Reihe von organisatorischen Einflussfaktoren, die bei der Konzeption des Archivsystems berücksichtigt werden müssen. Dazu gehören unter anderem

- der Zeitraum des Einsatzes des Archivsystems,
- die Aufbewahrungsfristen,
- der Vertraulichkeitsbedarf der Dokumente,
- der Verfügbarkeitsbedarf der Dokumente
- der Integritätsbedarf der Dokumente
- der Authentizitätsbedarf der Dokumente
- die Verkehrsfähigkeit der Dokumente
- die Festlegung akzeptabler Antwortzeiten,
- der Personalaufwand,
- die Kenntnisse und IT-spezifischen Qualifikationen der Benutzer,
- die Ergonomie und Bedienfreundlichkeit des Archivsystems und
- die finanziellen Randbedingungen.

Die angegebenen Einflussfaktoren sind nachfolgend detaillierter dargestellt.

Um entsprechend lange Aufbewahrungsfristen abdecken zu können, wird empfohlen, das elektronische Archiv nach dem geltenden Stand der Technik und basierend auf den aktuellen Standards und Normen aufzusetzen. Die Implementierung der einzelnen Prozesse des OAIS-Modells (Übernahme, Datenmanagement, Speicherung, Zugriff, Planung der digitalen Bestandserhaltung und Administration), sowie Aufbewahrung der archivierten Daten in Form von selbsttragenden Archivinformationspakete (X)AIP (mit Inhaltsdaten, Metadaten sowie Beweisdaten) und Anwendung der Maßnahmen für die Beweiswert-Erhaltung garantieren einen beweissicheren Umgang mit gespeicherten Daten.

Einsatzzeitraum des Archivsystems

Die Einsatzdauer eines Archivsystems ist getrennt von der Zeitdauer der Archivierung zu kalkulieren. Es ist eine Abschätzung vorzunehmen, über welchen Zeitraum das konkret auszuwählende System betriebsbereit sein soll. Dies wirkt sich auf die Auswahl der Komponenten und speziell auf die geforderte Lebensdauer der Komponenten aus. Ein langer Zeitraum impliziert die Auswahl langlebiger IT-Komponenten sowie die Gestaltung entsprechender Service- und Lieferverträge, die typischerweise mit höheren Kosten verbunden sind. Ein kurzer Zeitraum impliziert eine frühere Migration des Archivs auf ein neues Archivsystem.

Vertraulichkeitsbedarf der

Bei der Bestimmung des Vertraulichkeitsbedarfs ist vor allem zu beachten, dass er sich während der Archivierungsfrist ändern kann. Hierbei können wirtschaftliche und juristische Einflussfaktoren eine Rolle spielen. Typischerweise ist davon auszugehen, dass der Vertraulichkeitsbedarf im Lauf der Zeit abnimmt (insbesondere im Falle einer Aussonderung der Daten in ein historisches Archiv).

Wenn ein langfristiger Schutz der Vertraulichkeit gefordert wird, so hat das Einfluss auf die organisatorische Gestaltung des Archivierungskonzepts (siehe OPS.1.2.2.M15 *Regelmäßige Aufbereitung von kryptographisch gesicherten Daten bei der Archivierung*) und die Auswahl technischer Komponenten.

Verfügbarkeitsbedarf der

Die elektronische Archivierung wird typischerweise zur langfristigen Aufbewahrung von Daten und Dokumenten eingesetzt. Hierbei ist als wesentliche Anforderung in einem der vorigen Punkte bereits festgelegt worden, für welchen Zeitraum die betreffenden Daten zu archivieren sind.

Daneben ist festzulegen, welche weitergehenden Anforderungen an die Verfügbarkeit zu stellen sind, z. B. die Ausfallsicherheit des Archivsystems, die Stabilität der verwendeten Speichermedien oder die Informationserhaltung der Daten.

Integritätsbedarf der

Die Integrität elektronisch archivierter Daten und Dokumente muss typischerweise auch nach einer langen Aufbewahrungsdauer noch sichergestellt und prüfbar sein (z. B. bis zum Ablauf der Aufbewahrungsfristen). Hierbei ist insbesondere davon auszugehen, dass bei langen Aufbewahrungsfristen die Ursprungsverfahren und -daten und weitere Kontextinformationen zwischenzeitlich nicht mehr existieren, so dass die Integritätsprüfung sowohl durch die Aufbewahrung von Kontextinformationen im Archivinformationspaket als auch durch Maßnahmen zur Informations- und Beweiswerterhaltung im Zusammenspiel mit dem Archivsystem bereitgestellt werden muss.

Es muss neben der Klassifizierung des Integritätsbedarfs (z. B. niedrig bis mittel, hoch oder sehr hoch) festgelegt werden, über welchen Zeitraum dies prüfbar sein soll.

Die Integrität der aufbewahrten Daten kann durch selbsttragende Archivinformationspakete (AIP) in Verbindung mit der Umsetzung der Anforderungen der Beweiswerterhaltung (siehe z. B. BSI TR-03125 [TR-ESOR]) dauerhaft gesichert werden.

Authentizitätsbedarf der

Analog zur Integrität muss auch der Authentizitätsbedarf und der Zeitraum (gemäß der Aufbewahrungsfrist) festgelegt werden, innerhalb dessen die Authentizität von Daten prüfbar sein muss. Auch hier ist davon auszugehen, dass typischerweise nach einer längeren Archivierungsdauer die Ursprungsverfahren bzw. -daten und Kontextinformationen zwischenzeitlich nicht mehr existieren. Die Authentizitätsprüfung muss also ebenso vor allem durch die Umsetzung der Maßnahmen zur Beweiswerterhaltung (siehe z. B. BSI TR-03125 [TR-ESOR]) dauerhaft gesichert werden.

Verkehrsfähigkeit der

Bei einer gerichtlichen Auseinandersetzung müssen die aufbewahrten Daten eventuell dem Gericht vorgelegt werden. Es müssen dabei nicht nur Inhaltsdaten, sondern auch Begleitdaten, z. B. Beweisrelevante Daten und technische Beweisdaten, sowie Metadaten in einer für das Gericht "verkehrsfähigen" Form vorgelegt werden, die die Anwendung der notwendigen Informations- und Beweiswert-Erhaltungsmaßnahmen während der Aufbewahrungszeit belegen. Hierzu wird die Verwendung selbsttragender AIPs sowie die Anwendung der Beweiswerterhaltung nach BSI TR-3125 [TR-ESOR] empfohlen.

Bestimmung akzeptabler Antwortzeiten

Zwischen der Anfrage an ein Archivsystem und der Antwort ergibt sich eine Verzögerung (Antwortzeit). Die Anforderungen an diese Verzögerung werden typischerweise durch eine zu erzielende mittlere und eine maximal akzeptable Antwortzeit definiert.

Die Antwortzeit ist nach unterschiedlichen Faktoren zu charakterisieren, z. B.

- die Zeitdauer bis zur Reaktion des Archivsystems bei einer Anfrage,
- die Zeitdauer bis zur Speicherbestätigung des Archivsystems und
- die Zeitdauer bis zur vollständigen Übertragung der gewünschten Daten an das Clientsystem.

Die geforderte Antwortzeit hängt dabei sehr stark vom Einsatzszenario ab. So können z. B. bei einer Recherche in Altdatenbeständen eines Enterprise Resource Planning (ERP)-Verfahrens durchaus Reaktionszeiten im Stundenbereich innerhalb der Regelarbeitszeit akzeptabel sein.

Typischerweise ergeben sich auch subjektive Anforderungen an die Antwortzeiten. So kann z. B. eine hohe Reaktionszeit auf Suchanfragen oder beim Öffnen archivierter Dokumente als störender empfunden werden als eine gleich lange Zeitdauer bis zur Speicherbestätigung bei der Ablage von Daten im Archiv.

Die Anforderungen an die Antwortzeit sind zu ermitteln und zu dokumentieren.

Personalaufwand

Der Personalaufwand für den Betrieb des Archivsystems beeinflusst wesentlich die Auswahl des Systems. Es ist zu ermitteln, welcher zusätzliche Personalaufwand und welche zusätzliche individuelle Belastung des Personals durch die Archivierung als tragbar angesehen werden.

Dies wirkt sich auf die künftige Personalplanung aus, da eventuell zusätzliches Personal erforderlich ist. Die Rollen Archivverwalter, Archivadministrator und (technischer) Benutzer sind mindestens zu besetzen. Wenn im laufenden Betrieb zu wenig Personal verfügbar ist, muss die fehlende Personalkapazität durch externe Wartungs- und Serviceverträge kompensiert werden.

Kenntnisse und IT-spezifische Qualifikationen der Benutzer

Die Auswahl geeigneter Bedienschnittstellen des Archivsystems wird unter anderem von den Vorkenntnissen der vorgesehenen Benutzer beeinflusst. Hier sollte ermittelt werden, welche IT-spezifischen Fachkenntnisse vorliegen.

Dies hat auch Einfluss auf Dienstleistungen im Umfeld der Archivierung, etwa die Organisation einer Benutzerunterstützung (Helpdesk) oder die Erweiterung des Helpdesks zur Unterstützung des Archivsystems.

Alle Benutzer müssen im Umgang mit dem Archivsystem geschult werden. Die erforderliche Schulung muss in den Gesamtkosten berücksichtigt werden.

Ergonomie und Bedienfreundlichkeit des Archivsystems

Je einfacher ein Archivsystem zu bedienen ist, desto besser akzeptieren es die Benutzer. Auch gehen sie dann eher ordnungsgemäß mit dem System um.

Neben gesetzlichen Anforderungen zur Ergonomie an Arbeitsplätzen ist hierbei auch der subjektive Eindruck von Benutzern zu berücksichtigen. Um die entsprechenden Anforderungen zu ermitteln, können die zukünftigen Benutzer z. B. befragt werden. Es sollten jedoch auch Erfahrungen aus Pilot- und Testinstallationen der vorgesehenen Archivsystem-Komponenten einfließen.

Im Falle eines Langzeitspeichers handelt sich gewöhnlich um einen nachgeordneten Dienst, der durch eine Geschäftsanwendung angesteuert wird. Deshalb ist diese Anforderung zweitrangig.

Finanzielle Randbedingungen

Die Einführung von Archivsystemen und die Gestaltung eines entsprechenden organisatorischen Rahmens werden typischerweise von den anfallenden Kosten beeinflusst:

- einmalige Investitionen,
- laufende Kosten, inklusive Personalkosten,
- Lizenzgebühren.

Die technische Planung von Archivsystemen wird daher typischerweise von einer Finanzplanung begleitet. Hierbei sind die institutionsinternen Regelungen (Budgetplanung, Verteilung von Kostenstellen etc.) zu berücksichtigen. Die notwendigen Schulungen für Benutzer und Administratoren müssen in die Kalkulation der Gesamtkosten einbezogen werden.

OPS.1.2.2.M2 Entwicklung eines Archivierungskonzepts [Informationssicherheitsbeauftragter (ISB)]

Um eine elektronische Archivierung in einer Institution einzuführen, sind die Ziele festzulegen, die damit erreicht werden sollen. Dabei muss das Management der betreffenden Institution einbezogen werden. Eventuell müssen die Ziele auch mit übergeordneten Organisationseinheiten koordiniert werden. Insbesondere ist festzulegen,

- welche Regularien (Compliance) einzuhalten sind (rechtlich-organisatorischer Rahmen),
- in welchen Bereichen bzw. für welche Prozesse welche Daten in welcher Form archiviert werden sollen,
- welches Sicherheitsniveau es zu erreichen gilt,
- welcher Funktions- und Leistungsumfang angestrebt ist und
- wer die Verantwortung hierfür trägt.

Die Ergebnisse sind im Archivierungskonzept zu fixieren.

Welche Regularien (Compliance) sind bei der Archivierung zu berücksichtigen?

Welche Informationen archiviert werden, ist auch von den gesetzlichen und vertraglichen Rahmenbedingungen der Institution abhängig. Dabei spielen vorgeschriebene Speicher- und Löschfristen für Daten eine entscheidende Rolle, die sich aus verschiedenen Gesetzen und Regelungen ergeben können (siehe hierzu auch OPS.1.2.2.M1 *Ermittlung von Einflussfaktoren für die elektronische Archivierung*). Ziel der Archivierung ist es unter anderem Nachweispflichten zu erfüllen, die sich aus Compliance-Vorgaben ergeben. Die Informationserhaltung gilt beispielsweise sowohl für die Langzeitspeicherung als auch für die historische Archivierung, wobei die Beweiswerterhaltung insbesondere im Falle eines Langzeitspeichers zu berücksichtigen ist.

Welche Daten sind zu archivieren?

Von den zu archivierenden Daten hängt ab, welche technischen Anforderungen das zukünftige Archivsystem erfüllen muss. Die Eingrenzung sollte aber so allgemein erfolgen, dass ausreichend Spielraum für die technische Ausgestaltung bleibt. Dabei ist aber zu beachten, dass sich Anforderungen im Laufe der Zeit auch ändern können, z. B. im Rahmen des OAIS-Referenzmodells: Planung der digitalen Bestanderhaltung (engl. Preservation Planning). Besonders auf Managementebene sind allgemeine Charakterisierungen sinnvoll wie:

- Daten/Dokumente der Abteilung,
- Daten/Dokumente der Geschäftsprozesse,
- Geschäftsdaten,
- Buchhaltungsdaten,
- Kundendaten sowie
- Daten der Klassifikationsstufe.

Wenn Daten mit unterschiedlichem Schutzbedarf archiviert werden sollen, wird empfohlen, die Ziele und Anforderungen an die Archivierung anhand der jeweiligen Schutzbedarfskategorie zu definieren. Ein Beispiel hierfür ist die Archivierung von Daten, die als offen, intern, vertraulich etc. klassifiziert worden sind.

Welches Sicherheitsniveau soll erreicht werden?

Das zu erreichende Sicherheitsniveau bei der Archivierung lässt sich auf Managementebene typischerweise wie folgt charakterisieren:

- Erfüllung gesetzlicher sowie institutionsinterner Anforderungen an den Schutz der Daten bei der Archivierung sowie darüber hinaus (z. B. nach Entsorgung der Datenträger),
- Widerstandsfähigkeit des Archivierungsprozesses gegen Manipulation,
- Informations- und Beweiswerterhaltung der archivierten Daten,
- Widerstandsfähigkeit des verwendeten Archivsystems gegen interne und externe Angriffe auf die gespeicherten Daten sowie das IT-System selbst.

Wenn Daten und Dokumente klassifiziert werden, kann das Sicherheitsniveau auch anhand dieser Klassifikation detaillierter differenziert werden.

Welcher Funktions- und Leistungsumfang soll erreicht werden?

Der angestrebte Funktions- und Leistungsumfang elektronischer Archivierung kann je nach Institution unterschiedlich ausfallen. Üblicherweise werden auf Managementebene die folgenden Anforderungen definiert:

- Integrationsfähigkeit in die bestehende IT-Systemlandschaft,
- Integrationsfähigkeit in bestehende Prozesse,
- Einhaltung (gesetzlich sowie intern) vorgeschriebener Aufbewahrungs- und Löschfristen für Daten,
- Erfüllung der Informations- und Beweiswert-Erhaltungsaufgaben,
- Aussonderungsmodalitäten und Beachtung der Anbietungspflicht.

Dies betrifft vor allem die öffentliche Verwaltung, da öffentliche Stellen dazu verpflichtet sind, alle Unterlagen, die sie für die laufende Aufgabenerfüllung nicht mehr benötigen (i. d. R. nach Ablauf der geltenden Aufbewahrungsfrist) einem dafür zuständigen Archiv anzubieten (z. B. Übergang aus einem Langzeitspeicher, in ein historisches Archiv). Erst wenn das zuständige Archiv entscheidet, dass die entsprechenden Daten nicht archivwürdig sind oder deren Übernahme durch das zuständige Archiv erfolgt ist, dürfen diese endgültig gelöscht werden. Über die Archivwürdigkeit von Daten kann in vielen Fällen erst nach Ablauf der Aufbewahrungsfrist entschieden werden, sodass die Daten am Ende der Aufbewahrungsfrist nicht immer automatisch gelöscht werden können.

- Einhaltung des angestrebten Sicherheitsniveaus der Daten sowie
- Migrationsfähigkeit des Archivsystems sowie der archivierten Daten, wenn sich Anforderungen und Einflussfaktoren ändern, z. B. im Rahmen der OAIS: Planung der digitalen Bestandserhaltung (engl. Preservation Planning).

Wer trägt die Verantwortung?

Es müssen Mitarbeiter benannt werden, die dafür verantwortlich sind, die elektronische Archivierung aufzubauen und zu betreiben. Üblicherweise beauftragt das Management eine Fachabteilung bzw. deren Leiter mit der Umsetzung der Archivierung. Hiermit müssen auch Zielvorgaben, Befugnisse, personelle und finanzielle Ressourcen verknüpft werden. Die Delegation der Umsetzung ist entsprechend den institutionsinternen Richtlinien durchzuführen und im Archivierungskonzept zu fixieren. Es ist zu beachten, dass im Falle der Archivierung bis zum Ablauf der Aufbewahrungsfristen die zuständige Fachabteilung die Datenhoheit und damit die fachliche Verantwortung für die Archivierung besitzt.

Entwicklung des Archivierungskonzepts

Der Aufbau eines Archivsystems sollte sorgfältig konzipiert werden. Dabei sind einerseits zahlreiche Einflussfaktoren (z. B. institutionsinterne oder rechtliche Vorgaben, technische und organisatorische Umgebungsbedingungen) zu beachten, andererseits bestehen vielfältige technische Möglichkeiten, um ein elektronisches Archiv aufzubauen. Daher sollte zunächst ein Konzept entwickelt werden, in dem alle Einflussgrößen und Entscheidungskriterien für die Wahl eines konkreten Archivierungssystems und der entsprechenden Produkte berücksichtigt werden.

Im Archivierungskonzept ist der technische bzw. organisatorische Einsatz des Archivsystems festzulegen, also z. B.

- Zuständigkeiten und Verantwortlichkeiten,
- Definition von Benutzerrollen (z. B. Archivverwalter, Administratoren, Benutzer, technische Benutzer),
- Definition von Zugriffsrechten und Modalitäten zur Rechtevergabe,
- die notwendigen Prozesse und Funktionen,
- Auswahl der zu archivierenden Daten,
- Form und Struktur der im Archiv abzulegenden Daten,
- Schutz der archivierten Daten, z. B. indem sie verschlüsselt bzw. signiert bzw. gesiegelt bzw. zeitgestempelt werden,
- angestrebte Systemanbindung bzw. die Einsatzbedingungen für Archivierungskomponenten,
- technische Ausgestaltung des Archivsystems,
- Integration des Archivsystems in die bestehende IT-Infrastruktur,
- Betrieb des Archivsystems, z. B. Beschreibung von Service Level Agreements.

Die Ergebnisse sollen aktualisierbar und erweiterbar schriftlich dokumentiert werden. Das Archivierungskonzept selbst sollte in allen umgesetzten Fassungen aufbewahrt werden. Die Mitarbeiter sind über den sie betreffenden Teil des Konzepts zu unterrichten. Dies sollte nachprüfbar dokumentiert werden.

Wie sich ein Archivierungskonzept aufbauen lässt, zeigt beispielhaft das nachfolgende Inhaltsverzeichnis:

Inhaltsverzeichnis Archivierungskonzept

- - Vertragsgestaltung
  - Maßnahmen der Bestandserhaltung (z. B. Refresh-Zyklen für die Speichermedien, Beobachtung der technischen Entwicklung der eingesetzten Datenformate, Produkte und Techniken)
  - Bestandsverzeichnis
  - Löschen von Daten
  - Vernichtung von unbrauchbaren Datenträgern
  - Vorhalten von arbeitsfähigen Lesegeräten

Bei der elektronischen Archivierung handelt es sich nicht um eine einmalige Aufgabe, sondern um einen dynamischen Prozess. Ein Archivierungskonzept muss daher regelmäßig den aktuellen Gegebenheiten angepasst werden, z. B. Planung der digitalen Bestandserhaltung (engl. Preservation Planning) gemäß dem OAIS-Modell.

OPS.1.2.2.M3 Geeignete Aufstellung von Archivsystemen und Lagerung von Archivmedien [IT-Betrieb, Leiter IT]

Da in Archivsystemen wichtige Behörden- bzw. Unternehmensdaten konzentriert aufbewahrt werden, müssen deren IT-Komponenten in gesicherten Räumen aufgestellt werden, die nur berechtigte Personen betreten dürfen. Dies betrifft neben den eingesetzten Servern und Netzkomponenten insbesondere die Speichereinheiten (Plattenarrays, Bandlaufwerke etc.).

Für die geeignete Aufstellung dieser IT-Komponenten sind alle relevanten Maßnahmen, die im IT-Grundschutz-Kompendium zur Infrastruktur-Sicherheit beschrieben sind, zu realisieren. Je nach Art und Größe des Speicher- oder Archivsystems sind die Bausteine INF.1 *Allgemeines Gebäude*, INF.2 *Rechenzentrum*, INF.5 *Serverraum* bzw. INF.6 *Schutzschrank* heranzuziehen. Hierbei sollte besonders darauf geachtet werden, dass die infrastrukturellen Komponenten (Stromzufuhr etc.) ausreichend zuverlässig sind. Wenn Speichersysteme eingesetzt werden, sind zudem angemessene Redundanzen in der technischen Infrastruktur zu schaffen, um die Verfügbarkeit dieser zentralen Ressourcen so gut wie möglich zu unterstützen.

Für die langfristige Aufbewahrung der verwendeten Archiv-Speichermedien sind die unten genannten Lagerbedingungen einzuhalten (siehe Abschnitt Geeignete Lagerung von Archivmedien). Vor allem die zweckmäßige Klimatisierung von Speichermedien, aber auch der Archivsysteme selbst, sind hier zu beachten.

Häufig werden elektronische Archive so realisiert, dass auf Archivmedien dauerhaft durch die Speichereinheit zugegriffen werden kann. Hierfür werden vielfach dedizierte Speichereinheiten eingesetzt, die selbsttätig Wechselmedien verwalten und einlegen können, beispielsweise Roboter für Bandlaufwerke oder Jukeboxen für Disc-Medien. Wenn ein Archivsystem solche Komponenten beinhaltet, werden meistens die Archivmedien während ihrer gesamten Lebensdauer nicht mehr aus der Speichereinheit ausgelagert. Das bedeutet, dass die an Archivmedien zu stellenden Lagerbedingungen (bezüglich Klimatisierung, Zugriffsschutz etc.) bereits in der Speicherkomponente erfüllt und überwacht werden müssen.

Wenn das Archivsystem ausgewählt wird, ist daher als Kriterium zu berücksichtigen, dass die erforderlichen Lagerbedingungen für Archivmedien in Speicherkomponenten eingehalten werden können bzw. welcher Zusatzaufwand hierfür entsteht.

Geeignete Lagerung von Archivmedien

Für den Langzeiteinsatz von Archivmedien sind besonders der Zugriffsschutz sowie klimatische Lagerbedingungen zu beachten und deren Einhaltung zu überwachen.

Sofern Archivmedien im Online-Zugriff, also im Archivsystem bzw. in Speicherlaufwerken gehalten werden, kann das Archivsystem nicht vom Archivmedium getrennt werden.

Wenn Archivmedien außerhalb des Archivsystems "offline" gelagert werden, so sind die im Baustein INF.7 *Datenträgerarchiv* beschriebenen Anforderungen unter besonderer Berücksichtigung der Anforderungen an die Klimatisierung anzuwenden.

Klimatisierung

Welche klimatischen Anforderungen erfüllt sein müssen, damit Archivmedien länger halten, hängt von den jeweils eingesetzten Archivmedien selbst ab. Hersteller geben hierzu vereinzelt unverbindliche Hinweise zu den Lagerbedingungen (z. B. hinsichtlich der Temperatur und Luftfeuchte) und zur Haltbarkeit der Medien.

Für den langfristigen Einsatz elektronischer Archivsysteme müssen die konkreten Lagerbedingungen jedoch von den Herstellern der eingesetzten Archivmedien verbindlich erfragt werden. Es sollten folgende Punkte vor der Auswahl der verwendeten Archivmedien geklärt werden (siehe auch OPS.1.2.2.M18 *Verwendung geeigneter Archivmedien*):

- Die klimatischen und physischen Lagerbedingungen für die betrachteten Archivmedien sollten seitens des Herstellers ausreichend detailliert beschrieben sein (inklusive der Auswirkungen auf die maximale Lebensdauer). Diese Angabe sollte verbindlich sein, möglichst mit einer Garantieerklärung des Herstellers bei Einhaltung der Lagerbedingungen.
- Die geeignete Lagerung technisch umzusetzen, kann unter Umständen sehr komplex sein. Je nach den vorhandenen technischen und infrastrukturellen Vorgaben können bestimmte Archivmedien auch gänzlich ungeeignet sein. Daher muss im Vorfeld geprüft werden, ob eine geeignete Lagerung mit vertretbarem Aufwand technisch überhaupt realisierbar ist.

Die Lagerbedingungen sollten im Betriebshandbuch des Archivsystems dokumentiert werden. Zusätzlich muss sichergestellt werden, dass die Lagerbedingungen kontinuierlich eingehalten und überwacht werden.

Physische

Über die klimatischen Bedingungen hinaus müssen die verwendeten Archivmedien vor unautorisiertem Zugriff und mechanischer Beschädigung oder Veränderung geschützt werden. Hierzu wird insbesondere auf die im Baustein INF.7 *Datenträgerarchiv* genannten Anforderungen verwiesen.

Neben Zutrittskontrolle zum Datenträgerraum, Brandschutz und Schutz vor Wassereinwirkung sind je nach Art der verwendeten Archivmedien weitere Maßnahmen zu realisieren, z. B. zum Schutz vor Magnetfeldern. Hierfür sind verbindliche Empfehlungen von Herstellern zu mechanischen Lagerbedingungen einzuholen und zu beachten.

Wenn die Lagerbedingungen nicht eingehalten werden, ist der verantwortliche Mitarbeiter zu alarmieren. Hierzu sind Eskalationsprozeduren und -wege zu definieren.

OPS.1.2.2.M4 Konsistente Indizierung von Daten bei der Archivierung [Benutzer, IT-Betrieb, Leiter IT]

Beim Betrieb eines Archivs ist es wichtig, alle abgelegten Daten, Dokumente und Datensätze bzw. ArchivInformationsPaket (AIP) eindeutig zu referenzieren, um sie bei späteren Archivanfragen korrekt wiederfinden zu können. Zusätzlich können Archivsysteme die Suchanfragen anbieten. Da eine Volltextsuche abhängig von Art und Umfang der archivierten Daten sehr lange dauern kann, können Archivsysteme zu jedem selbsttragenden AIP einen separaten Datensatz mit Indexangaben in einer eigenen Suchdatenbank (Metadaten, vgl. auch Datenmanagement im OAIS-Modell) speichern. Struktur und Umfang der Indexangaben sind in der Regel konfigurierbar und sollten die folgenden Eigenschaften aufweisen:

- Eindeutigkeit: Die Dokumenten-/Datensatzbezeichner müssen eindeutig sein.
- Unterstützung zu erwartender Suchanfragen: Durch die Kontextangaben sollen spätere Suchanfragen beschleunigt werden. Da der spätere Suchkontext nicht feststeht, kann im Vorfeld nur eine Abschätzung späterer Suchanfragen vorgenommen und versucht werden, die Kontextangaben so aussagekräftig wie möglich zu gestalten.
- Geringer Umfang: Ein geringer Umfang an Indexdaten beschleunigt spätere Suchanfragen, jedoch kann ein zu geringer Umfang der Indexdaten Suchanfragen behindern bzw. das Auffinden von Daten erschweren. Der Umfang der Kontextangaben ist letztlich in Abhängigkeit vom erwarteten Datenvolumen festzulegen.

Diese Parameter müssen grundsätzlich vor der Inbetriebnahme des Archivs festgelegt werden. Trotzdem kann es im Laufe der Zeit notwendig werden, die Eigenschaften zu ändern. Je nach Umfang und Art der Änderung der Indexdaten kann dies eine sehr aufwändige Neuindizierung der Archivdatenbestände erforderlich machen.

Der konkrete Kontext für einzelne zu archivierende Dokument kann auf unterschiedliche Art und Weise erzeugt werden. Drei Verfahren werden dabei unterschieden:

- manuelle Erstellung:Über Eingabemasken können Indexangaben zu jedem Dokument manuell erzeugt werden. Hierdurch besteht besonders bei großen Datenmengen die Gefahr, dass inkonsistente Indexangaben erfasst werden.
- halbautomatische Erzeugung:Diese Verfahren automatisieren die Vergabe von Indexdaten, gestatten jedoch eine manuelle Kontrolle und Korrektur.
- vollautomatische Erzeugung:Hierbei werden Indizes vollautomatisch ohne manuelle Eingriffsmöglichkeit vergeben.

Die Wahl des Verfahrens ist abhängig vom erwarteten Datenvolumen. Werden in unregelmäßigen Abständen Informationen archiviert, ist ein manuelles Verfahren auf der Grundlage konkreter Vorgaben zur Erstellung eines Kontextes ausreichend.

Werden regelmäßig große Datenvolumen archiviert, sollte ein halbautomatisches Verfahren zur Erzeugung der Indexdaten gewählt werden. Hier besteht die Möglichkeit, diese Informationen manuell zu kontrollieren und zu korrigieren, bevor die Informationen und die zugehörigen Indexdaten archiviert werden und dann gegebenenfalls nicht mehr nachträglich geändert werden können.

Bei der vollautomatischen Erzeugung der Indexdaten können Fehler nicht erkannt bzw. korrigiert werden. Eine eventuelle Fehlzuordnung von zu archivierenden Daten, z. B. zu Geschäftsprozessen, kann dann nicht erkannt oder ausgeschlossen werden. Dieses Verfahren sollte deshalb nur dann angewandt werden, wenn alle Daten so strukturiert sind, dass alle Indexdaten in jedem Fall zweifelsfrei und zuverlässig extrahiert werden können.

OPS.1.2.2.M5 Regelmäßige Aufbereitung von archivierten Datenbeständen [Leiter IT]

Für eine ordnungsgemäße Archivierung muss über den gesamten Archivierungszeitraum hinweg sichergestellt werden, dass

- das benutzte Datenformat dem Stand der Technik entspricht und von den benutzten Anwendungen derzeit und zukünftig verarbeitet werden kann,
- die gespeicherten Daten auch zukünftig lesbar sind und unter Beibehaltung der Semantik und des Beweiswerts reproduziert werden können,
- das benutzte Dateisystem auf dem Speichermedium von allen beteiligten Komponenten verarbeitet werden kann,
- die Speichermedien jederzeit technisch einwandfrei gelesen werden können,
- die verwendeten kryptografischen Verfahren zur Bewahrung des Beweiswertes kryptografisch signierter Dokumente und/oder der Vertraulichkeit verschlüsselter Dokumente dem Stand der Technik entsprechen und
- für alle Komponenten der Speichereinheit (Speichermedien, Laufwerke, Jukeboxen sowie die Steuersoftware) Ersatz- und Wartungsmöglichkeiten bestehen.

Ist abzusehen, dass eine der geforderten Eigenschaften in naher Zukunft nicht mehr gegeben ist, müssen die betroffenen Systeme ausgetauscht werden. Dabei ist zu berücksichtigen, dass unter Umständen eine erhebliche Menge an archivierten Daten migriert werden muss.

Die Transformation auf aktuelle Datenformate und die Migration auf neuere Speichermedien, IT-Hardware oder IT-Software wird in OPS.1.2.2.M16 *Regelmäßige Erneuerung technischer Archivsystem-Komponenten* beschrieben.

Wie sich verschlüsselte oder signierte Dokumente aufbereiten lassen, wird in OPS.1.2.2.M15 *Regelmäßige Aufbereitung von kryptographisch gesicherten Daten bei der Archivierung* und OPS.1.2.2.M20 *Geeigneter Einsatz kryptographischer Verfahren bei der Archivierung* erläutert.

OPS.1.2.2.M6 Schutz der Integrität der Indexdatenbank von Archivsystemen [IT-Betrieb, Leiter IT]

Die Indexdatenbank ist besonders wichtig, damit ein Archivsystem korrekt funktioniert. In ihr sind die Verweise auf sämtliche archivierten Dokumente bzw. ArchivInformationsPakete (AIP) abgelegt. Fehlende oder beschädigte Einträge in der Indexdatenbank können dazu führen, dass archivierte Dokumente nicht oder nur sehr schwer wiedergefunden und Geschäftsvorgängen zugeordnet werden können. Daher muss für einen ordnungsgemäßen Archivbetrieb die Integrität der Indexdatenbank sichergestellt werden und überprüfbar sein. Zur Integritätssicherung sind folgende Empfehlungen zu berücksichtigen:

Redundante Ablage der Indexeinträge

Abhängig von der Archivgröße sind folgende Abstufungen vorzusehen:

- Bei kleinen Archiven mit geringem Datenaufkommen und geringen Anforderungen an die Antwortzeiten ist es ausreichend, eine tägliche Datensicherung der Indexdatenbank vorzunehmen. Die Datensicherung sollte gemäß Baustein OPS.1.1.6 *Datensicherung* vorgenommen werden.
- Bei Archiven mit hohem Datenaufkommen sowie hohen Anforderungen an die Antwortzeit sollte die Indexdatenbank selbst redundant ausgelegt, d. h. gespiegelt sein. Auch hier ist zusätzlich eine tägliche Datensicherung durchzuführen. Die gespiegelten Teil-Datenbanken sollten in unterschiedlichen Brandabschnitten aufgestellt sein.

Regelmäßige Integritätsprüfung

Die Indexdatenbank sollte regelmäßig (mindestens wöchentlich, bei großen Archiven täglich) geprüft werden, ob sie konsistent und integer ist, z. B. indem Prüfsummen benutzt werden. Alle in der Indexdatenbank referenzierten Dokumente bzw. ArchivInformationsPaket (AIP) müssen auf den Archivmedien auffindbar sein. Integritätsverletzungen müssen dokumentiert und zeitnah behoben werden.

In regelmäßigen Abständen (z. B. monatlich) sollte zudem geprüft werden, ob die Datensicherungen der Indexdatenbank lesbar und wiederverwendbar sind. Bei redundant ausgelegten Datenbanken sollte getestet werden, ob die Funktionsübergabe noch ordnungsgemäß funktioniert, wenn ein Teil ausfällt.

Alle Ergebnisse der regelmäßigen Integritätsprüfung sollten ebenfalls archiviert werden, damit Datenänderungen später nachvollzogen werden können.

OPS.1.2.2.M7 Regelmäßige Datensicherung der System- und Archivdaten [IT-Betrieb, Leiter IT]

Elektronische Archivsysteme unterliegen denselben Risiken hinsichtlich eines Datenverlustes wie andere IT-Systeme auch. Die Auswahl geeigneter Datenträger allein bietet keinen ausreichenden Schutz vor Verlust, beispielsweise bei Zerstörung oder Diebstahl des Archivmediums selbst.

Eine redundante Speicherung der Archivdaten, der zugehörigen Indexdatenbank und der Systemdaten ist daher unerlässlich. Für die Datensicherung ist grundsätzlich die im Baustein OPS.1.1.6 *Datensicherung* beschrieben Vorgehensweise zu verwenden.

Alternativ zu einer Datensicherung der Archivdaten können diese auch redundant auf physisch getrennten und in unterschiedlichen Brandabschnitten aufgestellten Archivsystemen gespeichert werden. Einige Hersteller von Archivsystemen bieten hierzu Hochverfügbarkeitslösungen an. Trotzdem muss auch in diesem Fall die Daten des Archivsystems selbst sowie die Indexdatenbank gesichert werden.

Wenn Datensicherungen wieder in das Archivsystem eingespielt werden, ist zu überprüfen, ob dadurch Datenverluste aufgetreten sind, also ob zu archivierende Daten erneut erfasst werden müssen. Außerdem muss kontrolliert werden, ob für die wieder eingespielten Daten Löschvermerke vorliegen, die berücksichtigt werden müssen.

OPS.1.2.2.M8 Protokollierung der Archivzugriffe [IT-Betrieb, Leiter IT]

Die Zugriffe auf elektronische Archive sind zu protokollieren. Hierdurch soll ermöglicht werden, alle Aktivitäten nachvollziehen und eventuelle Fehler korrigieren zu können. Die folgende Aufzählung gibt einen Überblick darüber, welche Arten von Ereignissen mithilfe der Protokollierung erkannt werden können:

- Vertraulichkeits- bzw. Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer,
- fehlerhafte Administration von Zugangs- und Zugriffsrechten,
- Ausschalten des Servers im laufenden Betrieb,
- Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von Archivsystemen,
- defekte Datenträger,
- Verlust gespeicherter Daten,
- Datenverlust bei erschöpftem Speichermedium,
- Manipulation an Daten oder Software,
- unberechtigtes Kopieren der Datenträger,
- Manipulation eines Kryptomoduls,
- Kompromittierung kryptografischer Schlüssel und
- unberechtigtes Überschreiben oder Löschen von Archivmedien.

Der Umfang der Protokollierung richtet sich einerseits nach den Anforderungen an die Nachvollziehbarkeit und Authentizität der in Archiven gespeicherten Daten. Andererseits müssen auch die institutionsintern abgestimmten Regelungen beachtet werden, z. B. zum Datenschutz.

Sofern möglich, sollten mindestens folgende Daten protokolliert werden:

- Datum und Uhrzeit des Zugriffs,
- Clientsystem, von dem aus zugegriffen wurde,
- Archivbenutzer und ausgeübte Benutzerrolle,
- ausgeführte Aktionen sowie
- eventuelle Fehlermeldungen und -codes.

Im Archivierungskonzept ist festzulegen, wie lange die Protokolldaten aufbewahrt werden sollen. Eventuell können die Protokolldaten mit archiviert werden.

Die Protokolldaten müssen unter Beachtung interner Vorgaben regelmäßig ausgewertet werden, um Missbrauch und Systemfehler zu erkennen. Die Auswertung kann manuell oder mit Unterstützung eines Tools erfolgen. Im Vorfeld sollten kritische Ereignisse definiert werden, also solche, bei deren Auftreten ein Administrator zu benachrichtigen ist. Solche Vorfälle sollten umgehend signalisiert werden, z. B. indem vorhandene Systemmanagement-Umgebungen genutzt werden. Außerdem ist es wichtig, dass die Benachrichtigung rollenbezogen und nicht personenbezogen erfolgt. Wird beispielsweise eine E-Mail an eine konkrete Person geschickt, bleibt die Nachricht eventuell unbeachtet, wenn diese Person nicht anwesend ist.

Folgende Ereignisse weisen bei der Archivierung typischerweise eine hohe Kritikalität auf und sollten daher permanent protokolliert, überwacht und umgehend signalisiert werden:

- Kopieren von Archivmedien,
- Kopieren von Archivsystem-Datenträgern,
- Löschen oder Löschmarkierung von Datensätzen,
- Offline-Schaltung von Archivmedien in Archivsystemen,
- Entnahme von Archivmedien aus dem Archivsystem,
- Einlegen von Archivmedien,
- Online-Schalten von Archivmedien,
- Fehler oder Probleme beim Zugriff auf das Archiv,
- Systemfehler und Timeouts,
- Katastrophenszenarien (Brand, unzulässige Temperatur, Wasser etc.), die in der Regel durch externe Sensorik gemeldet werden.

Nachdem ein Ereignis signalisiert wurde, sollte es sofort geprüft und gegebenenfalls weiter eskaliert werden. Typischerweise erfolgt eine erste Eskalation an den Leiter IT. Es können aber auch andere Eskalationsprozesse vorgesehen werden.

OPS.1.2.2.M9 Auswahl geeigneter Datenformate für die Archivierung von Dokumenten [IT-Betrieb, Leiter IT]

Grundsätzlich können in den Archiven Dokumente jeglicher Art abgelegt werden, z. B. DOCX, RTF, XLSX, ZIP. Um allerdings langzeitgespeicherte Dokumente wirtschaftlich sinnvoll erhalten zu können, sollten sie in ein geeignetes Format (siehe z. B. [TR-ESOR-F]) überführt werden.

Für herkömmliche Textdokumente empfiehlt es sich, diese in einen passenden Standard der PDF/A-Formatfamilie umzuwandeln. Für spezifische Formate, für die das nicht möglich oder sinnvoll ist, sollte geprüft werden, welche alternativen langzeitspeicherfähigen Formate infrage kommen. Um diese Dokumente zu erhalten, muss jedoch regelmäßig geprüft werden, ob sie noch lesbar sind. Ist das nicht der Fall bzw. zeichnet sich das ab, müssen sie in neuere Formate konvertiert werden.

Für die langfristige Archivierung elektronischer Dokumente (nachhaltige Verfügbarkeit, maschinelle Lesbarkeit und Verfügbarkeit) müssen geeignete Datenformate gewählt werden. Das Datenformat sollte langfristig eine originalgetreue Reproduktion der Archivdaten sowie ausgewählter Merkmale des ursprünglichen Dokumentmediums (z. B. Papierformat, Farben, Logos, Seitenzahl, Wasserzeichen, Unterschrift) ermöglichen. Die derzeit verwendeten Datenformate sind hierfür unterschiedlich geeignet, ihre Eignung hängt sehr stark vom Einsatzzweck der archivierten Daten und ihren Ursprungsmedien ab. Bei einem Wechsel des Medien- und Datenformats können jedoch in der Regel nicht alle Strukturmerkmale des Ursprungsmediums gleichzeitig abgebildet werden.

Da im Vorfeld meist nicht absehbar ist, welche Merkmale des Originaldokuments bei einer späteren Reproduktion nachgewiesen werden sollen und mit welchem Beweiswert dies erfolgen soll, werden Dokumente typischerweise in mehreren elektronischen Datenformaten gleichzeitig archiviert. Dadurch soll eine möglichst hohe Überdeckung der Merkmale des Originaldokuments erreicht werden.

Für die Wahl geeigneter Datenformate sind folgende Kriterien maßgeblich:

- das Datenformat sollte möglichst langfristige Relevanz haben,
- die Dokumentstruktur sollte eindeutig interpretiert werden können,
- der Dokumentinhalt sollte elektronisch weiterverarbeitet werden können,
- die gesetzlichen Vorschriften sollten beachtet werden,
- die Grammatik und Semantik des Datenformates muss ausführlich dokumentiert sein, sodass später problemlos migriert werden kann,
- Merkmale des Originaldokuments (elektronisch oder in Papierform) sollen später eindeutig nachweisbar sein, auch wenn das Originaldokument nicht mehr vorhanden ist.

Typischerweise wird neben einer strukturellen Repräsentation (in einer Strukturbeschreibungssprache) bei Papierdokumenten auch eine grafische Repräsentation des Dokuments (Digitalisierung) archiviert. Hinzu kommen unter Umständen elektronische Signaturen Wahrung von Authentizität und Integrität

In den folgenden Abschnitten werden typische Datenformate beschrieben und diskutiert, ob sie sich für die elektronische Archivierung eignen. Die Liste der Formate ist nicht als abgeschlossen zu betrachten. Entsprechend der Anforderungen eines einzelnen Archivs kann die Liste erweitert werden.

A. Metadaten

XML

Die Extensible Markup Language (XML) wurde als Nachfolger des Standards SGML (Standard Generalized Markup Language) entwickelt und enthielt ursprünglich eine Teilmenge des Sprachumfangs von SGML. Wichtige Merkmale von XML sind:

- In XML können Tags und Attribute neu definiert werden. Hierdurch können Anpassungen an der Syntax und Semantik der Beschreibungselemente vorgenommen werden.
- Analog zu HTML können Links in die Dokumentenstruktur integriert werden. Somit können auf einfache Art und Weise bestehende Dokumente referenziert und z. B. Bilder in Dokumente eingebunden werden.
- XML kann direkt in Webbrowsern angezeigt werden. Zur Darstellung wird eine separate Definition des Layouts in Form der Beschreibungssprache XSL (Extensible Stylesheet Language) benötigt.

XML kann in manchen Fällen als Format für die Langzeitspeicherung von elektronischen Dokumenten genutzt werden (z. B. SIARD-Format für die Aufbewahrung von relationalen Datenbanken). Bei der Archivierung sind jedoch unbedingt auch die Semantikspezifikation (DTD, Document Type Definition) bzw. das XML-Schema und eventuell auch die Layout-Informationen (in XSL beschrieben) zu archivieren.

XML wird häufig benutzt, um Metadaten (z. B. die Formate PREMIS oder Dublin Core) aufzubewahren und um einzelne (selbsttragende) Informationspakete (z. B. in Anlage TR -ESOR-F spezifizierte XAIP für ein selbsttragendes XML-basierten Archivinformationspaket) aufzubauen.

XML-Schema (XSD)

Mithilfe von XML-Schema kann die Struktur von XML-Dokumenten definiert werden. Hierfür werden formelle Regeln und Beschränkungen vorgegeben, die auf beliebige XML-Dokumente (Instanzen) angewandt werden, deren Zugehörigkeit zu einer bestimmten Klasse der XML-Dokumente geprüft werden kann. Diese Prüfung wird Validierung genannt und im Erfolgsfall bestätigt sie, ob ein XML-Dokument gegenüber einem vorgegebenen XML-Schema syntaktisch korrekt ist.

Im Umfeld der Archivierung werden entsprechende Schemata beispielsweise in folgenden Anwendungsbereichen benutzt:

- Definition der Struktur Archivinformationspakete, z. B. XAIP (vgl. Anhang [TR-ESOR-F]),
- Definition der Struktur der Metadaten, z. B. xDomea, SIARD, xBarch (vgl. hierzu auch [TR-ESOR-F]),
- Definition der bestimmten Formate für elektronische Signaturen, z. B. XAdES,
- Definition der beliebigen zu archivierenden Inhalte.

B. Inhaltsdaten – Dokumente

Text (ASCII)

Ein Textdokument, das ausschließlich mithilfe des ASCII-Zeichensatzes kodiert wurde, kann nur rudimentäre Layoutinformationen beinhalten. Solche Dokumente sind somit nur für einfache Information oder Metadaten geeignet. Der 7-Bit-ASCII-Code wurde 1972 von ISO unter 646 spezifiziert und bietet eine solide Grundlage für eine langfristige Verkehrsfähigkeit der Daten.

Eine Weiterentwicklung des ASCII-Codes war der 8-Bit-ASCII-Code, der zusätzlich zu den 7-Bit-ASCII-Zeichen einige Sonderzeichen enthält, z. B. Umlaute für die deutsche Sprache. Eine weitere Stufe ist der Unicode-Standard, der entsprechend auf 8-Bit (UTF-8), 16-Bit (UTF-16) oder 32-Bit (UTF-32) pro Zeichencode basiert, nun aber stets 7-Bit-ASCII-Code als erste 128-Zeichen beinhaltet.

PDF und PDF/A

Das Portable Document Format (PDF) ist ein Dokumentformat, bei dem neben der Strukturinformation von elektronischen Dokumenten auch wesentliche Layoutinformationen mitgespeichert werden. PDF wurde von der Firma Adobe auf Basis des Datenformats PostScript entwickelt.

Das Erscheinungsbild wird dabei durch einen Datenstrom beschrieben, der eine Reihe von grafischen Objekten enthält. Durch diese Beschreibung ist ein Dokument vollkommen festgelegt. Die Entscheidung über das Erscheinungsbild wird dabei zum Zeitpunkt der Erstellung des Dokuments getroffen und ist dann fixiert. Gegenüber einer rein bildlichen Darstellung (Pixeldarstellung) benötigen PDF-Dokumente meist deutlich weniger Speicherplatz.

Zielsetzung beim Einsatz von PDF ist es, das Erscheinungsbild eines elektronischen Dokuments unabhängig von der zur Erstellung benutzten Software, der Hardware-Plattform oder dem Betriebssystem zu bewahren. PDF eignet sich daher primär für die Archivierung von Dokumenten, bei denen eine Abbildung in Papierform vorgesehen ist bzw. die den Charakter von Briefen und Geschäftsdokumenten haben.

Speziell für die Anforderungen der Langzeitspeicherung wurde mit PDF/A eine Version von PDF als ISO 19005-1:2005 genormt. PDF/A (A steht hier für Archivierung) definiert eine stabile Untermenge von PDF, mit der zu archivierende Dokumente so beschrieben werden können, dass alle erforderlichen Informationen in der Datei selber enthalten sind und zwar vollständig, eindeutig, zugänglich und erschließbar.

PDF/A kann als Format für die Langzeitspeicherung von elektronischen Dokumenten genutzt werden. Hierbei ist die Konformität der Dokumente zur PDF/A-Spezifikation zu überprüfen.

Mithilfe von PDF/A-3-Container lassen sich beliebige binäre Daten in einem Zusammenhang aufbewahren. Dadurch ist dieses Format eventuell eine Alternative für die Implementierung von Archivdatenpaketen.

ODF

Die Organization for the Advancement of Structured Information Standards (OASIS) hatte das Open Document Format (ODF) als ein XML-basiertes Dokumentenformat für die Verwendung in Büroanwendungen zur Abbildung von Texten (mit Layout), Tabellenkalkulationen, Präsentationen und weiteren Dokumenten standardisiert. Der Inhalt und das Layout der Dokumente sind dabei strikt voneinander getrennt.

ODF eignet sich relativ gut, um komplexe Dokumente auszutauschen, die weiterbearbeitet werden sollen. Für eine langfristige Aufbewahrung von finalen Dokumentenbeständen wird jedoch eher PDF/A-Format empfohlen.

Office Open XML Formats (OO-XML)

Die Office Open XML File Formats beschreibt eine Sammlung von Office-Formaten, die analoge Anwendungsbereiche, wie das oben genannte ODF, abdecken. Ursprünglich wurden die XML-basierten Formate durch die Firma Microsoft entwickelt und im Rahmen einer ECMA- sowie ISO-Standardisierung offen gelegt.

Das OO-XML wird insbesondere durch die einzelnen Produkte der Office-Suite von Microsoft als Ablageformat für Daten verwendet. Ähnlich wie bei ODF eignet sich OO-XML dafür, Dokumente auszutauschen, die weiterbearbeitet werden sollen. Für die langfristige Aufbewahrung der finalen Dokumente wird jedoch eher PDF/A empfohlen.

TIFF

Das Format TIFF (Tagged Image File Format) wird zur Speicherung gerasterter Bilder verwendet. Eine TIFF-Datei besteht aus einem Datei-Header und der Bildinformation. Der Header enthält sogenannte Tags, in denen Eigenschaften des aufgezeichneten Bildes gespeichert sind, z. B. Auflösung oder verwendete Kompressionsverfahren. Wichtige Merkmale von TIFF sind:

- Bildinformationen können sowohl in Schwarz/Weiß als auch in Grauabstufungen verlustfrei gespeichert werden, jedoch nur dann, wenn eine Farbtiefe von 24-Bit (Truecolor) gewählt wird. Nur in dieser Stufe können alle Graustufen wiedergegeben werden. Um Farbinformationen originalgetreu aufzunehmen und zu speichern, ist jedoch eine regelmäßige Feineinstellung der optischen Sensoren notwendig, damit die Farbinformation nicht durch Farbverschiebungen verfälscht werden. Dies kann z. B. durch einen Farbabgleich mit Weiß als Referenzfarbe erfolgen.
- Alle gängigen Grafik- und Präsentationsprogramme unterstützen das TIFF-Format. Darüber hinaus wird es auch von Archiv- und Workflow-Systemen unterstützt.
- Faxgeräte benutzen TIFF als gängiges Datenformat.
- Die Bilddaten können komprimiert abgespeichert werden. TIFF ist mit den meisten Kompressionsverfahren kompatibel. Zwei der wichtigsten Kompressionsverfahren werden hier kurz angesprochen:
    - ITU/CCITT - Gruppe 4: Die ITU-Kompression benutzt TIFF als Eingangsformat. Dabei wird bei normalen Textdokumenten ein Kompressionsfaktor von etwa 1:40 erreicht. Es ist damit ideal geeignet für Schwarz/Weiß-Dokumente. Die Kompression ist verlustfrei. Die ITU-Kompression ist im Bereich der Archivierung weltweit standardisiert.

TIFF ist sowohl in komprimierter als auch in unkomprimierter Form als Format für die Langzeitspeicherung von Bildern und Bildrepräsentationen von Dokumenten geeignet. Es wird empfohlen, ein verlustfreies Kompressionsverfahren zu verwenden, z. B. ITU/CCITT-Gruppe 4, um den benötigten Speicherbedarf zu minimieren.

JPEG

JPEG wurde von der Joint Photographic Experts Group entwickelt und eignet sich besonders für Farb- und Grauwertbilder. In diesem Bereich ist die JPEG-Kompression auch effektiver als die ITU-Gruppe-4-Kompression.

JPEG kann anhand einiger Parameter unterschiedlich konfiguriert werden. Je nach Einstellung werden dann unterschiedliche Kompressionsraten erreicht. Allerdings können auch Verluste auftreten. Wichtige Merkmale von JPEG sind:

- Alle gängigen Grafik- und Präsentationsprogramme unterstützen das Format JPEG.
- Die Konvertierung in JPEG ist in einigen Kompressionsstufen verlustbehaftet, es können dann zugunsten einer geringen Dateigröße wesentliche Bildinformationen verloren gehen.

JPEG ist als Format für die Langzeitspeicherung von Bildern und Bildrepräsentationen von Dokumenten geeignet. Für eine revisionssichere Archivierung wird empfohlen, bei der Auswahl der Kompressionsstufe eine verlustfreie Kompression zu wählen, z. B. JPEG 2000 Part 6.

PNG

Das Portable Network Graphics Format (PNG) eignet sich aufgrund der Möglichkeiten der verlustfreien Kompression und inkrementellen Anzeige der Grafiken insbesondere für die Anwendung im Internet. Das PNG-Format wurde offen gelegt und ist durch ISO standardisiert (vgl. ISO/IEC 15948).

Da sogenannte Kalibrierungsinformationen innerhalb der PNG codierten Bilder untergebracht werden können und das Format standardmäßig von allen gängigen Bildverarbeitungsprogrammen unterstützt wird, ist PNG für die Archivierung geeignet.

C. Audio- und Video-Formate

Bei der digitalen Verarbeitung von Audio- und Videodaten entstehen schon bei zeitlich kurzen Aufzeichnungen sehr große Datenmengen. Daher ist eine effektive Kompression wichtig.

Verlustfreie Kompressionsverfahren für Audio- und Videodaten erreichen derzeit jedoch nur Kompressionsraten von etwa 2:1. Gebräuchlicher sind Verfahren, die eine Kompressionsrate bis zu 200:1 erreichen, jedoch nicht verlustfrei arbeiten. Der durch die Kompression entstehende, teilweise erhebliche Datenverlust wird typischerweise akzeptiert, solange er mit dem menschlichen Auge bzw. Ohr nicht wahrnehmbar ist bzw. nicht als störend empfunden wird.

Die Eignung verlustbehafteter Kompressionsverfahren für die Archivierung von Video- und Tonmaterial ist anwendungsspezifisch zu prüfen.

Im Folgenden werden einige typische Formate vorgestellt:

MPEG, insbesondere MPEG-4 Part 14

Innerhalb der ISO ist die Motion Pictures Expert Group (MPEG) für die Bearbeitung weltweiter Standards zur Kompression digitalisierter Bewegtbilder verantwortlich. Derzeit sind drei verschiedene Verfahren bekannt:

- MPEG1: Dieses Format gibt es in drei verschiedenen Layern. Layer 3 ist in der Kurzform MP3 bekannt und als Kompression für Audiodaten verbreitet.
- MPEG2: Dieses Format ist derzeit für die Speicherung von Videodaten auf DVD in Gebrauch und als Standard akzeptiert.
- MPEG4 (MP4): Dieses Format definiert ein Containerformat für die Ablage von Multimedia-Dateien.
- MPEG-7 (ISO/IEC 15938): Dieses Format dient nicht zur Kompression von Audio- und Videodateien, sondern zur Organisation multimedialer Daten.

Insbesondere das MP4-Format in den standardisierten Teilen 12 und 14 (vgl. ISO/IEC 14496-12 und -14) bietet sich als ein für die Archivierung geeignetes Audio- bzw. Videoformat an.

OGG Encapsulation Format

Das in RFC3533 spezifizierte Containerformat für die Multimedia-Dateien OGG ist eine bekannte und verbreitete Methode, Audio- und Video-Informationen zu speichern. Es handelt sich hier um ein von Softwarepatenten freies und unbeschränktes Format, das zusammen mit einem zur Verfügung stehenden Codecs (z. B. Vorbis, FLAC oder Theora) sehr gut für die Archivierung geeignet ist.

AAC

Eine weitere Alternative für die Langzeitspeicherung von Audio-Dateien bietet Advanced Audio Coding (AAC). AAC ist durch die ISO standardisiert worden (vgl. ISO/IEC 13818-7) und ist auch Teil der MPEG-2- und MPEG-4-Spezifikation. Das Format selbst ist frei von Patenten, jedoch müssen Lizenzgebühren durch die Hersteller eines AAC-Codecs entrichtet werden. AAC kann als eine durchaus geeignete Alternative für die Archivierung betrachtet werden.

WAVE

Audiodaten werden üblicherweise mit Hilfe der Linear Pulse Code Modulation (LPCM) codiert. In diesem Fall werden die einzelnen Sequenzen jeweils separat in Intervallen gespeichert. LPCM wird sinnvollerweise im Waveform Audio File Format (WAVE) gespeichert. Die WAVE-Spezifikation beschreibt eine unbegrenzte Anzahl an Datenblöcken, die sowohl den Content selbst als auch die Metadaten beinhalten. WAVE ermöglicht die unkomprimierte Speicherung von Audiodaten und sollte für die Aufbewahrung digitalen Master von Audioaufzeichnungen verwendet werden. Daneben ist das Format WAVE frei verfügbar.

AVI

Um digitale Videodaten abzulegen sind verschiedene Elemente zu betrachten: visuelle Daten, Audiodaten, Untertitel oder Verweise auf externe Untertitel sowie Metadaten die für die korrekte Wiedergabe des Videos erforderlich sind. Konsequenterweise muss das Archivsystem Funktionen beinhalten, die nicht nur das Containerformat selbst erkennen, sondern auch alle Format der enthaltenen Dateien selbst. AVI ist ein solches Format. Es wurde von Microsoft und IBM entwickelt, die Dokumentation ist jedoch vollständig offen und nutzbar.

Gemeinsam mit den Basismaßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich Archivierung.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Archivierung".

OPS.1.2.2.M10 Erstellung einer Richtlinie für die Nutzung von Archivsystemen [IT-Betrieb, Leiter IT]

Durch eine Richtlinie mit entsprechenden Regelungen ist sicherzustellen, dass das Archivsystem so benutzt wird, wie es im Archivierungskonzept (siehe OPS.1.2.2.M2 *Entwicklung eines Archivierungskonzepts*) vorgesehenen ist. Hierzu sollten Richtlinien für die Benutzung und die Administration des Archivsystems erstellt werden. Die Richtlinien sind entsprechend den institutionsinternen Gepflogenheiten zu verankern und bekanntzugeben. Wenn externe Personen das Archivsystem benutzen sollen, müssen sie dazu verpflichtet werden, die Richtlinien zu beachten.

Die Administrationsrichtlinien sollten mindestens die folgenden Punkte umfassen:

- Festlegung der Rollen und Verantwortlichkeiten für Betrieb und Administration des Archivsystems,
- Vereinbarungen über Leistungsparameter (Service Level Agreements) beim Betrieb des Archivsystems, insbesondere wenn die Administration oder der Betrieb durch Externe erfolgen soll,
- Modalitäten der Vergabe von Zutritts- und Zugriffsrechten zu den Komponenten des Archivsystems und den Archivmedien,
- Modalitäten der Vergabe von Zugangsrechten zu den vom Archiv bereitgestellten Diensten,
- Regelungen zum Umgang mit archivierten Daten und Archivmedien,
- Überwachung des Archivsystems und der Umgebungsbedingungen für das Archivsystem und die verwendeten Archivmedien,
- Regelung zur Datensicherung der Software-Komponenten des Archivsystems selbst,
- Protokollierung der Aktivitäten am Archivsystem.

Die Benutzerrichtlinien sollten mindestens umfassen:

- Erläuterung der Zielsetzung der elektronischen Archivierung und der Aufbewahrungsfristen für Daten,
- Festlegung der Rollen und Verantwortlichkeiten für Arbeiten mit dem Archivsystem,
- Festlegung, in welchem Umfang die Nutzung des Archivsystems verpflichtend ist,
- Modalitäten der Vergabe von Zugangsrechten zu den vom Archiv bereitgestellten Diensten,
- Schulungsanforderungen an Benutzer, damit sie zur Nutzung des Archivsystems freigeschaltet werden dürfen,
- Regelung der Vergabe von Kontextinformationen zu den archivierten Daten (siehe auch OPS.1.2.2.M4 *Konsistente Indizierung von Daten bei der Archivierung)*,
- Verpflichtung zum sorgfältigen Umgang mit recherchierten Daten unter Beachtung der eventuellen Zweckbindung der Informationen,
- Regelung zum Umgang mit Daten nach Ablauf der festgelegten Archivierungsdauer,
- Regelung, dass Daten, deren Löschung nach einem festgelegten Zeitraum vorgesehen ist, nicht mehr verwendet werden dürfen, obwohl sie unter Umständen aus technischen Gründen noch vorhanden sind,
- Regelung zum Umgang mit personenbezogenen Daten,
- Nutzung der vom Archivsystem bereitgestellten Schutzmechanismen, um eine spätere Prüfung der Integrität und Authentizität der archivierten Daten zu ermöglichen, sowie zur Gewährleistung der erforderlichen Vertraulichkeit,
- Gewährleistung der Verkehrsfähigkeit der archivierten Daten,
- Verpflichtung zur Überprüfung der Integrität und Authentizität recherchierter Daten vor der Weiterverwendung,
- Umgang mit Daten, deren Integrität oder Authentizität sich nicht nachweisen lässt, z. B. bei fehlgeschlagener Signaturprüfung,
- Protokollierung der Benutzeraktivitäten am Archivsystem,
- Abrechnungsmodalitäten bei Nutzung des Archivsystems durch mehrere Organisationseinheiten.

Die Regelungen sowie deren Kenntnisnahme durch die Administratoren und Benutzer des Archivsystems sind zu dokumentieren.

OPS.1.2.2.M11 Einweisung in die Administration und Bedienung des Archivsystems [Benutzer, IT-Betrieb, Leiter IT]

Um ein Archivsystem korrekt und sicher administrieren zu können, müssen sich die Verantwortlichen und hier vor allem die Administratoren und Archivverwalter mit den eingesetzten Systemen auskennen. Hierfür ist eine Schulung der verantwortlichen Archivverwalter und Administratoren notwendig. Dadurch sollen Konfigurationsfehler und Fehlverhalten vermieden werden. Die Schulung sollte mindestens folgende Themen umfassen:

- Systemarchitektur und Sicherheitsmechanismen des verwendeten Archivsystems und des darunterliegenden Betriebssystems,
- Installation und Bedienung des Archivsystems, Handhabung der verwendeten Archivmedien und Kennzeichnung der Archivmedien,
- Einsatzbedingungen des Archivsystems und der Archivmedien (Klimatisierung etc.),
- Dokumentation der Administrationstätigkeiten,
- Protokollierung der Systemereignisse am Archivsystem,
- Vorgehensweise bei der Definition von Regeln/Prozeduren für die Prozesse des Archivsystems
- Vorgehensweise zur Konfiguration des Archivsystems (soweit dies nicht der Hersteller vornimmt)
- Vorgehensweise bei der Auffrischung von Datenbeständen (siehe OPS.1.2.2.M5 *Regelmäßige Aufbereitung von archivierten Datenbeständen* und OPS.1.2.2.M15 *Regelmäßige Aufbereitung kryptographisch gesicherter Daten bei der Archivierung*),
- Grundbegriffe von Verschlüsselung und digitaler Signatur, wenn kryptografische Verfahren verwendet werden,
- Vorgehensweise bei der Vernichtung ausgesonderter Archivmedien,
- Systemüberwachung und Wartung des Archivsystems,
- Eskalationsprozeduren, z. B. bei Nichteinhaltung von Reaktionszeiten, Unterschreiten der Rest-Speicherkapazität der Archivmedien, Manipulation oder Sabotage des Archivsystems oder Ereignissen höherer Gewalt sowie unberechtigten Zugriffen.

Die Schulung der Administratoren und Archivverwalter ist zu dokumentieren. Bei Systemänderungen sollten sie entsprechend weitergebildet werden.

Einweisung der Benutzer in die Bedienung des Archivsystems

Die Archivierung ist eine besonders verantwortungsvolle Aufgabe und stellt hohe Anforderungen an die Bedienung. Die dafür vorgesehenen Mitarbeiter sind auf diese Verantwortung besonders hinzuweisen und vorzubereiten. Hierzu müssen die Benutzer entsprechend geschult werden. Eine derartige Schulung sollte unter anderem folgende Themen umfassen:

- Vorgehensweise bei der Umwandlung analoger Daten: Die korrekte Vorgehensweise bei der Erfassung der Dokumente, der Umwandlung in die elektronische Form sowie der elektronischen Archivierung sind zu erläutern und anhand von praktischen Beispielen zu üben.
- Korrekte Nutzung der Prozesse des Archivsystems (Ablage, Änderung, Abruf, Löschen etc.)
- Vorgehensweise zur digitalen Bestandserhaltung
- Rechtliche Rahmenbedingungen der Archivierung: Bei der Archivierung sind rechtliche Anforderungen einzuhalten (siehe OPS.1.2.2.M1 *Ermittlung von Einflussfaktoren für die elektronische Archivierung)*. Diese Anforderungen und die Folgen, wenn sie nicht eingehalten werden, müssen den Benutzern deutlich gemacht werden.
- Schutz der Vertraulichkeit und Integrität der Dokumente: Die korrekte Vorgehensweise bei der Behandlung vertraulicher Informationen sowie bei der Integritätssicherung und -prüfung archivierter Daten ist zu demonstrieren. Auf mögliche Folgen bei fehlerhafter Bedienung ist hinzuweisen.
- Institutionsspezifische Sicherheitsrichtlinien und ihre Anwendung bei der elektronischen Archivierung: Bei der Konzeption des Archivsystems sind üblicherweise diverse Sicherheitsmaßnahmen vorgesehen worden, die von den einzelnen Benutzern des Archivsystems umgesetzt werden müssen. Dies kann z. B. die Art der Kennzeichnung der Archivmedien oder auch den Umgang mit als vertraulich oder anderweitig klassifizierten Informationen betreffen. Alle Benutzer müssen auf diese Sicherheitsrichtlinien hingewiesen werden.

Die Schulung der Mitarbeiter ist zu dokumentieren. Bei Systemänderungen sollten sie entsprechend weitergebildet werden.

OPS.1.2.2.M12 Überwachung der Speicherressourcen von Archivmedien [IT-Betrieb, Leiter IT]

Die auf den Archivmedien vorhandene, freie Speicherkapazität ist kontinuierlich zu überwachen. Wenn die freie Speicherkapazität unter einen festzulegenden Schwellwert sinkt, sollte der Administrator benachrichtigt werden. Gegebenenfalls sollte an die Systemmanagement-Umgebung signalisiert werden, dass der Schwellenwert erreicht wurde.. Sinkt die freie Speicherkapazität weiter unter einen kritischen Grenzwert, sollte alarmiert werden. Dabei ist besonders darauf zu achten, dass sie rollenbezogen erfolgt, das heißt unabhängig von konkreten Personen. Damit ist sichergestellt, dass sie auch im Krankheitsfall oder bei Urlaub wahrgenommen wird.

Der Schwellwert, der kritische Grenzwert sowie die Eskalationsprozeduren und -wege sind institutionsspezifisch festzulegen.

Die Grenzwerte müssen anhand der verwendeten Archivmedien und des durchschnittlichen Volumens der zu archivierenden Daten bestimmt werden. Nachdem der kritische Alarm ausgelöst wurde, muss gewährleistet sein, dass für eine hinreichende Zeit weiterhin das durchschnittliche Datenaufkommen archiviert werden kann. Typischerweise wird für den Schwellwert eine Restkapazität von 15 % der Gesamtkapazität des Speichermediums und für den kritischen Grenzwert eine Restkapazität von 10 % zugrunde gelegt.

Um etwaige Lieferengpässe bei Speichermedien zu überbrücken, sollte eine ausreichende Zahl leerer Archivmedien an einem bekannten Ort gelagert werden. Dabei müssen die klimatischen und physischen Lagerbedingungen eingehalten werden (siehe OPS.1.2.2.M3 *Geeignete Aufstellung von Archivsystemen und Lagerung von Archivmedien*).

Für den Fall der Alarmierung ist zu dokumentieren, in welcher Weise und in welchem Zeitraum auf die Alarme reagiert werden soll. Das ist z. B. in Service Level Agreements (SLAs) festzulegen, falls der Betrieb des Archivsystems durch Dritte erfolgt.

Neben dem Speicherplatz müssen eventuell noch betriebssystem- oder anwendungsspezifische Restriktionen überwacht werden. Die entsprechenden Programmdokumentationen müssen daraufhin geprüft werden. In Zweifelsfällen oder bei fehlenden Angaben in der Dokumentation sollte der jeweilige Hersteller befragt werden. Beispielsweise können die Anzahl der maximal zugelassenen Dateien pro Verzeichnis oder die maximal erlaubten Datenbankeinträge überschritten werden, sodass keine weiteren Dateien auf dem Speichermedium angelegt werden können.

OPS.1.2.2.M13 Regelmäßige Revision der Archivierungsprozesse

Die Archivierungsprozesse (vgl. OAIS-Modell bzw. BSI TR-03125 [TR-ESOR]) sind regelmäßig einer Revision zu unterziehen, um zu überprüfen, ob sie noch korrekt sind und ordnungsgemäß ablaufen. Daraus lässt sich dann ableiten, ob die im Archiv abgelegten Daten korrekt und authentisch sind.

Für die Revision ist eine geeignete Vorgehensweise entsprechend OPS.1.2.2.*M2 Entwicklung eines Archivierungskonzepts* beschriebenen Konzept zu entwickeln und in Form einer Checkliste zu dokumentieren. Diese sollte mindestens die folgenden Punkte umfassen:

Fragen zu Verantwortlichkeiten

- Sind die verantwortlichen Personen benannt und in ihre Aufgaben eingewiesen worden? Ist das dokumentiert?
- Bestehen Vertretungsregelungen für alle verantwortlichen Personen?

Fragen zum Organisationsprozess

- Bestehen institutionsweite Regelungen zum Einsatz elektronischer Archivierung?
- Ist institutionsweit geregelt und dokumentiert, welche Dokumente/Daten zu archivieren sind? Ist diese Regelung umfassend und vollständig?
- Sind die Sicherheitsanforderungen an die Daten und Dokumente ausreichend dokumentiert?
- Werden die institutionsweiten Regelungen regelmäßig an aktuelle Entwicklungen angepasst?
- Werden alle Anpassungen der Regelungen ordnungsgemäß dokumentiert und archiviert?
- Werden die relevanten Standards ordnungsgemäß eingehalten?

Fragen zum Einsatz der Archivierung

- Bestehen eindeutige Regelungen, welche Daten und Dokumente zu archivieren sind?
- Bestehen dokumentierte Regelungen, welche Kontextangaben an zu archivierende Daten vergeben werden, etwa die Angabe von Dokumentkategorien?
- Werden die zu archivierenden Daten vollständig und reproduzierbar archiviert?
- Werden die Anforderungen an die Vertraulichkeit der zu archivierenden Dokumente eingehalten?
- Werden die Anforderungen an die Authentizität der zu archivierenden Daten eingehalten?
- Werden die Anforderungen an die Integrität der zu archivierenden Daten eingehalten?
- Werden die Anforderungen an die Verfügbarkeit der zu archivierenden Daten eingehalten?
- Werden die Anforderungen an die Verkehrsfähigkeit der zu archivierenden Daten eingehalten?
- Werden die rechtlichen Vorgaben an die Archivierung eingehalten?
- Sind alle Benutzer und Administratoren entsprechend ihrer Rollen und ihrer Aufgaben geschult und eingewiesen? Ist dies dokumentiert?

Fragen zur Redundanz der Archivdaten

- Werden Archivdaten ausreichend redundant gespeichert und aufbewahrt, z. B. mithilfe redundanter Archivsysteme oder alternativer Backup-Medien?
- Erfolgt eine regelmäßige Datensicherung der Archivsysteme sowie gegebenenfalls der Archivdaten?
- Sind die Datensicherungen den Vorgaben entsprechend durchgeführt worden?
- Sind die Datensicherungen der Archivdaten vollständig und lesbar?
- Gab es seit der letzten Revision Datenverluste? Wenn ja, wie häufig und wie schwer waren diese Vorfälle?
- Traten Fehler bei der Rekonstruktion archivierter Daten auf? Wenn ja, wie häufig waren diese Vorfälle und waren die Fehler behebbar?

Fragen zur Administration

- Wird der geforderte Refresh-Zyklus der Archivmedien eingehalten?
- Werden die notwendigen Maßnahmen für die Bewahrung des Beweiswerterhaltes der kryptografisch signierten Daten und Dokumente (z. B. Bewahrung der Gültigkeit der dazu gehörenden Signaturen, Siegel, Zeitstempel, technischen Beweisdaten (Evidence Records) etc.) durchgeführt?
- Werden die notwendigen Maßnahmen durchgeführt, um die Vertraulichkeit der Daten zu bewahren?
- Werden die Maßnahmen zur Informationserhaltung der Daten durchgeführt.
- Werden nicht mehr benötigte, beschriebene Archivmedien ordnungsgemäß vernichtet und entsorgt?
- Werden Lesegeräte und Speichermedien im geforderten Maße vorgehalten?

Technische Beurteilung des Archivsystems

Die Revision sollte jeweils die Archivsystem-Komponenten und die verwendeten Datenformate technisch bewerten, um Weiterentwicklungen und geplante Änderungen des Herstellers frühzeitig zu erkennen.

Bei dieser Prüfung kann sich herausstellen, dass technische Komponenten des Archivsystems geändert werden müssen. Dann muss sichergestellt werden, dass ausgetauschte Komponenten, z. B. Laufwerke, Speichermedien, Betriebssoftware, einwandfrei mit allen anderen Komponenten zusammenarbeiten.

Die Prüfergebnisse der Revisionen sind ebenfalls gemäß den Anforderungen an den Archivierungsprozess zu archivieren.

OPS.1.2.2.M14 Regelmäßige Beobachtung des Marktes für Archivsysteme [Leiter IT]

Die geforderten Aufbewahrungszeiten für Archivdaten liegen normalerweise um ein Vielfaches höher als die durchschnittliche Lebenserwartung einzelner Bestandteile eines elektronischen Archivs. Dies betrifft sowohl Hardware- als auch Software-Komponenten sowie die verwendeten Datenformate und kryptografischen Verfahren.

Um den vollen Funktionsumfang über den gesamten Zeitraum der Archivierung dennoch sicherzustellen, ist davon auszugehen, dass einzelne Hardware-Komponenten, ganze Baugruppen oder auch Software-Komponenten eventuell mehrfach ausgetauscht werden müssen.

Eine wichtige Voraussetzung dafür ist eine regelmäßige Marktbeobachtung, mit der sich abzeichnende Veränderungen rechtzeitig registriert werden können. Solche Veränderungen sind beispielsweise:

- Änderung eines alten Standards oder Verabschiedung eines neuen Standards bei Funktionen und Prozessen, Architektur, Datenformaten, beweisrelevanten Daten oder technischen Beweisdaten, Schnittstellen, Speichermedien oder anzubindenden Fachverfahren
- Veränderungen beim Hersteller des genutzten Archivsystems oder seiner Speicherkomponenten (Wechsel auf neue Systemplattformen, Beendigung einer Produktreihe und Einstellung des Supports, Einstellung der Produktion von Speichermedien, Insolvenz eines Herstellers),
- Bekanntwerden von Sicherheitslücken oder Schwachstellen, z. B. bei eingesetzten Verschlüsselungsalgorithmen,
- Drohender Verlust der Sicherheitseignung bei kryptografischen Algorithmen,
- Änderung eines vorhandenen oder Verabschiedung eines neuen Datenformats, das für die Kodierung der AIP-Container-, Inhalts-, Meta-, Beweis- oder weiterer aufbewahrter Daten verwendet wird.

Es wird empfohlen, einen regelmäßigen Kontakt zu allen beteiligten Herstellern aufzubauen, beispielsweise durch die Teilnahme an Informationsforen, Fachkonferenzen, z. B. Newsgroups und Mailinglisten, in denen aktuelle Informationen über das eingesetzte Archivsystem versandt werden.

Es sollte mindestens ein Mitarbeiter dafür verantwortlich sein, die oben beschriebenen Informationen regelmäßig aufzunehmen, hinsichtlich ihrer Bedeutung für das verwendete Archivsystem auszuwerten und gegebenenfalls notwendige Aktivitäten zu empfehlen. Hierzu muss festgelegt werden, wie eine eventuell erforderliche Migration des Systems eingeleitet wird. Die hier gewonnenen Informationen fließen in die regelmäßige Revision des Archivierungsprozesses ein.

Es ist dabei zu beachten, dass die Langzeitspeicherung die aufbewahrten Informationen erhalten soll und nicht das Archivsystem selbst. Somit sind eine konsequente Verwendung von selbsttragenden verkehrsfähigen Archivinformationspaketen (AIP) sowie die Wahrnehmung der Aufgaben der Langzeiterhaltung (Preservation Planning) gemäß OAIS-Modell zu empfehlen.

OPS.1.2.2.M15 Regelmäßige Aufbereitung von kryptografisch gesicherten Daten bei der Archivierung [IT-Betrieb, Leiter IT]

Kryptografische Verfahren unterliegen einem Alterungsprozess, da im Laufe der Zeit durch mathematische oder technische Weiterentwicklungen Schwächen aufgezeigt werden können, die bei der Auswahl noch nicht bekannt oder relevant waren.

Bei Aufbewahrungsfristen von zehn Jahren und länger ist davon auszugehen, dass verschlüsselte oder signierte Daten wiederholt mit neuen Schlüsseln und gegebenenfalls auf Basis neuer Algorithmen verschlüsselt werden müssen, um die Vertraulichkeit bzw. Integrität/Authentizität der Daten weiterhin zu schützen.

Um beurteilen zu können, ob ein Algorithmus weiterhin zuverlässig und ausreichend sicher ist, sollten die Entwicklungen auf dem Gebiet der Kryptografie kontinuierlich beobachtet werden, beispielsweise anhand der Technischen Richtlinie BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen (siehe [TR-02102]) und der ETSI- Spezifikation (siehe [TS 119 312] und [SOG-IS]). Darüber hinaus sind einschlägige Informationsquellen laufend dahingehend auszuwerten, ob Möglichkeiten bekannt werden, bestehende Verfahren zu kompromittieren.

Für die **Verschlüsselung** gelten die folgenden Maßnahmen:

Bevor die verwendeten Kryptoverfahren nicht mehr zeitgemäß sind und daher die Vertraulichkeitder archivierten Daten nicht mehr sichergestellt werden kann, müssen die verschlüsselten Daten mithilfe von sicheren digitalen Verfahren neu verschlüsselt werden.

Folgende Aspekte sind bei den Maßnahmen zur **Bewahrung der Vertraulichkeit** zu beachten (siehe auch Baustein CON.1 *Kryptokonzept*):

- Es muss ein nach aktuellen Maßstäben sicherer Kryptoalgorithmus verwendet werden, von dem angenommen werden kann, dass er für einen langen Zeitraum sicher ist (siehe die Empfehlungen oben).
- Es muss ein sicheres Verfahren zur Verschlüsselung und zur Schlüsselverteilung gewählt werden, das den Anforderungen der Archivierungsanwendung gerecht wird und den Empfehlungen der Technischen Richtlinie BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen (siehe [TR-02102]) und der ETSI- Spezifikation (siehe [TS 119 312] und [SOG-IS]) genügt.
- Die neu erzeugten Schlüssel müssen entweder zentral erzeugt werden und auf sicherem Weg an die Benutzer des Kryptoverfahrens verteilt werden oder jeder Benutzer erzeugt seine Schlüssel (sicher) selbst.
- Eine Authentisierung der Kryptoschlüssel ist vorzusehen, z. B. durch ein elektronisches Zertifikat.

Die Verteilung der Schlüssel kann auf zwei unterschiedlichen Wegen erfolgen: Falls die Schlüsselerzeugung durch eine unabhängige, vertrauenswürdige Instanz erfolgen soll, ist sicherzustellen, dass die neuen Schlüssel vertraulich und unverfälscht an den ursprünglichen Eigentümer der Daten übertragen werden.

Bei der Nutzung asymmetrischer Verfahren zur Verschlüsselung kann der Dokumenteneigentümer alternativ selbst ein neues Schlüsselpaar erzeugen und den öffentlichen Schlüssel der archivierenden Instanz mitteilen.

In jedem Fall ist zu berücksichtigen, dass eine derartige Neuverschlüsselung einen gewissen Vorlauf braucht: Die Eigentümer der Daten bzw. der Schlüssel müssen benachrichtigt, die notwendigen Schlüssel generiert und verteilt werden. Bei einer großen Anzahl verschiedener Eigentümer und großen Datenmengen ist ein entsprechender Aufwand einzukalkulieren.

Die Maßnahmen zur **Bewahrung des Beweiswertes** sind der Technischen Richtlinie BSI TR 03125 (siehe [TR-ESOR]) zu entnehmen. Dabei gilt:

Um entsprechend lange Aufbewahrungsfristen abdecken zu können, wird empfohlen, das neue elektronische Beweismittel zum Nachweis der Integrität und/oder Authentizität und/oder des Beweiswertes kryptografisch signierter Dokumente im elektronischen Archiv gemäß dem geltenden Stand der Technik und basierend auf den aktuellen Standards und Normen zu erzeugen.

Insbesondere die BSI-Technische Richtlinie TR-03125 TR-ESOR (siehe [TR-ESOR]) auf Basis der DIN 31647 stellen aktuell den maßgeblichen Stand der Technik für den Zweck der Bewahrung des Beweiswertes zum Nachweis der Integrität und/oder Authentizität von kryptografisch signierten Dokumenten dar. Dabei wird die Bewahrung mittels sicherer digitaler Signaturtechniken sichergestellt. Details dazu befinden sich in BSI TR-03125 (siehe [TR-ESOR]).

Dabei ist zu beachten: Geeignete kryptografische Verfahren zur Bewahrung des Beweiswertes kryptografisch signierter Dokumente/Daten oder zum Schutz der Vertraulichkeit der aufbewahrten Daten bei der Archivierung sind elektronische Signaturen, Siegel, Zeitstempel und technische Beweisdaten (Evidence Records) bzw. Verschlüsselung. Das ist für die elektronische Archivierung eine Herausforderung, da die Verfahren technisch bedingt nur eine begrenzte Lebensdauer haben, die jedoch vorher nicht immer bekannt ist. Andererseits sind sie aber auch erforderlich, wenn elektronische Dokumente beweissicher beziehungsweise vertraulich archiviert werden müssen. Die Aussagekraft elektronischer Signaturen, Siegel, Zeitstempel oder technischer Beweisdaten (Evidence Records) hängt sehr stark von deren Interpretation zum Zeitpunkt der Prüfung und damit vom so genannten Gültigkeitsmodell ab.

Gültigkeit

Die Gültigkeit einer elektronischen Signatur, eines Siegels oder eines Zeitstempels wird üblicherweise wie folgt definiert: Eine elektronische Signatur ist genau dann gültig,

- wenn sie mathematisch richtig ist und
- wenn zum Zeitpunkt der Signaturprüfung der zugehörige Signaturschlüssel und alle Zertifikate bis hin zum Wurzelzertifikat gültig sind (Schalenmodell).
- wenn zum Zeitpunkt der Signaturausübung der zugehörige Signaturschlüssel und alle Zertifikate bis hin zum Wurzelzertifikat gültig waren (Kettenmodell).

Die Prüfung technischer Beweisdaten (Evidence Record) kann gemäß TR 03125 TR-ESOR (siehe [TR-ESOR]) auf Basis von RFC 4998 und RFC 6283 erfolgen.

Aussagekraft

Elektronische Signaturen und Siegel können zu unterschiedlichen Zwecken eingesetzt werden, unter anderem

- zum Nachweis der Integrität von Dateien,
- zur Beglaubigung der Authentizität von kryptografischen Schlüsseln oder elektronischen Daten

Ein elektronischer Zeitstempel und technische Beweisdaten (Evidence Records) bestätigen die Integrität der gestempelten Daten sowie deren Existenz zu einem gegebenen Zeitpunkt.

Der Einsatz und die Aussagekraft elektronischer Signaturen, Siegeln ,Zeitstempeln oder von technischen Beweisdaten können anwendungsspezifisch in einer Sicherheitsrichtlinie (Policy) vorgegeben werden. Darin sollte unter anderem festgelegt werden,

- unter welchen Voraussetzungen elektronische Signaturen, Siegel, Zeitstempel sowie technische Beweisdaten erzeugt werden,
- von welcher Stelle elektronische Signaturen, Siegel, Zeitstempel sowie technische Beweisdaten erzeugt werden (bei Zertifikats-Signaturen z. B. in einem neutralen Trust Center),
- welches Gültigkeitsmodell für die Anwendung herangezogen wird,
- ob und wie elektronische Signaturen, Siegel, Zeitstempel sowie technische Beweisdaten gegebenenfalls widerrufen werden können,
- wie die Bewahrung der Integrität, Authentizität sowie des Beweiswertes kryptografisch signierter Dokumente mittels sicherer digitaler Signaturtechniken (z. B. neue Signaturen, (Archiv-)Zeitstempel, Hashbäume oder Evidence Records etc.) sichergestellt werden kann,
- welche Aussage damit verbunden sein soll, d. h. was damit beglaubigt wird. Bei einem Zeitstempel beispielsweise, ob ein Dokument zu einem bestimmten Zeitpunkt vorliegt.

Die Sicherheitsrichtlinie muss schriftlich dokumentiert und archiviert werden, damit bei einer späteren Prüfung der elektronischen Signatur, Siegel, Zeitstempel sowie technischen Beweisdaten klar ist, was diese aussagt bzw. beweisen soll und was nicht. Außerdem sollte sie auch in geeigneter Form veröffentlicht werden, damit alle, die auf die Signaturen vertrauen müssen bzw. wollen, sich darauf beziehen können.

Sicherheitseignung

Die Sicherheitseignung elektronischer Signaturen, Siegel, Zeitstempel sowie technischer Beweisdaten wird durch die technische Entwicklung von Hard- und Software sowie Fortschritte in der Kryptografie beschränkt. Daher müssen sie regelmäßig nach dem Stand der Technik aktualisiert werden. Zusätzlich ist in bestimmten Zeitabständen eine "Re-Signing" oder "Re-Hashing" für technische Beweisdaten (Evidence Records) erforderlich, beispielsweise gemäß RFC 4998, RFC 6283 bzw. TR-ESOR-M.3 (siehe [TR-ESOR-M3]).

Empfehlung

Archivierte Daten müssen neu verschlüsselt und die elektronischen Beweismittel neu erzeugt werden, bevor ein kryptografisches Verfahren nicht mehr sicher ist. Um lange Aufbewahrungsfristen abdecken zu können, sollten für Archivdaten nur kryptografische Verfahren auf Basis aktueller Standards und Normen verwendet werden.

OPS.1.2.2.M16 Regelmäßige Erneuerung technischer Archivsystem-Komponenten [IT-Betrieb, Leiter IT]

Archivsysteme müssen über lange Zeiträume auf einem aktuellen technischen Stand gehalten werden. In der Informationstechnik haben Standards für Hard- und Software sowie Datenformate zur digitalen Speicherung bisher jedoch nur kurzzeitig Bestand gehabt. Es ist davon auszugehen, dass dies auch künftig so bleibt, da die Standards in hohem Maße vom technischen Fortschritt geprägt werden. (vgl. Bestandserhaltung gemäß OAIS-Modell).

Hardware-Komponenten unterliegen zudem Verschleißerscheinungen und müssen daher regelmäßig gewartet sowie gegebenenfalls ausgetauscht werden. Zusätzlich ist damit zu rechnen, dass Hersteller unvorhergesehen die Unterstützung bestehender Systeme einstellen oder, z. B. aufgrund von Insolvenz, nicht mehr in der Lage sind, langfristige Unterstützung zu gewährleisten.

Es ist daher damit zu rechnen, dass die Komponenten des Archivs regelmäßig erneuert werden müssen und eventuell der komplette Datenbestand auf ein neues Archivsystem migriert werden muss. Dieser Prozess ist eng mit OPS.1.2.2.M14 *Regelmäßige Beobachtung des Marktes für Archivsysteme* verknüpft.

Vor der Installation neuer Hard- und Software in ein laufendes Archivsystem ist diese ausführlich zu testen, um die Stabilität des bestehenden Systems nicht zu gefährden. Bei der Installation z. B. neuer Datenträger und Laufwerke muss darauf geachtet werden, dass sie mit den bestehenden Systemen und Datenträgern kompatibel sind.

Vor der Inbetriebnahme neuer Komponenten oder der Einführung neuer Datenformate ist ein Migrationskonzept zu erstellen, in dem alle Änderungen und Tests beschrieben werden. Die Konvertierung der einzelnen Daten ist immer zu dokumentieren. Diese Dokumentation ist zusammen mit den konvertierten Daten aufzubewahren (Transfervermerk). Das Archivierungskonzept (siehe OPS.1.2.2.M2 *Entwicklung eines Archivierungskonzepts*) ist unter Umständen anzupassen. Bei größeren Änderungen muss die in der Bausteinbeschreibung beschriebene Planungsphase erneut durchlaufen werden.

Bei der Änderung von Formaten muss geprüft werden, ob bei der Konvertierung von Altdaten in die neuen Formate aufgrund rechtlicher Anforderungen zusätzlich die Daten in ihren ursprünglichen Formaten archiviert werden müssen.

OPS.1.2.2.M17 Auswahl eines geeigneten Archivsystems [Leiter IT]

Die Auswahl eines Archivsystems erfolgt auf der Grundlage der im Archivierungskonzept (siehe *OPS.1.2.2.M2 Entwicklung eines Archivierungskonzepts*) festgeschriebenen Vorgaben. Typischerweise werden folgende Mindestanforderungen an das einzusetzende Archivsystem gestellt, wobei institutionsspezifische Anforderungen zu ergänzen sind:

- Versionierung von Dokumenten/Datensätzen: Das Archivsystem sollte die mehrfache Speicherung von Dokumenten/Datensätzen in unterschiedlichen Fassungen unterstützen (Versionierung).
- Funktionen und Prozesse angelehnt an das OAIS-Modell sowie [TR-ESOR]
- Zugriffsschutz auf die archivierten Daten: Durch das Archivsystem sollte ein Zugriffsschutz auf die archivierten Daten und die Funktionen des Archivsystems umgesetzt werden können. Dies sollte auf der Grundlage eines vorgegebenen Berechtigungskonzepts erfolgen.

- Mehrstufiges, rollenbasiertes Berechtigungskonzept: Bei einer rollenbasierten Rechtevergabe werden Zugriffsrechte nicht an konkrete Benutzer vergeben, sondern an definierte Benutzergruppen (Rollen). Im Gegensatz zu normalen Berechtigungsgruppen werden in einem rollenbasierten Zugriffsmodell auch Rollenkonflikte berücksichtigt. Dies bedeutet zum Beispiel, dass eine Person nicht gleichzeitig die Rolle des Administrators und des Revisors einnehmen kann.
- Protokollierung: Das Archivsystem sollte es ermöglichen, alle Vorgänge rund um die Archivierung zu protokollieren und nachvollziehbar zu machen (siehe auch OPS.1.2.2.M8 *Protokollierung der Archivzugriffe*). Dabei sollte es auch möglich sein, kritische Ereignisse zu definieren und einen Administrator zu benachrichtigen, wenn solche auftreten.

- Einrichtung eines Benutzerkontos für die Revision: Für Zugriffe während der regelmäßigen Revision des Archivsystems sollte ein entsprechendes Benutzerkonto mit den dafür notwendigen Rechten eingerichtet werden. Die konkrete Rechtevergabe ist institutionsintern festzulegen. Im Rahmen der Revision werden typischerweise Leserechte (read-only) auf Konfigurationsdaten und Protokolldaten eingerichtet.
- Erweiterbarkeit des Archivsystems: Das Archivsystem sollte erweiterbar sein, damit es bei Änderungen der Anforderungen angepasst werden kann. Die Erweiterbarkeit betrifft vor allem die eingesetzten Speicherkomponenten und Speichermedien, aber auch sonstige Hardware-Änderungen sowie die Archivsystem-Software und Nutzungslizenzen.

- Geringe Zugriffszeit: Für das Archivsystem wird typischerweise eine geringe Zugriffsverzögerung und gleichzeitig eine hohe Bandbreite bei der Übertragung und Bereitstellung der angeforderten Dokumente verlangt. Die Anforderungen sind institutionsspezifisch zu ermitteln. Hierbei ist neben der Einbindung in die vorhandene Systemumgebung auch das abzusehende Benutzerverhalten zu berücksichtigen. Die festgelegten Anforderungen wirken sich auf die Auswahl der Archivmedien und der Speicherlaufwerke aus. Ebenso können die Anforderungen die Auswahl und Dimensionierung von Cache-Komponenten beeinflussen.
- Ausreichende Kapazität der Archivmedien: Die Archivmedien sollten eine ausreichende Kapazität aufweisen. Sowohl die mehrfache Speicherung von Dokumenten zur Versionierung als auch die zu erwartende Datenmenge sollten bei der Kapazitätsplanung berücksichtigt werden.

- Systemgesteuertes Einlegen oder Entnehmen von Archivmedien: Das Archivsystem sollte unterstützen, dass Archivmedien nur systemgestützt aus den Laufwerken entnommen werden können. Hierdurch soll gewährleistet werden, dass Archivmedien nur nach kontrollierter Offline-Schaltung (unmount) sowie unter Beachtung entsprechender Zugriffsrechte entnommen werden und die Entnahme protokolliert werden kann. Gleiches gilt für die Online-Schaltung (mount) von Archivmedien. Dies ist erforderlich, damit eine konsistente Verwendung der Archivmedien sichergestellt ist. Für Notfälle sehen in der Regel alle Archivsysteme und Laufwerke manuelle Möglichkeiten vor, Archivmedien zu entnehmen.
- Kapazitätsüberwachung der Archivmedien: Die Restkapazität der in Benutzung befindlichen Archivmedien muss laufend überwacht werden. Wird eine Restkapazitätsgrenze unterschritten, muss eine Signalisierung bzw. Alarmierung erfolgen.

- Alarmierung und Signalisierung: Das Archivsystem muss die Signalisierung von Systemmeldungen an übergreifende Systemmanagement-Umgebungen gestatten. Wenn keine Anbindung an eine Systemmanagement-Umgebung vorgesehen ist, so sollte über E-Mail, SMS oder SNMP individuell alarmiert werden können.
- Einhaltung von Standards: Die Einhaltung von Standards erleichtert die Interoperabilität zwischen einzelnen Komponenten. Dies ist erforderlich, weil damit gerechnet werden muss, dass im Betriebszeitraum einzelne Komponenten ausgetauscht werden müssen oder das System erweitert werden soll. Standards sind insbesondere in folgenden Bereichen relevant:

-
  - Archivmedien und Aufzeichnungsverfahren (siehe OPS.1.2.2.M18 *Verwendung geeigneter Archivmedien*),
  - Dateiformate und Komprimierungsverfahren (siehe OPS.1.2.2.M9 *Auswahl geeigneter Datenformate für die Archivierung von Dokumenten*).
  - Komponenten, Prozesse, Organisation des Archivsystems
  - Beweiswerterhaltung der elektronischen Daten,
  - Anbindung an die vorhandene IT-Umgebung (Schnittstellen).

Es sollte überlegt werden, die Daten durch Verschlüsselung und sichere elektronische Signaturtechniken zu schützen. Weiterhin kann die Grundverschlüsselung von Archivmedien durch das Archivsystem implementiert werden. Hierdurch soll ein Missbrauch des Archivmediums außerhalb des Archivsystems verhindert werden.

OPS.1.2.2.M18 Verwendung geeigneter Archivmedien [IT-Betrieb, Leiter IT]

Die dauerhafte elektronische Archivierung von Daten erfordert den Einsatz geeigneter Datenträger (Archivmedien). Für die Wahl der Archivmedien sollten folgende Fragen berücksichtigt werden:

- Welches Datenvolumen soll archiviert werden?
- Welche Zugriffszeiten sind im Mittel zu erbringen?
- Wie hoch ist die Zahl gleichzeitiger Zugriffe im Mittel?
- Welche Aufbewahrungsfristen sollen durch das Archivmedium abgedeckt werden?

In den folgenden Abschnitten werden typische Archivmedien und deren Einsatzbereiche beschrieben. Für die Datenträger werden üblicherweise magnetische, magnetooptische oder optische Speichertechniken verwendet. Die Vor- und Nachteile der Techniken sind in den jeweiligen Abschnitten beschrieben.

Sämtliche beschriebenen Archivmedien sind anfällig gegenüber physischen Beschädigungen, etwa durch

- Wasser,
- Feuer bzw. Hitzeentwicklung,
- Verkratzen des Mediums,
- Zerknittern und Aufreißen des Mediums im Bandlaufwerk sowie

- Sabotage und Diebstahl.

Archivmedien müssen daher sorgsam aufbewahrt und geschützt werden. Außerdem muss der unbefugte Zugriff auf die Datenträger verhindert werden. Hierzu wird, abhängig vom konkreten Einsatzszenario des elektronischen Archivs, die Anwendung der im Baustein INF.7 *Datenträgerarchiv* bzw. INF.6 *Schutzschrank* beschriebenen Maßnahmen zum Schutz der Datenträger empfohlen.

Digitale magnetische Speichermedien

Bei magnetischen Speichersystemen wird durch gezielte lokale Veränderung eines magnetisierten Grundmediums ein Speichereffekt erzielt. Die Magnetisierung kann durch ein Lesegerät erfasst, die gespeicherten Daten können dadurch gelesen werden. Durch erneutes Einwirken eines Magnetfeldes können die gespeicherten Daten verändert werden. Dies erfolgt gezielt durch Verwendung eines Schreib-/Lesegerätes oder ungezielt durch starke externe Magnetfelder (z. B. elektromagnetische Felder in der Nähe von Transformatoren oder großen Spulen).

Magnetische Datenträger sind anfällig gegenüber Angriffen mit starken Magnetfeldern, die auf das Speichermedium einwirken. Da das magnetisierte Grundmedium typischerweise als Verbundwerkstoff aus Kunststoffen sowie einer metallischen (magnetisierbaren) Beschichtung hergestellt wird, ist außerdem auch bei sorgsamer Behandlung mit langfristigen Veränderungen zu rechnen. Diese können z. B. durch Zersetzung (durch Weichmacher in Kunststoffen), Aufquellen (Ablösung von Kunststoff- und Metallschichten) oder Oxydation (der Metallschicht) bedingt sein.

Aufgrund der verwendeten Techniken sind magnetische Speicher zudem stets wiederbeschreibbar bzw. löschbar. Sie müssen daher im Rahmen der Archivierung stets mit zusätzlichen Sicherungsverfahren eingesetzt werden, um zu verhindern, dass Dokumente verändert werden. Typische magnetische Speicher sind Festplatten und (Magnet-)Bandmedien.

- Festplatten: In Festplatten sind typischerweise das Speichermedium und das Schreib-/Lese-Laufwerk zusammen in einer Einheit untergebracht. Sie sind daher fehleranfällig gegen mechanische Ausfälle. Durch die physische Kapselung wird eine dichtere Anordnung der Magnetmedien bei gleichzeitigem Schutz vor Staubpartikeln ermöglicht, sodass Festplatten meist über mehrere Schreib-Lese-Einheiten verfügen. Festplatten weisen typischerweise eine hohe Kapazität und eine geringe Zugriffszeit bei hoher Übertragungsrate auf.
- Magnetbänder: Magnetbänder bestehen aus einem aufgewickelten Magnetstreifen, der in der Regel an einem Schreib-Lesekopf sequenziell vorbeigeführt wird. Magnetband und Schreib-Lese-Einheit sind typischerweise nicht miteinander verbunden. Magnetbänder weisen technisch bedingt eine sehr lange Zugriffszeit und eine sehr geringe Übertragungsrate auf. Ihre Speicherdichte und ihr Platzverbrauch sind jedoch vergleichbar mit Festplatten. Magnetbänder eignen sich für die Speicherung großer Datenmengen, auf die nur selten und sequenziell zugegriffen werden muss. Sie sind daher geeignet für Backups, bei denen eine mittelfristige, jedoch nicht langfristige Stabilität erwartet wird.

Digitale magneto-optische Speichermedien

Bei der magneto-optischen (MO) Speichertechnologie werden gespeicherte Daten, ähnlich wie bei optischen Speichern, durch Abtasten eines Speichermediums mit einem Laserstrahl gelesen. Der optische Effekt wird dabei durch eine Magnetschicht verursacht, deren Partikel beim Durchlaufen und Reflexion des Laserstrahls als Polarisationsfilter wirken. Die Polarisation der Oberfläche lässt sich punktuell beeinflussen, indem ein Magnetfeld angelegt wird, das nur an einer (wiederum durch einen Laser) speziell aufgeheizten Region des Speichermediums wirkt. In einem Schreibprozess werden die Regionen der Medienoberfläche gezielt unterschiedlich polarisiert.

Auch bei magneto-optischen WORM-Medien kann technisch bedingt ein nachträgliches unbefugtes Überschreiben (Brennen) bislang ungenutzter Bereiche nicht ausgeschlossen werden. Es handelt sich demnach auch hier nicht um echte Write-Once-Medien, sondern lediglich um nicht-löschbare Datenträger.

Magneto-optische Systeme weisen eine hohe Langzeitstabilität (nach Herstellerangaben mehr als 30 Jahre) und eine Speicherkapazität von bis zu 9,1 GB je Medium auf.

Netzbasierte Speichermedien

Netzbasierte Speichermedien sind für die Langzeitspeicherung und Archivierung immer wichtiger. Sie lassen sich einfach als Dienst integrieren und sind hervorragend skalierbar sowie verfügbar. Insbesondere folgende zwei Vertreter können empfohlen werden:

- Storage-Area-Network (SAN): SANs wurden für serielle, kontinuierliche und mit großer Geschwindigkeit erfolgende Übertragung von großen Datenmengen konzipiert. Ein SAN kann mehrere im Netz vorhandene Festplattensysteme, Tape-Libraries etc. den Servern für eine sehr schnelle Speicherung der Daten zur Verfügung stellen. Gängige unterstütze Übertragungsraten liegen im Bereich von 16 GBit/s.
- cloudbasierte Speichersysteme: Infrastruktur-Cloud-Dienste erlauben eine einfache Implementierung von hoch skalierbaren und hoch verfügbaren Speichermedien, die der Langzeitspeicherung bzw. Archivierung zur Verfügung gestellt werden können (siehe hierzu auch Baustein OPS.2.2 *Cloud-Nutzung)*.

Hierarchisches Speichermanagement

Mithilfe eines gemäß den Prinzipien des hierarchischen Speichermanagements (HSM) umgesetzten Langzeitspeichers lassen sich die Zugriffszeiten auf die mit großer Häufigkeit benötigten Objekte deutlich verkürzen. Dafür werden die Speichermedien stufenförmig aufgebaut, sortiert nach der steigenden Zugriffszeit. Die am häufigsten benötigten Daten werden im schnellen Medium vorgehalten und können nach und nach auf den nachgeordneten langsameren (und billigeren) Speicher ausgelagert werden, wenn diese später nicht mehr so oft benötigt werden.

Insgesamt ist auf Basis der im Archivierungskonzept definierten technischen, rechtlichen und organisatorischen Anforderungen zu entscheiden, welches Speichermedium eingesetzt werden soll.

OPS.1.2.2.M19 Regelmäßige Funktions- und Recoverytests bei der Archivierung [IT-Betrieb, Leiter IT]

Durch verschiedene Ursachen in den Bereichen Datenträger, Hardware und beim Programmablauf kann es bei der Archivierung zu Datenverlusten kommen. Regelmäßige Funktions- und Recoverytests sind daher unumgänglich.

Datenträger unterliegen ebenso wie alle anderen Archivierungskomponenten Verschleißerscheinungen und sollten daher mindestens einmal jährlich geprüft werden, ob sie noch lesbar und integer sind.

Werden Fehler auf einem Archivmedium festgestellt, so ist unverzüglich sicherzustellen, dass die betroffenen Dateien aus dem Backup-Bestand wieder hergestellt werden. Wenn fehlerhafte Archivdatenträger ausgetauscht werden müssen, so sind diese nach der Kopie der darauf enthaltenen Daten sicher zu löschen bzw. zu vernichten. Der gesamte Vorgang ist zu dokumentieren.

Alle Hardwarekomponenten, insbesondere die mechanischen Teile des Archivs, müssen regelmäßig auf einwandfreie Funktion geprüft werden. Nur so kann gewährleistet werden, dass archivierte Datenbestände den geforderten Verfügbarkeitsanforderungen entsprechen und beim Schreiben und Lesen der Daten die Datenintegrität gegeben ist.

Der Archivierungsvorgang selbst kann fehlerhaft verlaufen. Mögliche Ursachen dafür können sein: Konfigurationsfehler, Softwarefehlfunktionen, Probleme mit den Speichermedien oder Änderungen und Fehler in der Ablaufsteuerung. Einmal pro Tag ist daher zu überprüfen, ob alle Archivierungsprozesse fehlerfrei abgelaufen sind. Das kann geschehen, indem Logdateien ausgewertet werden sowie durch eine stichprobenartige Ansicht der erstellten Archivmedien durch den Administrator.

Die notwendigen Integritätsprüfungen der Indexdatenbank sind in Maßnahme OPS.1.2.2.M6 *Schutz der Integrität der Indexdatenbank von Archivsystemen* beschrieben.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

OPS.1.2.2.M20 Geeigneter Einsatz kryptografischer Verfahren bei der Archivierung [Leiter IT] (CI)

Archivierte Daten sollten parallel mit mindestens zwei verschiedenen kryptografischen Verfahren verarbeitet werden und die elektronischen Beweismittel auf dieselbe Art und Weise neu erzeugt werden, bevor ein kryptografisches Verfahren nicht mehr sicher ist. Um lange Aufbewahrungsfristen abdecken zu können, sollten für Archivdaten nur kryptografische Verfahren auf Basis aktueller Standards und Normen verwendet werden.

OPS.1.2.2.M21 Übertragung von Papierdaten in elektronische Archive (CI)

Für die Übertragung von Papierdaten in elektronische Archive wird die Anwendung der [TR-03138 RESISCAN] empfohlen.

3 Weiterführende Informationen

3.1 Wissenswertes

Damit sich Geschäftsprozesse und -unterlagen in elektronischen Geschäftsanwendungen abbilden lassen, müssen die entstehenden Dokumente geeignete archiviert werden. So können sie später wieder verwendet, wieder gefunden sowie noch einmal aufbereitet werden. Das betrifft sowohl Datensätze als auch elektronische Repräsentationen eingescannter Geschäftsdokumente. Der Lebenszyklus elektronischer Dokumente kann grundsätzlich in drei Phasen unterteilt werden (vgl. Abbildung 1):

- Phase 1 – Bearbeitung der Dokumente: In dieser Phase werden normalerweise die Dokumente innerhalb einer Geschäftsanwendung gehalten und öfter angepasst. Die Datenhoheit liegt bei der zuständigen Instanz, z. B. einer Behörde oder einem Unternehmen.
- Phase 2 – Langzeitspeicherung (LZSP) der Dokumente: Die Dokumente erreichen einen stabilen (finalen) Stand und werden bis zum Ablauf einer festgelegten Frist aufbewahrt, z. B. nachdem ein Vorgang abgeschlossen wurde. Die Datenhoheit liegt bei der zuständigen Instanz.
- Phase 3 – Aussonderung und dauerhafte Aufbewahrung der Dokumente: Nach dem Ablauf der Aufbewahrungsfrist müssen die aufbewahrten Dokumente vernichtet werden. Im Fall von Behörden müssen die zu vernichtenden Dokumente dem zuständigen Archiv zwecks dauerhafte Aufbewahrung angeboten werden. Die Datenhoheit geht somit auf das Archiv über.

Davon abgeleitet werden die Langzeitspeicherung, (dauerhafte) Archivierung und Datensicherung (Backup) für die weitere Verwendung in diesem Baustein voneinander abgegrenzt.

- Aufbewahrung und Erhaltung (Information und Beweiswert) von elektronischen Dokumenten **für den Zeitraum der geltenden Aufbewahrungsfristen** wird **Langzeitspeicherung** (LZSP) genannt.
- Die dauerhafte und unveränderbare Aufbewahrung und Erhaltung von elektronischen Dokumenten, mit dem Ziel der **Sicherstellung der historischen Überlieferung** insbesondere in staatlichen und kommunalen Archiven (z. B. Bundesarchiv), wird als (dauerhafte) **Archivierung** bezeichnet.
- Eine vom IT-System physisch getrennte und vor Gefahren geschützte Aufbewahrung einer Kopie von System- und Nutzdaten, die in regelmäßigen Abständen erneuert wird, wird als **Datensicherung** (Backup) bezeichnet.

ISO 14721 - Open Archival Information System

Die ISO 14721 (auch OAIS-Referenzmodell (Referenz Model for an Open Archival Information System) genannt) stellt eine fachliche Grundlage für die Langzeitspeicherung und Archivierung dar. Es ist ein organisatorisches Modell für den Aufbau von elektronischen Systemen zur Langzeitspeicherung und Archivierung und wurde als ISO-Standard im Jahr 2003 veröffentlicht und 2012 aktualisiert.

Das OAIS-Referenzmodell beschreibt die notwendigen Komponenten (Prozesse und Informationspakete) zur langfristigen oder dauerhaften Aufbewahrung von elektronischen Dokumenten.

Ein System, das nach OAIS aufgebaut ist, besteht aus mehreren Prozessen, die einzelne Funktionen übernehmen und miteinander kommunizieren.

Eine zentrale Rolle im OAIS-Referenzmodell spielt das darin definierte Archivinformationspaket (Archival Information Package, AIP). Es enthält neben den Primärdaten alle zur Interpretation, Lesbarkeit, Nutzbarkeit, Verständlichkeit und Recherche notwendigen Informationen, beweisrelevante Nachweise der Integrität und Authentizität der aufzubewahrenden Unterlagen sowie auch die Primärdaten in standardisierter und herstellerunabhängiger Form in einem Paket. Ein AIP besteht demnach aus:

- Metainformationen,
- Inhalts-/Primärinformationen,
- beweisrelevanten Daten und
- technischen Beweisdaten.

Das OAIS-Referenzmodell wurde für End-Archive konzipiert, die ihr Archivgut dauerhaft aufbewahren. So hat auch das Bundesarchiv sein elektronisches Archivsystem entsprechend den Vorgaben und Empfehlungen des OAIS- Referenzmodells entwickelt.

Der modulare Aufbau des OAIS-Referenzmodells ermöglicht eine authentische Wahrung und Reproduzierbarkeit des Archivguts. Für den Bereich der Langzeitspeicherung sind die Ausführungen zur Erhaltung des Beweiswerts, der Lesbarkeit sowie der Verfügbarkeit der elektronischen Objekte wesentlich.

Das OAIS-Referenzmodell kann, insbesondere das Modul Bestanderhaltung, als organisatorische Hilfe im Rahmen der Langzeitspeicherung dienen.

Dieses Modul hat zur Aufgabe, die

- Les- und Nutzbarkeit,
- Unverfälschbarkeit,
- Vollständigkeit sowie
- die Sicherheit vor Verlust

des Archivguts zu gewährleisten.

In der praktischen Arbeit umfasst dies die Überwachung der Lesbarkeit von Formaten, deren Konvertierung oder auch die Migration auf andere Speichermedien. Um dabei alle wichtigen Einflussfaktoren zu berücksichtigen und die Bestandserhaltung sicherzustellen, ist eine entsprechende Konzeption zu entwickeln und umzusetzen.

Das in ISO 14721:2012 genormte OAIS gilt aus oben genannten Gründen als zentrale Norm zur Langzeitspeicherung und Archivierung elektronischer Unterlagen und sollte z.B. insbesondere auch für Stellen und Einrichtungen des Bundes als Basis für die Umsetzung ihrer Langzeitspeicherungs- und Archivsysteme dienen.

Die ISO 14721 definiert die für Langzeitspeicherung und Archivierung notwendigen Prozesse Übernahme, Datenmanagement, Speichersystem, Zugriff, digitale Langzeiterhaltung und Systemadministration sowie die Informationspakete Übergabeinformationspaket (SIP), Archivinformationspaket (AIP) und Ausgabeinformationspaket (DIP). Vergleiche dazu auch Abbildung 2.

Das Archivinformationspaket (engl. Archival Information Packet, AIP) soll in einer selbsttragenden Form alle zur Erfüllung des Aufbewahrungszwecks notwendigen Informationen bis zum Ablauf der geltenden Aufbewahrungsfristen in einer möglichst hard- und softwareneutralen Form beinhalten. Dabei geht es primär um die Inhaltsdaten (die aufzubewahrenden Daten selbst), beschrieben durch die notwendigen Metadaten (sowohl fachliche als auch technische Metadaten) und die zum Nachweis der Authentizität und Integrität notwendigen Daten. Es ist dabei entscheidend, eine ausreichende Menge der Metadaten zu erfassen (Kontextsicherung), um den aufbewahrten Vorgang auch in der Zukunft vollständig rekonstruieren zu können.

Der Übernahme-Prozess (engl. Ingest) beinhaltet die notwendigen Funktionen zur Übernahme der Dokumente in das digitale Archiv, indem das aus der Geschäftsanwendung übergebene SIP in ein korrespondierendes AIP überführt wird. Es werden dabei die Dokumente in langfristig lesbare Dateiformate überführt, die Inhalte geeignet indexiert, Metadaten erhoben bzw. generiert sowie die AIP-Struktur erzeugt.

Der Speicher-Prozess (engl. Archival Storage) ist für die physische Ablage und Bereitstellung der aus dem Übernahme-Prozess hervorgegangenen AIP-Strukturen notwendig. Dieses kann durch Einsatz von unterschiedlichen Speichertechniken aus dem Speicher-Segment umgesetzt werden, z. B. Plattenspeicher, SAN.

Der Datenmanagement-Prozess (engl. Data Management) verwaltet und stellt die gesammelten Beschreibungsdaten (engl. Metadata) zu Verfügung. Die Metadaten werden durch den Übernahme-Prozess abgelegt und können durch den Zugriff-Prozess verwendet werden. Dabei kann es sich auch um die Geschäftsanwendung selbst handeln, deren Daten aufbewahrt werden sollen.

Der Zugriff-Prozess (engl. Access) bietet eine Möglichkeit, die gewünschten Daten mithilfe von Metadaten aus dem Datenmanagement zu finden sowie diese auch abzurufen. Die Daten werden dem Speicher in Form eines AIP entnommen und dem Konsumenten in Form eines Ausgabepakets (DIP) zur Verfügung gestellt.

Der Planung und Steuerung der Maßnahmen zur digitalen Bestandserhaltung dienen der Langzeiterhaltung der Dokumente (engl. Preservation Planning). Basierend auf den Metadaten können Maßnahmen umgesetzt werden, welche die Informations- (z. B. Migration der Formate der gespeicherten Inhaltsdaten etc.) und die Beweiswerterhaltung (z. B. Signatur-/Hasherneuerung etc.) gewährleisten.

Mithilfe des Systemadministration-Prozesses (engl. Systemadministration) werden die Aufgaben zum Aufbau und Betrieb, zur Weiterentwicklung, Überwachung und Kontrolle des Langzeitarchivs umgesetzt.

Die Spannweite der Realisierungsmöglichkeiten eines solchen Archivsystems umfasst

- kleine Archivsysteme, z. B. bestehend aus einem Archivserver mit angeschlossenem Massenspeicher als Teil der Geschäftsanwendung, bis hin zu
- komplexen, gegebenenfalls weltweit verteilten Archivsystemen zur institutionsweiten Archivierung von relevanten Geschäftsdaten als verfahrensübergreifende IT-Dienste.

DIN 31644

Das allgemeingültige OAIS-Modell wird in Deutschland durch die DIN 31644 "Kriterien für vertrauenswürdige digitale Langzeitarchive" mit organisatorischen und funktionalen Anforderungen an ein vertrauenswürdiges Langzeitarchiv untermauert. Der Fokus der Norm liegt dabei auf der Informationserhaltung.

DIN 31647

Die DIN 31647 "Beweiswerterhaltung kryptographisch signierter Dokumente" enthält fachliche und funktionale Anforderungen an ein generisches System zur Beweiswerterhaltung kryptografisch signierter Unterlagen unter Wahrung der Authentizität und Integrität (indirekt auch Verfügbarkeit, Nachvollziehbarkeit sowie Verkehrs- und Austauschfähigkeit) innerhalb eines Archivsystems. Die Norm ergänzt somit die DIN 31644.

Eine Referenzarchitektur zur Umsetzung der DIN 31647 und des OAIS-Referenzmodells ist durch die technische Richtlinie BSI TR-03125 (siehe [TR-ESOR]) gegeben.

TR-03125 des BSI

Die Technische Richtlinie TR-03125 Beweiswerterhaltung kryptographisch signierter Dokumente (TR-ESOR) (siehe [TR-ESOR]) auf Basis der Standards [RFC4998] und [RFC6283] wurde vom BSI mit dem Ziel bereitgestellt, die Integrität und Authentizität archivierter Daten und Dokumente bis zum Ende der gesetzlich vorgeschriebenen Aufbewahrungspflicht unter Wahrung des rechtswirksamen Beweiswertes zu erhalten.

Auch kann die TR-03125 (siehe [TR-ESOR]) Abhilfe leisten, wenn nicht signierte Dokumente integritätsgesichert werden sollen.

Die Richtlinie enthält konkrete technische Vorgehensweisen und behandelt dabei die Themen:

- Daten- und Dokumentenformate,
- Empfehlungen zu einer Referenzarchitektur, zu ihren Prozessen, Modulen und Schnittstellen als Konzept einer Middleware,
- Austauschformate für Archivdatenobjekte und Beweisdaten,
- Austauschformate für Schnittstellenspezifikationen
- Konformitätsregeln für die Konformitätsstufe 1 "logisch-funktional" und die Konformitätsstufe 2 "technisch-interoperabel" sowie für die Konformitätsstufe 3 "Bundesbehördenprofil".

Eine Infrastruktur, die TR-03125 (siehe [TR-ESOR]) entspricht, besteht aus mehreren Modulen, die Funktionen zur Beweiswerterhaltung bereitstellen (vgl. Abbildung 3).

Der Einsatz einer TR-03125-Middleware zwischen der IT-Applikation und dem Langzeitspeichersystem empfiehlt sich somit insbesondere

- für kryptografisch signierte Dokumente, die langfristig in dieser Form benötigt werden oder
- falls der Schutzbedarf von Dokumenten sehr hoch ist oder
- wenn ein besonders verkehrsfähiger Integritätsnachweis für Dokumente angestrebt wird.

Die Referenzarchitektur ermöglicht es Softwareherstellern und Benutzern, TR-03125-konforme Systeme aufzubauen und zertifizieren zu lassen.

Die Richtlinie empfiehlt darüber hinaus den Einsatz offener, interoperabler und standardisierter Datenformate und herstellerunabhängiger Schnittstellen entsprechend nationaler und internationaler Standards.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Archivierung" finden sich unter anderem in folgenden Veröffentlichungen:

[DIN31644] DIN 31644:2012-04

Information und Dokumntation - Kriterien für vertrauenswürdige digitale Langzeitarchive, April 2012

[DIN31647] DIN 31647:2015-05

Information und Dokumentation - Beweiswerterhaltung kryptograhisch signierter Dokumente, Mai 2015

[EIDAS-DG] EIDAS-DG

Gesetzt zur Durchführung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaents und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Durchführungsgesetz), Bundesblatt Jahrgang 2017 Teil I Nr. 52, ausgegeben zu Bonn am 28. Juli 2017

[EIDAS-VO] EIDAS-VO

Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG vom 23. Juli 2014

[ISO14721] ISO 14721:2012

International Organization for Standardization (Hrsg.), Space data and information transfer system - Open archival information system (OAIS) - Reference model, September 2012

[RESISCAN] BSI TR-03138 RESISCAN

Ersetzendes Scannen, März 2017, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikation/TechnischeRichtlinien/TR03138/TR-03138.pdf, zuletzt abgerufen am 26.07.2018

[RFC4998] Evidence Record Syntax (ERS)

RFC4998, August 2007, https://www.ieft.org/rfc/rfc4998.txt zuletzt abgerufen am 26.07.2018

[RFC6283] Extensible Markup Language Evidence Record Syntax (XMLERS)

RFC 6283, Juli 2011, https://www.ietf.org/rfc/rfc6283.txt, zuletzt abgerufen am 26.07.2018

[SOG-IS] SOG-IS Crypto Working Group

SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms, 2016, https://www.sogis.org/uk/supporting_doc_en.html, zuletzt abgerufen am 26.07.2018

[TR02102] Kryptographische Verfahren

Empfehlungen und Schlüssellängen: BSI TR-02102, Bundesamt für Sicherheit in der Informationstechnik (BSI), Januar 2018, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html , zuletzt abgerufen am 13.09.2018

[TR-ESOR] BSI TR- 03125 TR-ESOR

Beweiswerterhaltung kryptographisch signierter Dokumente, Hauptdokument, 2014, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125-V1_2.pdf, zuletzt abgerufen am 26.07.2018

[TR-ESOR-B] BSI TR-03125 TR-ESOR

Beweiswerterhaltung kryptographisch signierter Dokumente, Anlage TR-ESOR-B: Profilierung für Bundesbehörden, Januar 2015, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikation/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_B_V1_2.pdf, zuletzt abgerufen am 26.07.2018

[TR-ESOR-E] BSI TR-03125 TR-ESOR

Beweiswerterhaltung kryptographisch signierter Dokumente, Anlage E: Konkretisierung der Schnittstellen auf Basis des eCard-API-Frameworks des eCard-API-Frameworks, 2015, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikation/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2.pdf, zuletzt abgerufen am 26.07.2018

[TR-ESOR-F] BSI TR-03125 TR-ESOR

Beweiswerterhaltung kryptographisch signierter Dokumente, Anlage TR-ESOR-F: Formate, 2015, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikation/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_F_V1_2.pdf, zuletzt abgerufen am 26.07.2018

[TR-ESOR-M3] BSI-TR-03125 TR-ESOR

Beweiswerterhaltung kryptographischer signierter Dokumente, Anlage TR-ESOR-M.3, ArchiSig Modul, 2014, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_M3_V1_2.pdf, zuletzt abgerufen am 26.07.2018

[TR-ESOR-XB] BSI TR-03125 TR_ESOR

Beweiswerterhaltung kryptographisch signierter Dokumente, Anlage TR-ESOR-XBDP, Profilierung des XAIP mit XBARCH, XDOMEA und PREMIS, 2014, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechischeRichtlinien/TR03125/BSI_TR_03125_Anlagen_XBDP_V1_2.pdf, zuletzt abgerufen am 26.07.2018

[TS119132] ETSI: Electronic Signatures and Infrastructures (ESI)

Cryptographic Suites, Version 1.2.1, Mai 2015

[VDG] Vertrauensdienstgesetz - VDG

Artikel 1 des Gesetzes zur Durchführung der Verordnung (EU) NR. 910/2014 des Europäischen Parlaments und des Rates vom 23.Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1993/93/EG (eIDAS-Durchführungsgesetz), Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 52, ausgegeben zu Bonn am 28. Juli 2017

OPS.1.2: Weiterführende Aufgaben

Umsetzungshinweise zum Baustein OPS.1.2.3 Informations- und Datenträgeraustausch

1 Beschreibung

1.1 Einleitung

Für den Informationsaustausch müssen zunächst Vertrauensbeziehungen zwischen den Kommunikationspartnern aufgebaut werden und geklärt werden, wie die ausgetauschten Informationen geschützt werden müssen und wie sie transportiert werden sollen.

Auch bei einer breitbandigen Netzanbindung kann es aus verschiedenen Gründen sinnvoll oder notwendig sein, für den Informationsaustausch Datenträger zu übermitteln. Datenträger können bei persönlichen Treffen oder auch per Versand ausgetauscht werden. Typischerweise verwendete Datenträger sind Wechselplatten, CD-ROMs, DVDs, USB-Sticks und -Festplatten. Dabei sollte nicht vergessen werden, dass auch Papierdokumente Datenträger sind, für die dieselben Sicherheitsanforderungen zu beachten sind, abhängig vom Schutzbedarf der jeweiligen Informationen.

Daneben wird in diesem Baustein auch die Speicherung der Daten auf dem Sender- und Empfänger-System, soweit es in direktem Zusammenhang mit dem Datenträgeraustausch steht, sowie der Umgang mit den Datenträgern vor bzw. nach dem Transfer berücksichtigt.

Beschrieben wird der Prozess des Informations- und Datenträgeraustausches, z. B. bei persönlichen Treffen, über IT-Netze oder auch per Versand.

1.2 Lebenszyklus

Planung und Konzeption

Im Vorfeld des Informations- und Datenträgeraustausches ist zu klären und verbindlich festzulegen, unter welchen Rahmenbedingungen und mit welchen Kommunikationspartnern ein Austausch stattfinden darf (siehe OPS.1.2.3.M2 Regelung des Informationsaustausches und OPS.1.2.3.M7 Regelung des Datenträgeraustausches).

Beschaffung

Die Auswahl geeigneter Datenträger ist mit den Kommunikationspartnern abzustimmen.

Umsetzung

Um Sicherheitsproblemen beim Informationsaustausch vorzubeugen, sollten geeignete Sicherheitsmaßnahmen festgelegt werden, die für die jeweiligen Schutzbedarf, Datenarten und Transportwege angemessen sind. Um eventuelle Schäden durch unsachgemäße Behandlung der Datenträger beim Transport so gering wie möglich zu halten, sollte eine geeignete Versandart festgelegt werden, die, je nach verwendetem Datenträger (z. B. Schriftstücke, CD-ROM, Magnetband) durchaus unterschiedlich sein kann.

Betrieb

Bei der Durchführung des Informations- und Datenträgeraustauschs ist eine Reihe von Maßnahmen zu beachten, um mögliche Schäden zu vermeiden bzw. in ihren Auswirkungen zu minimieren. Dazu gehören Zugriffs- und Manipulationsschutz, z. B. durch Verschlüsselung ebenso wie bei Datenträgern eine sichere Aufbewahrung und Verpackung sowie eine eindeutige Kennzeichnung, um die Verwechslungsgefahr zu verringern. Zur allgemeinen Hygiene gehört bei digitalen Informationen eine Überprüfung auf Computer-Viren vor dem Versenden oder der Übergabe und ebenfalls nach dem Empfang.

Aussonderung

Wenn Datenträger mit unterschiedlichen Kommunikationspartnern ausgetauscht werden, sollten diese Datenträger vor ihrer erneuten Verwendung physikalisch gelöscht werden, um die Übermittlung von Informationsresten an den falschen Empfänger zu vermeiden.

Notfallvorsorge

Da es nie auszuschließen ist, dass Informationen ihren Empfänger nicht erreichen, beispielsweise weil Datenträger beim Transport verloren gehen, sollten die übermittelten Daten zumindest so lange noch lokal in einer Kopie vorgehalten werden, bis der korrekte Empfang bestätigt wurde. Je nach Art und Zweck des Informations- und Datenträgeraustausches kann auch eine längere Speicherung als Beweismittel für spätere Konflikte erforderlich sein.

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Informations- und Datenträgeraustausch" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

OPS.1.2.3.M1 Festlegung zulässiger Kommunikationspartner [Leiter Organisation]

Sollen Informationen an einen Kommunikationspartner außerhalb der eigenen Institution übertragen werden, so muss sichergestellt werden, dass der Empfänger die notwendigen Berechtigungen zum Erhalt und zum Weiterverarbeiten dieser Informationen besitzt. Ebenso muss die Identität des Kommunikationspartners überprüft werden, bevor vertrauliche Informationen weitergegeben werden. Werden Informationen zwischen mehreren kommunizierenden Stellen ausgetauscht, so sollte für alle Beteiligten ersichtlich sein, wer diese Informationen ebenfalls erhalten hat beziehungsweise erhalten wird. Um die oben genannten Kriterien zu erfüllen, muss festgelegt werden, welche Kommunikationspartner welche Informationen erhalten dürfen. Hierfür ist es erforderlich, dass alle Informationen entsprechend ihrer strategischen Bedeutung für die Institution klassifiziert sind.

OPS.1.2.3.M2 Regelung des Informationsaustausches [Leiter Organisation]

Informationen können in unterschiedlichen Formen vorliegen. Meistens werden im Bereich des IT-Grundschutzes in Papierform vorliegende Informationen bzw. elektronisch erfasste Informationen betrachtet. Generell müssen alle Informationen angemessen geschützt werden, angefangen von Gedanken und Ideen über geschriebene und gedruckte Darstellungen bis zu elektronischen Nachrichten, Sprach-, Bild oder Videoaufzeichnungen.

Sollen zwischen zwei oder mehreren Kommunikationspartnern Informationen ausgetauscht werden, so ist zu deren Schutz eine Reihe von unterschiedlichen Aspekten zu beachten. Bei jeder Art von Informationsaustausch ist zunächst zu klären,

- wie schutzbedürftig diese sind,
- mit wem diese ausgetauscht werden dürfen (siehe OPS.1.2.3.M1 Festlegung zulässiger Kommunikationspartner) und
- wie diese dabei zu schützen sind, z. B. indem sie verschlüsselt werden.

Hierfür müssen klare und verständliche Regelungen vorliegen, die alle Formen des Informationsaustausches abdecken, also zum Beispiel den mündlichen Austausch ebenso wie Datenaustausch per Datenträger, Mail, Fax, (Mobil-) Telefon oder Internet. Generell muss sichergestellt sein, dass Informationen nicht in falsche Hände, Augen und Ohren gelangen können und sie nicht unbemerkt verändert werden können.

Allen Mitarbeitern muss bewusst sein, dass sie dafür verantwortlich sind, interne Informationen angemessen zu schützen. Beispielsweise dürfen Ideenskizzen auf Papier nicht in Besprechungsräumen liegengelassen werden, Projektplanungen nicht in öffentlichen Verkehrsmitteln oder im Restaurant diskutiert werden, Anrufern nicht ungeprüft Interna mitgeteilt werden. Schutzbedürftige Informationen dürfen nicht unbeaufsichtigt an Druckern oder Faxgeräten ausgedruckt oder gar liegengelassen werden. Wandtafeln und Whiteboards in Besprechungs-, Schulungs- und Veranstaltungsräumen müssen am Ende der jeweiligen Sitzung gereinigt werden, benutzte Flipchart-Blätter sind gegebenenfalls zu entfernen. Mitarbeiter sollten regelmäßig auf solche Aspekte hingewiesen werden, beispielsweise über passende Erläuterungen und Veranschaulichungen im Intranet oder in der Hauszeitung.

Die Empfänger müssen darauf hingewiesen werden, dass die übermittelten Daten nur zu dem Zweck benutzt werden dürfen, zu dem sie weitergegeben wurden. Auch aus Datenschutzgründen (siehe zum Beispiel BDSG, Weitergabekontrolle) sollte eine Übersicht erstellt werden, welche Empfänger berechtigt sind, Informationen, insbesondere personenbezogene Daten, per Datenübertragung oder Datenträgeraustausch zu erhalten.

Beispiel:

Eine Institution schließt mit einem Cloud-Diensteanbieter einen Vertrag zur Nutzung eines definierten Cloud Services. Der gewählte Cloud-Diensteanbieter nutzt zur Leistungserbringung seinerseits Services eines Subauftragnehmers und gibt die Daten der Institution zur Verarbeitung an diesen weiter. Alle Kommunikationswege sowie die Art und der Umfang der weitergegebenen Daten sind in diesem Fall durch den Cloud-Diensteanbieter transparent darzulegen.

Bei Kommunikationspartnern sollte regelmäßig überprüft werden, ob diese berechtigt sind, die jeweiligen Informationen zu erhalten. So könnte sich unter anderem die Firmenzugehörigkeit, die Post- oder E-Mail-Adresse oder die Faxnummer geändert haben und übermittelte Informationen so die Falschen erreichen. Bei einem Erstkontakt sollte zusätzlich die Identität des Gegenübers überprüft werden, da Visitenkarten auf beliebige Namen ausgestellt werden können. Daher ist es zu empfehlen, bei neuen Geschäftspartnern Rückfrage in deren Behörde oder Unternehmen zu halten oder Referenzen einzuholen.

Wie analoge und elektronische Informationen beim Informationsaustausch zu schützen sind, ist unter anderem ausführlich im Baustein APP.1.1 E-Mail/Groupware beschrieben.

OPS.1.2.3.M3 Unterweisung des Personals zum Informationsaustausch [Fachverantwortliche]

Mitarbeiter müssen ausreichend darüber informiert werden, welche Rahmenbedingungen und Restriktionen bei der Informationsweitergabe einzuhalten sind (siehe OPS.1.2.3.M2 Regelung des Informationsaustausches). Wenn sie hierin nur unzulänglich eingewiesen werden, kann dies zu einer Vielzahl von Sicherheitsproblemen führen. Hierzu gehört beispielsweise, dass Mitarbeiter darüber informiert werden,

- mit welchen Kommunikationspartnern welche Informationen ausgetauscht werden dürfen (siehe OPS.1.2.3.M1 Festlegung zulässiger Kommunikationspartner),
- dass die Identität der Kommunikationspartner überprüft werden sollte, bevor vertrauliche Informationen weitergegeben werden,
- in welchen Räumlichkeiten Informationen kommuniziert und verarbeitet werden dürfen,
- über welche IT-Netze Informationen transportiert werden dürfen und wie diese dabei abzusichern sind,
- welche Arten von Datenträger für Datenträgeraustausch zulässig sind und wie diese abzusichern sind.

Außerdem sind die prinzipiellen Schritte für den Ablauf eines Informations- und Datenträgeraustausches zu fixieren und zu veröffentlichen, z. B. im Intranet. Die Mitarbeiter sind zur Einhaltung der Regelungen zu verpflichten.

Zusätzlich müssen die am Informations- und Datenträgeraustausch beteiligten Mitarbeiter sensibilisiert werden, welche konkreten Gefährdungen vor, während und nach dem Transport bestehen. Dementsprechend müssen diese Mitarbeiter ausführlich mit den einzuhaltenden Sicherheitsmaßnahmen vertraut gemacht werden.

Bevor digitale Datenträger eingelesen werden, die im Postfach lagen, obwohl sie nicht erwartet wurden, sollte bei den angegebenen Absendern nachgefragt werden, ob sie die Datenträger wirklich geschickt haben (siehe auch OPS1.1.4 Schutz vor Schadprogrammen). Dasselbe ist bei E-Mail oder anderer Kommunikation zu beachten. Bei unbekanntem Absender oder nicht erwarteten Lieferungen sollte das Sicherheitsmanagement informiert werden, wenn von der Leitungsebene keine anderen Regelungen für diesen Fall verabschiedet wurden.

Werden bestimmte IT-gestützte Verfahren zum Schutz der Daten während des Austausches eingesetzt (wie etwa Verschlüsselung oder Checksummen-Verfahren), so sind die dafür zuständigen Mitarbeiter in die Handhabung dieser Verfahren ausreichend einzuarbeiten.

OPS.1.2.3.M4 Schutz vor Schadsoftware [Benutzer]

Unmittelbar vor und unmittelbar nach einer Datenübertragung sowie beim Austausch bzw. beim Versand von Datenträgern müssen diese auf Schadsoftware überprüft werden (siehe OPS1.1.4 Schutz vor Schadprogrammen). Dabei ist darauf zu achten, dass das eingesetzte Schutzprogramm auch Makro-Viren erkennen kann und es sich auf einen aktuellen Stand befindet.

Der Absender sollte ein Protokoll der Schadsoftware-Überprüfung dem übermittelten Datenträger beifügen oder einer Datei, die elektronisch versandt wird, anhängen. Es empfiehlt sich, dieses Protokoll als Kopie zu verwahren. Der Empfänger hätte anhand dieses Protokolls einen ersten Eindruck von der Integrität der übermittelten Daten. Dies entbindet den Empfänger jedoch nicht von einer erneuten Schadsoftware-Überprüfung. Der Absender kann andererseits bei eventuellen Beschwerden bezüglich Schadsoftwareplausibel machen, dass ein Befall bei ihm unwahrscheinlich war.

OPS.1.2.3.M5 Verlustmeldung [Benutzer]

Verlust oder Diebstahl eines Datenträgers beim Datenträgeraustausch oder der Verdacht auf Manipulation muss umgehend gemeldet werden. Das gilt auch für private Datenträger, die dienstlich genutzt werden. Hierfür muss es in jeder Institution klare Meldewege und Ansprechpartner geben. Bei Verlust eines Datenträgers muss schnell gehandelt werden, da es hier nicht nur darum geht, die Daten zu übermitteln, sondern auch darum, potenziellen Missbrauch der betroffenen Informationen zu verhindern.

Wenn sich auf den Datenträgern vertrauliche Daten befunden haben, muss nach deren Verlust umgehend gehandelt werden, beispielsweise:

- Als vertraulich eingestufte Informationen (z. B. Patientenakten): Alle betroffenen Bereiche (z. B. Fachabteilung, Kunden, etc.) müssen benachrichtigt werden, um entsprechende Maßnahmen ergreifen zu können.

Auch Defekte bei geringpreisigen mobilen Datenträgern sollten gemeldet werden, damit das IT-Management erkennen kann, ob hiervon größere Lieferungen betroffen sind. Insbesondere bei Datenträgern, die für Datensicherungen und Archivierung eingesetzt werden, ist eine hohe Verlässlichkeit und eine lange Lebensdauer wichtig.

Wenn verlorene Datenträger wieder auftauchen, müssen sie auf eventuelle Manipulationen untersucht werden. Besteht ein Verdacht, muss das Gerät entweder gleich entsorgt oder von einem Spezialisten weiter untersucht werden. Um sicherzustellen, dass sich keine manipulierten Programme oder Schadsoftware auf den wiedererlangten Datenträgern befinden, sollten sie physikalisch gelöscht werden (siehe OPS.1.2.3.M8 Physikalisches Löschen von Datenträgern vor und nach Verwendung).

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Informations- und Datenträgeraustausch".

OPS.1.2.3.M6 Vereinbarungen zum Informationsaustausch mit Externen [Leiter Organisation]

Bei einem regelmäßigen Informationsaustausch mit externen Partnern sollten die Rahmenbedingungen hierfür vereinbart werden. Dabei sollte geklärt werden, wie das gegenseitige Verständnis vom Schutzbedarf der Informationen ist. Falls notwendig, sollte ein gemeinsames Klassifikationsschema genutzt werden. Außerdem sollte festgehalten werden:

- ob und wie welche Arten von Informationen zu schützen sind,
- über welche Übertragungswege der Informationsaustausch überhaupt stattfinden darf,
- dass Vertraulichkeitsvereinbarungen durch die beteiligten Mitarbeiter unterzeichnet werden (siehe auch OPS.1.2.3.M10 Abschluss von Vertraulichkeitsvereinbarungen),
- dass Informationen nur dann an Dritte weitergegeben werden dürfen, wenn der Ersteller bzw. Informationseigentümer dem zustimmt,
-
- auf welche Art und Weise das im Informationsverbund des Partners etablierte Sicherheitsniveau nachgewiesen wird, beispielsweise per Audit,
- wie über Sicherheitsvorfälle an die Partner berichtet werden soll,
- wie Streitfälle über den Umgang mit Informationen eskaliert werden,
- wie Frühwarnungen über mögliche Sicherheitsprobleme ausgetauscht werden,
- welche rechtlichen Rahmenbedingungen zu beachten sind.

Bei Sicherheitsvorfällen oder in Notfällen kann die normale Form der Kommunikation zwischen den Partnern gestört sein. Es sollte geklärt sein, ob in solchen Fällen der Informationsaustausch weiter betrieben werden soll. Falls ja, sollten gemeinsam entsprechende Notfallpläne erarbeitet werden.

OPS.1.2.3.M7 Regelung des Datenträgeraustausches [Leiter Organisation]

Der ordnungsgemäße Datenträgeraustausch sollte auf Basis der Vorgaben für den Informationsaustausch geregelt werden (siehe OPS.1.2.3.M2 Regelung des Informationsaustausches). Hierbei sollten im Vorfeld die berechtigten Empfänger sowie geeignete Versandarten für die verschiedenen Arten von Datenträgern und auszutauschenden Informationen festgelegt werden. Außerdem sollte festgelegt werden, wie die Datenträger in der eigenen Institution, beim Transport und beim Empfänger zu schützen sind.

Sollen zwischen zwei oder mehreren Kommunikationspartnern Datenträger ausgetauscht werden, so sind zum ordnungsgemäßen Austausch eine Reihe von Empfehlungen zu beachten.

Abhängig von der Art der Datenträger und des Schutzbedarfs der Daten muss eine geeignete Versandart festgelegt werden. Dabei sind insbesondere die Art der Datenträger und der Schutzbedarf der Informationen zu berücksichtigen.

Neben den in OPS.1.2.3.M14 Datenträgerverwaltung dargestellten Umsetzungshinweisen sollte sich die Versandart der Datenträger am Gefährdungspotential orientieren. Hinsichtlich Verfügbarkeit ist die Versandart derart auszuwählen, dass eine rechtzeitige Zustellung garantiert werden kann. Je mehr Personen mit der Beförderung befasst und je länger die Zeiten sind, in denen der Datenträger unbeaufsichtigt bleibt, desto weniger kann im Allgemeinen die Vertraulichkeit und Integrität garantiert werden. Dementsprechend sind angemessene Versandarten auszuwählen.

Man kann dabei z. B. zwischen folgenden Versandarten wählen:

- Post (mit verschiedenen Versandangeboten, die unterschiedliche Garantien für die Transportgeschwindigkeit und Absicherung umfassen),
- Kurierdienste,
- persönlicher Kurier und
- persönliche Übergabe.

Für eine Behörde oder ein Unternehmen empfiehlt es sich, eine Liste zu führen, in der für verschiedene Datenträger und deren Schutzbedarf angemessene Versandarten vorgeschlagen werden. Dies erleichtert den Mitarbeitern die Auswahl nicht nur in Bezug auf das bestmögliche Preis-Leistungs-Verhältnis, sondern auch auf die optimale Sicherheit. Diese Liste sollte mindestens folgende Aspekte umfassen:

- durchschnittliche Transportzeit der Versandart bzw. des Kuriers
- Vertrauenswürdigkeit der Versandart bzw. des Kuriers
- Kosten.

Die Adressierung muss eindeutig erfolgen, um eine fehlerhafte Zustellung zu vermeiden. So sollten neben dem Namen des Empfängers auch die Organisationseinheit und die genaue Bezeichnung der Behörde bzw. des Unternehmens angegeben sein. Innerhalb einer Institution sollten Verzeichnisse der gebräuchlichsten Adressen gepflegt werden, damit möglichst aktuelle und korrekte Adressen der Empfänger verwendet werden.

Auch die Adresse des Absenders muss eindeutig und vollständig angegeben werden. Hierfür sollte innerhalb der Institution eine Vorgabe erstellt werden, die den Umfang und den Aufbau der Absender-Angabe einheitlich regelt.

Digitalen Datenträgern sollte (optional) ein Datenträgerbegleitzettel beigelegt werden, der folgende Informationen umfasst:

- Absender,
- Empfänger,
- Art und Menge der Datenträger,
- Seriennummer (soweit vorhanden),
- Identifikationsmerkmal für den Inhalt des Datenträgers,
- Datum des Versandes, gegebenenfalls Datum bis wann der Datenträger spätestens den Empfänger erreicht haben muss,
- Hinweis, dass Datenträger auf Viren überprüft sind,
- Parameter, die zum Lesen der Informationen benötigt werden, z. B. Bandgeschwindigkeit.

Jedoch sollte nicht vermerkt werden,

- welches Passwort für die eventuell geschützten Informationen vergeben wurde,
- welche Schlüssel für eine Verschlüsselung der Informationen verwendet wurde,
- welchen Inhalt der Datenträger hat.

Der korrekte Empfang sollte überprüft werden. Bei Sendungen mit hochvertraulichen oder termingebundenen Inhalten sollten die Empfänger über die Absendung und den gewählten Transportweg informiert werden. Bei hohem Schutzbedarf empfiehlt es sich, den Empfänger um eine Empfangsbestätigung zu bitten.

Es sind jeweils Verantwortliche für den Versand und für den Empfang zu benennen. Ergeben sich Hinweise auf Manipulationen oder einen Verlust, ist sofort das Sicherheitsmanagement zu unterrichten.

OPS.1.2.3.M8 Physikalisches Löschen von Datenträgern vor und nach Verwendung [Benutzer]

Neben den in OPS.1.1.8 Löschen und Vernichten enthaltenen Hinweisen zur Löschung oder Vernichtung von Datenträgern sind für den Datenträgeraustausch folgende Punkte zu beachten:

Datenträger, die für den Austausch bestimmt sind, sollten vor dem Beschreiben mit den zu übermittelnden Informationen physikalisch gelöscht werden. Es soll damit sichergestellt werden, dass keine Restdaten weitergegeben werden, für deren Erhalt der Empfänger keine Berechtigung besitzt.

Eine für den normalen Schutzbedarf ausreichende physikalische Löschung kann erreicht werden, indem der komplette Datenträger oder zumindest die genutzten Bereiche mit einem bestimmten Muster überschrieben werden. Bei magnetischen Datenträgern ist bereits ein einmaliges Überschreiben ausreichend. Bei Datenträgern, die auf Flash-Speicher basieren, wie etwa USB-Sticks, kann aus technischen Gründen nicht sichergestellt werden, dass ein vollständiges Überschreiben auch tatsächlich alle gespeicherten Daten löscht. Für den normalen Schutzbedarf ist dies jedoch ebenfalls ausreichend. Bei erhöhtem Schutzbedarf sollte auf die Verwendung von Flash-Speicher verzichtet werden, oder der Speicher sollte vollständig verschlüsselt werden. Möglich ist auch eine Formatierung des Datenträgers, wenn diese nicht wieder rückgängig gemacht werden kann, also keine Schnellformatierung. Es sollte vermieden werden, nur einzelne Dateien zu löschen, hierbei bleiben häufig Restinformationen erhalten, die die Rekonstruktion der gelöschten Dateien ermöglichen. Den Mitarbeitern sollten geeignete Programme zum physikalischen Löschen vor und nach Verwendung von Datenträgern zur Verfügung gestellt werden.

In der Regel sind die übertragenen Daten auch für den Empfänger schützenswert. Analog ist auch hier nach dem Wiedereinspielen der Daten eine physikalische Löschung des Datenträgers vorzusehen.

Auf den Einsatz von nicht-löschbaren Datenträgern (wie z. B. WORMs) ist zum Zwecke des Datenaustausches dann zu verzichten, wenn sich darauf weitere, nicht für den Empfänger bestimmte Informationen befinden, die nicht gelöscht werden können.

OPS.1.2.3.M9 Beseitigung von Restinformationen in Dateien vor Weitergabe [Benutzer]

Vor dem Versenden einer Datei per E-Mail, IT-Netze oder Datenträgeraustausch bzw. vor dem Veröffentlichen einer Datei auf einem Webserver sollte diese daraufhin überprüft werden, ob sie Restinformationen enthält, die nicht zur Veröffentlichung bestimmt sind. Solche Restinformationen können verschiedenen Ursprungs sein und dementsprechend unterschiedlich können auch die Aktionen sein, die dagegen zu unternehmen sind. Die häufigsten Ursachen für solche Restinformationen sind im Folgenden beschrieben.

Generell sollte Standard-Software wie z. B. für Textverarbeitung oder Tabellenkalkulation darauf überprüft werden, welche Zusatzinformationen in damit erstellten Dateien gespeichert werden. Dabei werden einige dieser Informationen mit, andere ohne Wissen des Benutzers gespeichert.

Vor der Weitergabe von Dateien sollten diese zumindest stichprobenartig auf unerwünschte Zusatzinformationen überprüft werden. Dazu sollte ein anderer Editor benutzt werden als der, mit dem die Datei erstellt wurde.

Dabei ist darauf zu achten, dass nicht alle Restinformationen einfach gelöscht werden können, ohne das Dateiformat zu zerstören. Wenn z. B. aus einer Textverarbeitungsdatei einige Bytes gelöscht werden, erkennt das Textverarbeitungsprogramm unter Umständen das Dateiformat nicht mehr. Um Restinformationen zu beseitigen,

- kann die Datei in einem anderen Dateiformat abgespeichert werden, z. B. als "Nur-Text", als Druckausgabe in PDF oder als HTML,
- können die Nutzdaten in eine zweite Instanz derselben Standard-Software kopiert werden, wobei auf dem IT-System keine andere Applikation laufen sollte. Dies empfiehlt sich insbesondere bei Dateien mit einer größeren Änderungshistorie.

Um der Weitergabe von Informationen vorzubeugen, die ursprünglich mit Wissen der Ersteller eingebracht worden sind, wie z. B. als "verborgen" formatierter Text, dessen Vorhandensein dann aber vergessen wurde, kann es sinnvoll sein, die Datei ausdrucken. Dabei sollten dann alle Optionen aktiviert werden, die beim Drucken versteckte Informationen mit ausgeben.

Restinformationen im Dateisystem

Wenn eine Datei auf normalem Wege gelöscht wird, so markiert das Betriebssystem diese nur im Dateisystem als gelöscht, ohne die eigentlichen Inhalte ebenfalls zu entfernen. Bei der Weitergabe von Datenträgern ist dies entsprechend zu berücksichtigen, da sonst z. B. gelöschte Zwischenversionen oder temporäre Dateien vom Empfänger wiederhergestellt werden könnten. Daneben haben viele Applikationen das Problem, dass das jeweilige Programm bei der Bearbeitung einer Datei den in Anspruch genommenen Speicherplatz nicht durchgehend mit Applikationsdaten überschreibt, sodass Lücken entstehen können, die ebenfalls alte Datenbestände enthalten können.

Dateien mit sensiblen Informationen sollten also nicht unmittelbar auf einem zur Weitergabe bestimmten Datenträger bearbeitet werden. Stattdessen sollte die finale Version der Datei vor der Weitergabe auf einen gemäß OPS.1.2.3.M8 Physikalisches Löschen von Datenträgern vor und nach Verwendung gelöschten Datenträger kopiert werden.

Zusätzlich sind besondere Eigenschaften des verwendeten Dateisystems zu beachten. So speichert das unter Windows übliche Dateisystem NTFS den Inhalt sehr kleiner Dateien (bis etwa 700 Bytes) direkt in der NTFS-Verwaltungsstruktur, der sogenannten Master File Table (MFT). Bei Dateien dieser Größe handelt es sich häufig um Konfigurationseinstellungen oder Meta-Informationen. Wachsen diese Dateien später, so bleiben die ursprünglichen Inhalte in der MFT unter Umständen erhalten. Außerdem können bei NTFS Informationen in Alternate Data Streams (ADS) gespeichert sein, die nicht direkt sichtbar sind. Handelt es sich um sensible Informationen, so ist eine Weitergabe im Normalfall nicht erwünscht. ADS können mit speziellen Tools betrachtet und entfernt werden, oder man kopiert die Datei in ein Dateisystem, das ADS nicht unterstützt (etwa FAT32 oder exFAT).

Verborgener Text / Kommentare

Eine Datei kann Textpassagen enthalten, die als "versteckt" oder "verborgen" formatiert sind. Einige Programme bieten auch die Möglichkeit an, Kommentare hinzuzufügen, die auf dem Ausdruck und oft auch am Bildschirm ausgeblendet sind. Solche Textpassagen können Bemerkungen enthalten, die nicht für den Empfänger bestimmt sind. Daher müssen in Dateien, bevor sie an Externe weitergegeben werden, solche Zusatzinformationen gelöscht werden.

Änderungsmarkierungen

Bei der Bearbeitung von Dateien kann es sinnvoll sein, hierbei Änderungsmarkierungen zu verwenden. Da diese auf dem Ausdruck und am Bildschirm ausgeblendet werden können, muss vor der Weitergabe von Dateien ebenfalls überprüft werden, ob diese Änderungsmarkierungen enthalten.

Versionsführung

In praktisch allen aktuellen Office-Suites gibt es die Möglichkeit, verschiedene Versionen eines Dokumentes in einer Datei zu speichern. Dies dient dazu, um bei Bedarf auf frühere Überarbeitungsstände zurückgreifen zu können. Dies kann aber sehr schnell zu riesigen Dateien führen, z. B. wenn Graphiken mitgeführt werden. Auf keinen Fall sollte die Option "Version beim Schließen automatisch speichern" gewählt werden, da hier bei jedem Schließen einer Datei die komplette Vorgängerversion zusätzlich gespeichert wird.

Dateieigenschaften

Als Dateieigenschaften oder Datei-Info werden in der Datei Informationen gespeichert, die bei späteren Suchen helfen sollen, Dateien wieder zu finden. Dabei können je nach Applikation Informationen wie Titel, Verzeichnisstrukturen, Versionsstände, Bearbeiter (nicht nur der Unterschreibende), Kommentare, Bearbeitungszeit, letztes Druckdatum, Dokumentnamen und -beschreibungen enthalten sein. Einige dieser Informationen werden von den Programmen selber angelegt und können nicht durch den Bearbeiter beeinflusst werden. Andere Informationen müssen manuell eingegeben werden. Vor der Weitergabe einer Datei an Externe ist zu überprüfen, welche zusätzlichen Informationen dieser Art die Datei enthält.

Schnellspeicherung

Manche Anwendungen, wie ältere Textverarbeitungsprogramme, nutzen die Option der Schnellspeicherung, um nur die Veränderungen seit der letzten Sicherung und nicht das gesamte Dokument speichern zu müssen. Dieser Vorgang nimmt unter Umständen weniger Zeit in Anspruch als ein vollständiger Speichervorgang. Der entscheidende Nachteil ist jedoch, dass die Datei unter Umständen Fragmente der Vorgängerversion enthalten kann, die durch die Überarbeitung hätten beseitigt werden sollen. Grundsätzlich sollten daher Schnellspeicherungsoptionen abgeschaltet werden.

Entscheidet sich der Benutzer trotzdem für die Schnellspeicheroption, sollte er bei folgenden Situationen immer einen vollständigen Speichervorgang durchführen:

- wenn die Bearbeitung eines Dokuments abgeschlossen ist,
- bevor eine weitere Anwendung ausgeführt wird, die viel Speicherplatz in Anspruch nimmt,
- bevor der Dokumenttext in eine andere Anwendung übertragen wird,
- bevor das Dokument in ein anderes Dateiformat konvertiert wird und
- bevor das Dokument per E-Mail oder Datenträgeraustausch versandt wird.

Die Benutzer sollten hinsichtlich der Gefahren von Rest- und Zusatzinformationen in Dateien informiert werden und ihnen die Problematik beispielhaft aufgezeigt werden. Es sollten stichprobenhafte Überprüfungen der Dateien auf enthaltene Restinformationen durchgeführt werden. Den Benutzern sollte vermittelt werden, wie sie Rest- und Zusatzinformationen in Dateien vermeiden können.

OPS.1.2.3.M10 Abschluss von Vertraulichkeitsvereinbarungen [Leiter Organisation]

Wenn beim Informationsaustausch vertrauliche Informationen an Externe weitergegeben werden, sollte diese dazu verpflichtet werden, diese ebenfalls vertraulich zu behandeln. Dazu muss zunächst ein gemeinsames Verständnis vom Schutzbedarf der Informationen hergestellt werden. Außerdem sollten Vertraulichkeitsvereinbarungen (Non-Disclosure-Agreements) abgeschlossen werden.

In einer Vertraulichkeitsvereinbarung sollte beschrieben sein,

- welche Informationen vertraulich behandelt werden müssen,
- für welchen Zeitraum diese Vertraulichkeitsvereinbarung gilt,
- welche Aktionen bei Beendigung dieser Vereinbarung vorgenommen werden müssen, z. B. Vernichtung oder Rückgabe von Datenträgern,
- wie die Eigentumsrechte an Informationen geregelt sind,
- welche Regelungen für den Gebrauch und die Weitergabe von vertraulichen Informationen an weitere Partner gelten, falls dies notwendig ist,
- welche Konsequenzen bei Verletzung der Vereinbarung eintreten.

Vertraulichkeitsvereinbarungen können mit einzelnen Personen oder mit anderen Institutionen geschlossen werden. Wird eine Vertraulichkeitsvereinbarung mit einer Institution geschlossen, muss diese alle betroffenen Mitarbeiter darüber unterrichten und diese auf die Einhaltung verpflichten.

In der Vertraulichkeitsvereinbarung kann auch auf die relevanten Sicherheitsrichtlinien und weitere Richtlinien der Institution hingewiesen werden. Eine Vertraulichkeitsvereinbarung bietet die rechtliche Grundlage für die Verpflichtung Externer zur vertraulichen Behandlung von Informationen. Aus diesem Grund muss sie alle relevanten Gesetze und Bestimmungen für die Institution in dem speziellen Einsatzbereich berücksichtigen, klar formuliert sein und aktuell gehalten werden.

Es kann sinnvoll sein, verschiedene Vertraulichkeitsvereinbarungen je nach Einsatzzweck zu verwenden. In diesem Fall muss klar definiert werden, welche Vereinbarung für welche Fälle notwendig ist.

Ein Beispiel für eine Vertraulichkeitsvereinbarung das "Traffic Light Protocol" (TLP). Dieses wird beispielsweise für die Kommunikation in der Allianz für Cyber-Sicherheit oder zwischen CERTs genutzt. Diese Verpflichtung dient der Schaffung von Vertrauen bzgl. des Schutzes ausgetauschter Informationen durch Regelung der Weitergabe mithilfe des TLP. Das TLP kann auch als Beispiel für die Gestaltung eigener Vertraulichkeitsvereinbarungen genutzt werden, siehe hierzu auch das Merkblatt zur Behandlung vertraulicher Informationen unter [ACS1].

OPS.1.2.3.M11 Kompatibilitätsprüfung des Sender- und Empfängersystems [IT-Betrieb]

Vor einem Informationsaustausch sollten die eingesetzten Systeme und Produkte auf Sender- und Empfängerseite auf ihre Kompatibilität geprüft werden.

Beim Datenträgeraustausch lassen sich Informationen abhängig vom Grad der Kompatibilität von Empfänger- und Sendersystem mehr oder weniger zuverlässig übertragen. Dabei sind je nach Komplexität auszutauschender Daten unterschiedliche Anforderungen an die Kompatibilität zu stellen. Vor Einrichtung eines regelmäßigen Informations- oder Datenträgeraustausches sollte daher die Übereinstimmung folgender Eigenschaften überprüft werden, um im Vorfeld Inkompatibilitäten festzustellen und wo erforderlich Abhilfe zu schaffen:

- Physikalisches Medium:
  Beim Datenträgeraustausch ist natürlich notwendig, dass die **physikalischen Medien** von Empfänger- und Sendersystem übereinstimmen. Dabei reicht aber mechanische Äquivalenz noch nicht aus, denn die Nichtübereinstimmung von Parametern wie Geschwindigkeit bei Bändern kann zu Problemen führen.
- Zeichencode (z. B. ASCII oder EBCDIC):
  Stimmen Sender- und Empfängersystem im verwendeten **Zeichencode** überein, so sind mit Hilfe des physikalischen Lesens einzelne Sektoren bzw. Blöcke im Klartext lesbar, die unzusammenhängend auf dem Datenträger verteilt sein können. Stimmen die verwendeten Zeichencodes nicht überein, werden die übertragenen Daten falsch interpretiert.
- Formatierung des Betriebs- bzw. Dateisystem von Datenträgeren:
  Verfügen beim Datenträgeraustausch Sender- und Empfänger-System darüber hinaus über das gleiche Betriebs- und Dateisystem oder sieht das Empfängerbetriebssystem vor, Formatierungen anderer Betriebssystem zu lesen (z. B. können nicht alle Unix-Betriebssysteme NTFS-Datenträger einlesen), dann können alle Dateien, wie sie beim Absender vorlagen, wiederhergestellt werden. Dies ist für Informationen ausreichend, die keiner weiteren Formatierung, wie sie von den meisten Anwendungsprogrammen (z. B. Textverarbeitungsprogrammen) vorgenommen werden, unterliegen.
- Anwendungssoftware:
  Wurden Anwendungsprogramme zur Erzeugung der zu übermittelten Dateien verwendet, ist auf Versionsgleichheit dieser Programme zu achten, da die Dateiformate evtl. unterschiedlich sein können. Die Versionsgleichheit muss nicht bestehen, wenn die Programmversionen aufwärts- bzw. abwärtskompatibel sind.
- Sicherheitssoftware und Sicherheitsparameter:
  Werden darüber hinaus Sicherheitsprodukte oder Schutzmechanismen bestimmter Anwendungsprogramme verwendet, so ist die Kompatibilität dieser Produkte sicherzustellen.
  Über die verwendeten Schlüssel oder Passwörter müssen sich Absender und Empfänger auf geeignetem Wege verständigen.

Treten Inkompatibilitäten auf, so sind zusätzliche Vorkehrungen bzw. Produkte bereitzustellen, die eine entsprechende Konvertierung vorsehen, oder die Absender- und Empfängersysteme sind geeignet auszustatten.

OPS.1.2.3.M12 Angemessene Kennzeichnung der Datenträger beim Versand [Benutzer]

Bei einer ausreichenden Kennzeichnung von auszutauschenden Datenträgern ist darauf zu achten, dass Absender und (alle) Empfänger unmittelbar zu identifizieren sind. Die Kennzeichnung der Datenträger bzw. deren Verpackung muss den Inhalt der Datenträger eindeutig für den Empfänger erkennbar machen. Es ist jedoch bei schützenswerten Informationen wichtig, dass diese Kennzeichnung für Unbefugte keinen Rückschluss auf die Art und Inhalte der gespeicherten Informationen zulässt.

Für Verschlusssachen sind in jedem Fall die jeweils gültigen Geheimschutzvorschriften einzuhalten.

Darüber hinaus sollten die Datenträger mit den verwendeten Formaten beziehungsweise den für das Auslesen notwendigen Parametern gekennzeichnet werden. So ist bei der Übermittlung von DVDs unter anderem zu vermerken, ob es sich um Video-, Audio- oder Daten-DVDs handelt. Weitere nützliche Kennzeichnungen können Datum des Versandes bzw. der Erstellung der Daten, eventuelle Versionsnummern oder Ordnungsmerkmale sein.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

OPS.1.2.3.M13 Verschlüsselung und digitale Signaturen [Benutzer] (CI)

Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen

Werden vertrauliche Informationen oder Informationen mit hohem Integritätsanspruch übertragen und besteht eine gewisse Möglichkeit, dass diese Daten Unbefugten zur Kenntnis gelangen, von diesen manipuliert werden oder durch technische Fehler verändert werden können, sollte ein kryptographisches Verfahren zum Schutz der Daten für den Transport oder die Übermittlung eingesetzt werden.

Vertraulichkeitsschutz durch Verschlüsselung

Vertrauliche Informationen sollten vor einer Übertragung verschlüsselt werden. Das entscheidende Merkmal eines Verschlüsselungsverfahrens ist die Güte des Algorithmus sowie der Schlüsselauswahl. Ein anerkannter Algorithmus, der für den normalen Schutzbedarf ausreicht, ist der Advanced Encryption Standard (AES), siehe auch CON.1 Kryptokonzept.

Um den Anforderungen der Vertraulichkeit der zu übertragenden Informationen zu entsprechen, müssen das IT-System des Absenders und des Empfängers den Zugriffsschutz auf das Verschlüsselungsprogramm ausreichend gewährleisten. Gegebenenfalls sollte dieses Programm auf einem auswechselbaren Datenträger gespeichert, in der Regel verschlossen aufbewahrt und nur bei Bedarf eingespielt und genutzt werden.

Integritätsschutz durch Checksummen, Verschlüsselung oder Digitaler Signaturbildung

Ist für den Datenaustausch lediglich die Integrität der zu übermittelnden Daten sicherzustellen, muss unterschieden werden, ob ein Schutz nur gegen zufällige Veränderungen, z. B. durch Übertragungsfehler, oder auch gegen Manipulationen geleistet werden soll. Sollen ausschließlich zufällige Veränderungen erkannt werden, können Checksummen-Verfahren (z. B. Cyclic Redundancy Checks) oder fehlerkorrigierende Codes zum Einsatz kommen. Schutz gegenüber Manipulationen bieten darüber hinaus Verfahren, die unter Verwendung eines symmetrischen Verschlüsselungsalgorithmus (z. B. Tripel-DES) aus der zu übermittelnden Information einen so genannten Message Authentication Code (MAC) erzeugen. Andere Verfahren bedienen sich eines asymmetrischen Verschlüsselungsalgorithmus (z. B. RSA) in Kombination mit einer Hashfunktion und erzeugen eine "Digitale Signatur". Die jeweiligen erzeugten "Fingerabdrücke" (Checksumme, fehlerkorrigierende Codes, MAC, Digitale Signatur) werden zusammen mit der Information an den Empfänger übertragen und können von diesem überprüft werden.

Weitere Informationen zum Einsatz kryptographischer Verfahren und Produkte finden sich in Baustein CON.1 Kryptokonzept.

Geeignetes Schlüsselmanagement

Die Verwendung kryptographischer Sicherheitsmechanismen (z. B. Verschlüsselung, digitale Signatur) setzt die vertrauliche, integere und authentische Erzeugung, Verteilung und Installation von geeigneten Schlüsseln voraus. Schlüssel, die Unbefugten zur Kenntnis gelangt sind, bei der Verteilung verfälscht worden sind oder gar aus unkontrollierter Quelle stammen (dies gilt auch für die Schlüsselvereinbarung zwischen Kommunikationspartnern), können den kryptographischen Sicherheitsmechanismus genauso kompromittieren wie qualitativ schlechte Schlüssel, die auf ungeeignete Weise erzeugt worden sind. Qualitativ gute Schlüssel werden in der Regel unter Verwendung geeigneter Schlüsselgeneratoren erzeugt. Für das Schlüsselmanagement sind folgende Punkte zu beachten:

- Schlüsselerzeugung: Die Schlüsselerzeugung sollte in sicherer Umgebung und unter Einsatz geeigneter Schlüsselgeneratoren erfolgen.
- Schlüsseltrennung: Kryptographische Schlüssel sollten möglichst nur für einen Einsatzzweck dienen. Insbesondere sollten für die Verschlüsselung immer andere Schlüssel als für die Signaturbildung benutzt werden.
- Schlüsselverteilung / Schlüsselaustausch: Die Kommunikationspartner müssen über aufeinander abgestimmte kryptographische Schlüssel verfügen. Dazu müssen alle Kommunikationspartner mit den dazu erforderlichen Schlüsseln versorgt werden. Schlüsselinstallation und -speicherung: Im Zuge der Schlüsselinstallation ist die authentische Herkunft sowie die Integrität der Schlüsseldaten zu überprüfen. Generell sollten Schlüssel nie in klarer Form, sondern grundsätzlich verschlüsselt im System gespeichert werden. Auf jeden Fall muss sichergestellt werden, dass bei der Installation des Verschlüsselungsverfahrens voreingestellte Schlüssel geändert werden.
- Schlüsselarchivierung: Für Archivierungszwecke sollte das kryptographische Schlüsselmaterial auch außerhalb des Kryptomoduls in überschlüsselter Form speicherbar und gegebenenfalls wieder einlesbar sein.
- Zugriffs- und Vertreterregelung: Zugriffs- und Vertretungsrechte sollten geregelt sein. Entsprechende Mechanismen müssen vom Schlüsselmanagement und von den einzusetzenden Kryptomodulen und -geräten unterstützt werden (z. B. Schlüsselhinterlegung für den Fall, dass ein Mitarbeiter das Unternehmen verlässt oder wegen Krankheit längere Zeit ausfällt).
- Schlüsselwechsel: Im Kryptokonzept muss basierend auf der Sicherheitsrichtlinie festgelegt werden, wann und wie oft Schlüssel gewechselt werden müssen.
- Schlüsselvernichtung: Nicht mehr benötigte Schlüssel (z. B. Schlüssel, deren Gültigkeitsdauer abgelaufen sind) sind auf sichere Art zu löschen bzw. zu vernichten (z. B. durch mehrfaches Löschen/Überschreiben und/oder mechanische Zerstörung des Datenträgers).

OPS.1.2.3.M14 Datenträgerverwaltung [IT-Betrieb, Leiter Organisation] (CIA)

Bei höherem Schutzbedarf sollte eine Datenträgerverwaltung eingerichtet werden, um den Zugriff auf Datenträger im erforderlichen Umfang und in angemessener Zeit gewährleisten zu können. Dies erfordert eine geregelte Verwaltung der Datenträger, die eine einheitliche Kennzeichnung sowie eine Führung von Bestandsverzeichnissen erforderlich macht. Weiterhin ist im Rahmen der Datenträgerverwaltung die sachgerechte Behandlung und Aufbewahrung der Datenträger, deren ordnungsgemäßer Einsatz und Transport und schließlich auch noch die Löschung bzw. Vernichtung der Datenträger zu gewährleisten. Bei analogen Datenträgern haben die meisten Institutionen eine eingespielte und erprobte Verfahrensweise für deren Verwaltungen, nämlich die klassische Aktenführung. Daher werden in dieser Maßnahme die digitalen Datenträger in den Vordergrund gestellt, die einzelnen Empfehlungen gelten aber sinngemäß für alle Arten von Datenträgern.

Bestandsverzeichnisse ermöglichen einen schnellen und zielgerichteten Zugriff auf Datenträger. Bestandsverzeichnisse geben beispielsweise Auskunft über Aufbewahrungsort, Aufbewahrungsdauer, berechtigte Empfänger.

Die äußerliche Kennzeichnung von Datenträgern ermöglicht deren schnelle Identifizierung. Die Kennzeichnung sollte jedoch für Unbefugte keine Rückschlüsse auf den Inhalt erlauben (z. B. die Kennzeichnung eines Magnetbandes mit dem Stichwort "Telefongebühren"), um einen Missbrauch zu erschweren. Eine festgelegte Struktur von Kennzeichnungsmerkmalen (z. B. Datum, Ablagestruktur, lfd. Nummer) erleichtert die Zuordnung in Bestandsverzeichnissen.

Für eine sachgerechte Behandlung von Datenträgern sind die Herstellerangaben, die üblicherweise auf der Verpackung zu finden sind, heranzuziehen. Hinsichtlich der Aufbewahrung von Datenträgern sind einerseits Maßnahmen zur Lagerung (magnetfeld-/staubgeschützt, klimagerecht) und andererseits Maßnahmen zur Verhinderung des unbefugten Zugriffs (geeignete Behältnisse, Schränke, Räume) zu treffen.

Der Versand oder Transport von Datenträgern muss in der Weise erfolgen, dass eine Beschädigung der Datenträger möglichst ausgeschlossen werden kann (z. B. Magnetbandversandtasche, luftgepolsterte Umschläge). Die Verpackung des Datenträgers ist an seiner Schutzbedürftigkeit auszurichten (z. B. mittels verschließbaren Transportbehältnissen). Versand- oder Transportarten (z. B. Kuriertransport) müssen ebenso festgelegt werden wie das Nachweisverfahren über den Versand (z. B. Begleitzettel, Versandscheine) und den Eingang beim Empfänger (z. B. Empfangsbestätigung). Der Datenträger darf über die zu versendenden Daten hinaus, keine "Restdaten" enthalten. Dies kann durch physikalisches Löschen erreicht werden. Stehen hierzu keine Werkzeuge zur Verfügung, so sollte der Datenträger zumindest formatiert werden. Dabei sollte sichergestellt werden, dass mit dem zugrunde liegenden Betriebssystem eine Umkehr des Befehls nicht möglich ist.

Weiterhin ist zu beachten, dass vor Abgabe wichtiger Datenträger eine Sicherungskopie erstellt wird. .

Für die interne Weitergabe von Datenträger können Regelungen getroffen werden wie Quittungsverfahren, Abhol-/Mitnahmeberechtigungen sowie das Führen von Bestandsverzeichnissen über den Verbleib der Datenträger.

Für den Fall, dass **von Dritten erhaltene Datenträger** eingesetzt werden, sind Regelungen über deren Behandlung vor dem Einsatz zu treffen. Werden zum Beispiel digitale Daten übermittelt, sollte generell ein Computer-Viren-Check des Datenträgers bzw. der Datensätze erfolgen. Dies gilt entsprechend auch vor dem erstmaligen Einsatz neuer digitaler Datenträger. Es ist empfehlenswert, nicht nur beim Empfang, sondern auch vor dem Versenden von digitalen Datenträgern diese auf Computer-Viren zu überprüfen.

Eine geregelte Vorgehensweise für die Löschung oder Vernichtung von Datenträgern verhindert den Missbrauch der gespeicherten Daten. Vor der Wiederverwendung von Datenträgern müssen die gespeicherten Daten vollständig gelöscht werden (siehe hierzu OPS.1.18 Löschen und Vernichten von Daten).

OPS.1.2.3.M15 Sichere Versandart und Verpackung [Benutzer, Poststelle] (C)

Für Informationen mit erhöhtem Schutzbedarf sollte geprüft werden, wie diese bei einem Datenträgeraustausch angemessen geschützt werden können. Hierfür muss eine dem Schutzbedarf angemessene Versandart und Verpackung durch den Versender ausgewählt werden. Eine Versandart für hochschutzbedürftige Informationen ist beispielsweise der Einsatz vertrauenswürdiger Kuriere. Grundsätzlich sollten die Daten verschlüsselt werden.

Neben den in OPS.1.2.3.M14 Datenträgerverwaltung dargestellten Umsetzungshinweisen sollte die Versandverpackung von Datenträgern so sein, dass Manipulationen an den Datenträgern durch Veränderungen an der Verpackung erkennbar sind.

Mögliche Maßnahmen sind die Verwendung von

- Umschlägen mit Siegel,
- verplombten Behältnissen,
- Umschlägen, die mit Klebefilm überklebt und anschließend mit nicht-wasserlöslicher Tinte mehrmals unregelmäßig überzeichnet werden,
- Sicherheitsetiketten, mit denen die Briefhüllen versiegelt werden.

Für den Geheimschutzbereich gibt es spezielle, hierfür eignungsgeprüfte Sicherheitsbriefhüllen, Siegelbänder und Sicherheitsetiketten.

Falls digitale Datenträger über einen Schreibschutz verfügen (z. B. Schieber bei Disketten, Schreibring bei Bändern), so sollte dieser genutzt werden. Je nach Schutzbedarf der auf den Datenträgern gespeicherten Daten sollte geprüft werden, welche der folgenden Sicherheitsmechanismen zweckmäßig sind:

- Die Dateien sollten möglichst schreibgeschützt auf den Datenträgern gespeichert werden. Hierfür kann beispielsweise der in vielen Office-Programmen vorhandene Zugriffsschutz genutzt werden (siehe auch APP.5.2 Office-Anwendungen).
- Sollen Manipulationen an den Informationen auf dem Datenträger selbst erkannt werden können, sind Verschlüsselungs- oder Checksummen-Verfahren einzusetzen (siehe OPS.1.2.3.M13 Verschlüsselung und digitale Signaturen).
- Um unbefugtes Auslesen zu verhindern, sollte der komplette Datenträger oder die einzelnen Dateien verschlüsselt werden.

OPS.1.2.3.M16 Sichere Aufbewahrung der Datenträger vor und nach Versand [Benutzer, Poststelle] (CIA)

Vor dem Versand eines Datenträgers ist zu gewährleisten, dass für den Zeitraum zwischen dem Speichern der Daten auf dem Datenträger und dem Transport ein ausreichender Zugriffsschutz besteht. Beschriebene Datenträger sollten so aufbewahrt werden, dass nur berechtigte Benutzer darauf zugreifen können, egal ob es sich um analoge oder digitale Datenträger handelt. Sind die zu übermittelnden Daten vertraulich, so müssen die Datenträger, auf denen sie sich befinden, bis zum Transport in entsprechenden Behältnissen (Schrank, Tresor) verschlossen aufbewahrt werden. Die für den Transport oder für die Zustellung Verantwortlichen (z. B. Poststelle) sind auf sachgerechte und sichere Aufbewahrung und Handhabung der Datenträger hinzuweisen.

OPS.1.2.3.M17 Verifizieren von Datenträgern vor Versand [Benutzer] (CI)

Vor dem Versenden eines Datenträgers ist dieser darauf zu überprüfen, ob die gewünschten Informationen - und auch nur diese - vom Datenträger rekonstruierbar sind. Dies ist sowohl bei Schriftstücken als auch bei elektronischen Datenträgern zu kontrollieren. Auch Briefe und andere analoge Datenträger sollten vor dem Versand noch einmal daraufhin gesichtet werden, ob sie einerseits vollständig sind und andererseits keine zusätzlichen Informationen enthalten, die nicht weitergegeben werden sollen. Dies ist vor allem wichtig, wenn aus Vertraulichkeitsgründen Teile von Vorgängen, wie beispielsweise Namensnennungen, nicht an Dritte übermittelt werden dürfen. Hierfür können diese Teilinformationen z. B. durch Schwärzen unkenntlich gemacht werden. Da geschwärzte Informationen aber häufig ohne größeren Aufwand wieder lesbar gemacht werden können, ist es allerdings besser, diese für die Weitergabe aus den Vorgängen ganz zu entfernen, z. B. indem sie vor dem Ausdrucken in einer Kopie der Ausgangsdatei gelöscht werden. Je nach Schutzbedarf der Informationen gibt es hierfür verschiedene Methoden:

- Dokumente sollten möglichst so strukturiert sein, dass nicht-öffentliche Inhalte einfach abgetrennt werden können, z. B. indem diese nur in einem Anhang erscheinen. Der Anhang sollte dann auch elektronisch in einer eigenen Datei vorliegen, die als vertraulich klassifiziert ist.
- Falls die Dokumente bereits in einer Form vorliegen, die keine saubere Trennung nach Vertraulichkeit zulassen, müssen schutzbedürftige Inhalte vor einer Weitergabe entfernt werden. Ein Grundproblem dabei ist es, alle sensiblen Informationen zu identifizieren und sorgfältig zu entfernen. Da bereits dies in der Praxis häufig nicht funktioniert, sollte möglichst darauf verzichtet werden, solche Dokumente "entschärft" weiterzugeben. Wenn dies trotzdem erforderlich ist, müssen alle kritischen Informationen entfernt und die Sicherheitsstufen der betroffenen Dokumente neu festgelegt werden. In jedem Fall muss vor der Herausgabe der Dokumente ein erneuter Freigabeprozess durchlaufen werden.

- Bei Papierdokumenten werden sensible Informationen häufig nur geschwärzt. Dies ist in folgenden Schritten durchzuführen:
  - Zunächst sind auf einer Papierfassung alle kritischen Informationen sorgfältig und in ausreichender Größe zu schwärzen.
  - Anschließend werden diese geschwärzten Dokumente kopiert.
  - Danach wird überprüft, ob die geschwärzten Passagen auf der Kopie tatsächlich nicht mehr lesbar sind.
  - Wenn dies sichergestellt ist und die Freigabe erteilt wurde, kann die Kopie weitergegeben werden. Das geschwärzte Original darf keinesfalls herausgegeben werden, da geschwärzte Passagen auf dem Original häufig leicht wieder lesbar gemacht werden können.
- Um vertrauliche Informationen in elektronischen Dokumenten zu entfernen, müssen die schutzbedürftigen Passagen zunächst durch andere Zeichen ersetzt und danach geschwärzt werden. Hierfür sollten Zeichenketten fester Länge verwendet werden, beispielsweise "XXXXXXXXXX", damit sich die ursprüngliche Bedeutung auch nicht mehr erraten lässt. Vor der Weitergabe sollte die Dateien daraufhin überprüft werden, ob sie Restinformationen enthalten, z. B. frühere Überarbeitungsstände (siehe auch OPS.1.2.3.M9 Beseitigung von Restinformationen in Dateien vor Weitergabe [Benutzer]).

Elektronische Datenträger sind vor der weiteren Verwendung physikalisch zu löschen, wenn vorher andere Daten darauf gespeichert waren (siehe OPS.1.2.3.M8 Physikalisches Löschen der Datenträger vor und nach Verwendung).

Die korrekte Übertragung kann bei elektronischen Datenträgern überprüft werden, indem ein Programm eingesetzt wird, das die ursprüngliche mit der übertragenen Datei zeichenweise vergleicht.

Vor dem Versand sollten alle Dateinamen auf den Datenträgern aufgelistet werden, um anhand der Namen zu überprüfen, dass nur die für den Empfänger bestimmten Dateien auf diesen Datenträgern enthalten sind.

OPS.1.2.3.M18 Sicherungskopie der übermittelten Daten [Benutzer] (A)

Sind die zu übertragenden Daten nur zum Zweck der Datenübertragung erstellt bzw. zusammengestellt worden und nicht auf einem weiteren Medium gespeichert, sollte eine Sicherungskopie dieser Daten vorgehalten werden. Bei Verlust oder Beschädigung der Daten auf dem Transportweg kann der Versand mit geringfügigem Aufwand erneut erfolgen.

3 Weiterführende Informationen

3.1 Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Informations- und Datenträgeraustausch" finden sich unter anderem in folgenden Veröffentlichungen:

[27002] ISO/IEC 27002:2013

Information technology - Security techniques - Code of practice for information security controls, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/SC 27, Oktober 2013

[27010] ISO/IEC 27010:2015

Information technology - Security techniques - Information security management for inter-sector and inter-organizational communications, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/SC 27, November 2015

[ACSVI] Merkblatt: Behandlung vertraulicher Informationen

Traffic Light Protocol (TLP), Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 3.1, Oktober 2014, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/merkblatt_behandlung_vertraulicher_informationen.html, zuletzt abgerufen am 05.10.2018

Umsetzungshinweise zum Baustein OPS.1.2.4 Telearbeit

1 Beschreibung

1.1 Einleitung

Unter Telearbeit wird jede auf die Informations- und Kommunikationstechnik gestützte Tätigkeit verstanden, die ausschließlich oder zeitweise außerhalb der Geschäftsräume und Gebäude des Arbeitgebers verrichtet wird.

Es gibt verschiedene Formen der Telearbeit: Sie kann beispielsweise als heimbasierte Telearbeit in der Wohnung des Mitarbeiters oder auch als mobile Telearbeit von unterwegs erbracht werden. Es ist ebenfalls möglich, dass die Mitarbeiter im Rahmen der On-Site-Telearbeit bei Kunden oder Lieferanten eingesetzt werden und dort mit der Ausstattung des eigenen Arbeitgebers arbeiten. Eine weitere Möglichkeit ist die Telearbeit in sogenannten Telecentern oder auch Satelliten- oder Nachbarschaftsbüros.

Bei der heimbasierten Telearbeit wird zwischen der ausschließlich zu Hause erbrachten Arbeit und der alternierenden Telearbeit unterschieden. Bei der alternierenden Telearbeit arbeiten die Arbeitnehmer wechselweise an ihrem Arbeitsplatz beim Arbeitgeber und am häuslichen Arbeitsplatz.

1.2 Lebenszyklus

Planung und Konzeption

Es sollte ein Konzept für Telearbeit erstellt werden, in dem die Sicherheitsziele, der Schutzbedarf der bei der Telearbeit zu bearbeitenden Informationen sowie die Risiken und Sicherheitsmaßnahmen aufgezeigt werden (siehe OPS.1.2.4.M6 Erstellung eines Sicherheitskonzeptes für Telearbeit).

Sichere Telearbeit setzt organisatorische Regelungen und personelle Maßnahmen voraus. Besonders zu beachten sind die speziellen Verpflichtungen der Telearbeiter und deren Einweisung in die Nutzungsregelungen der Kommunikation. Sie sind unter anderem in OPS.1.2.4.M1 Regelungen für Telearbeit und OPS.1.2.4.M5 Sensibilisierung und Schulung der Telearbeiter beschrieben.

Umsetzung

Nachdem die organisatorischen und planerischen Vorarbeiten durchgeführt wurden, können die Telearbeitsrechner und andere IT-Systeme installiert werden. Dabei sind folgende Maßnahmen zu beachten:

- Sicherheit des Telearbeitsrechners: Der Telearbeitsrechner muss so gestaltet sein, dass im unsicheren Einsatzumfeld eine sichere Nutzung möglich ist. Insbesondere sollten nur autorisierte Personen den Telearbeitsrechner offline und online benutzen (siehe OPS.1.2.4.M2 *Sicherheitstechnische Anforderungen an den Telearbeitsrechner*).
- Sichere Kommunikation zwischen Telearbeitsrechner und Institution: Da die Kommunikation über öffentliche Netze erfolgt, sind besondere Sicherheitsanforderungen für die Kommunikation zwischen Telearbeitsrechner und Institution zu erfüllen (siehe OPS.1.2.4.M3 *Sicherheitstechnische Anforderungen an die Kommunikationsverbindung*).

Betrieb

Die Benutzer haben einen wesentlichen Einfluss auf die Sicherheit bei der Telearbeit. Die Telearbeiter müssen daher zur Einhaltung der Sicherheitsvorgaben und für die Nutzung der IT-Systeme geschult werden (siehe *OPS.1.2.4.M5 Sensibilisierung und Schulung der Telearbeiter*).

Notfallvorsorge

Alle relevanten Daten, die im Rahmen der Telearbeit erstellt oder verändert wurden, müssen gesichert werden (siehe OPS.1.2.4.M4 *Datensicherung bei der Telearbeit*).

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Telearbeit" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

OPS.1.2.4.M1 Regelungen für Telearbeit [Personalabteilung, Vorgesetzte]

Institutionen müssen Regelungen für die Telearbeit festlegen. Dabei sind verschiedene arbeitsrechtliche und arbeitsschutzrechtliche Rahmenbedingungen zu beachten. Strittige Punkte sollten entweder durch Betriebsvereinbarungen oder durch zusätzlich zum Arbeitsvertrag getroffene individuelle Vereinbarungen zwischen Telearbeiter und Arbeitgeber geklärt werden. In diesen Vereinbarungen sollten beispielsweise folgende Punkte geregelt werden:

- Freiwilligkeit der Teilnahme an der Telearbeit
- Mehrarbeit und Zuschläge
- Aufwendungen für Fahrten zwischen Betrieb / Kunden und häuslicher Wohnung
- Aufwendungen zum Beispiel für Strom, Heizung und Miete
- Haftung (bei Diebstahl oder Beschädigung der IT, aber auch bei Arbeitsunfall oder Berufskrankheit)
- Beendigung der Telearbeit

Die für die Telearbeit im Umgang mit Informationen und der Informations- und Kommunikationstechnik notwendigerweise umzusetzenden Sicherheitsmaßnahmen sollten zusätzlich in einer Sicherheitsrichtlinie zur Telearbeit dokumentiert werden, sofern es sich nicht anbietet, die Inhalte in bereits bestehende Richtlinien der Institution zu integrieren.

Folgende Aspekte sollten beispielsweise in den Regelungen für Telearbeit beachtet werden:

- **Arbeitszeitregelung:** Es sollte geregelt sein, wie die Arbeitszeiten auf Tätigkeiten zwischen der Institution und dem Telearbeitslatz verteilt sind. Auch müssen feste Zeiten festgelegt werden, an denen der Mitarbeiter am Telearbeitsplatz erreichbar ist.

- **Reaktionszeiten:** Es sollte geregelt werden, in welchen Abständen die Telearbeiter aktuelle Informationen abrufen sollen (zum Beispiel wie häufig E-Mails gelesen werden) und in welchem Zeitraum sie darauf zu reagieren haben.
- **Umgang mit vertraulichen Informationen:** Bei der Telearbeit werden vertrauliche Informationen sowohl analog, also zum Beispiel auf Papier, als auch digital bearbeitet. Unabhängig davon, in welcher Form Informationen vorliegen, müssen sie vor unbefugtem Zugriff und anderen Sicherheitsrisiken geschützt werden. Daher ist der komplette Lebensweg vertraulicher Informationen angemessen abzusichern.
- **Arbeitsmittel:** Es sollte festgeschrieben werden, welche Arbeitsmittel die Telearbeiter einsetzen dürfen und welche nicht benutzt werden sollten (zum Beispiel nicht freigegebene Software). So kann ein E-Mail-Anschluss zur Verfügung gestellt werden, aber die Nutzung von anderen Internet-Diensten untersagt werden. Weiterhin könnte untersagt werden Datenträgern wie beispielsweise DVDs oder USB-Sticks zu benutzen, sofern der Telearbeitsplatz dies nicht erfordert.
- **Datensicherung:** Die Telearbeiter sind zu verpflichten, regelmäßig lokal gespeicherte Daten zu sichern. Zusätzlich sollte vereinbart werden, dass jeweils eine Generation der Datensicherungen in der Institution hinterlegt wird. Falls die Datensicherung über den Fernzugriff zur Institution bereits ausreichend sichergestellt ist und kein erhöhter Schutzbedarf vorliegt, kann von einer lokalen Datensicherung abgesehen werden.
- **Synchronisation von Datenbeständen:** Datenbestände, die sowohl in der Institution als auch an Telearbeitsplätzen bearbeitet werden, müssen geeignet synchronisiert werden. Das Vorgehen bei der Synchronisation muss genau geplant werden, damit keine Konflikte entstehen und es zu keinem Datenverlust kommt. Die Konflikte treten z. B. auf, wenn zwei Benutzer den gleichen Datensatz in gespiegelten Datenbeständen geändert haben. Es empfiehlt sich, die Datenbestände mithilfe einer geeigneten Software zu synchronisieren.
- **Datenschutz:** Datenschutz: Die Telearbeiter sind darauf zu verpflichten, einschlägige Datenschutzvorschriften einzuhalten.
- **Datenkommunikation:** Es muss festgelegt werden, welche Daten auf welchem Weg übertragen werden beziehungsweise welche Daten nicht oder nur verschlüsselt elektronisch übermittelt werden dürfen. Ebenso ist festzulegen, welche Dokumente zwischen Institution und Telearbeitsplatz transportiert werden können und wie diese dabei zu schützen sind.
- **Transport von Dokumenten und Datenträgern:** Die Art und Absicherung des Transports von Dokumenten und Datenträgern, zwischen dem Telearbeitsplatz und der Institution, ist zu regeln. Vertrauliche Daten auf digitalen Datenträgern sollten immer nur verschlüsselt transportiert werden.
- **Meldeweg:** Die Telearbeiter sind zu verpflichten, sicherheitsrelevante Vorkommnisse unverzüglich an eine im Vorfeld zu bestimmende Stelle in der Institution zu melden. Dafür ist es notwendig, die Telearbeiter entsprechend den geltenden Richtlinien einzuweisen. Hierfür eignet sich zum Beispiel die Richtlinie zum Incident Management.
- **Zutrittsrecht Telearbeitsplatz:** Es sollte ein Zutrittsrecht zum Telearbeitsplatz, gegebenenfalls nach vorheriger Anmeldung, vereinbart werden. Wichtig ist das in erster Linie, damit im Vertretungsfall Akten und Daten für den stellvertretenden Mitarbeiter verfügbar sind.
- **Vertretungsregelung:** Für jeden Telearbeiter sollte ein Vertreter bestimmt werden, der über die laufenden Aktivitäten informiert sein muss, damit er auch kurzfristig die Vertretung übernehmen kann. Dazu müssen die Arbeitsergebnisse durch die Telearbeiter immer sorgfältig dokumentiert werden. Eventuell sind sporadische oder regelmäßige Treffen zwischen dem Telearbeiter und seinem Vertreter sinnvoll. Ergänzend muss geregelt werden, wie der Vertreter im unerwarteten Vertretungsfall auf die Daten, auf den Telearbeitsrechner oder am Telearbeitsplatz vorhandene Unterlagen zugreifen kann. Dieser Vertretungsfall sollte probeweise durchgespielt und der Test anschließend vom Telearbeiter und seiner Vertretung ausgewertet werden. Dadurch ist es möglich, den Vertretungsprozess stetig zu optimieren.

Die Regelungen für die Telearbeit sind jedem Telearbeiter auszuhändigen. Entsprechende Merkblätter sind regelmäßig zu aktualisieren.

OPS.1.2.4.M2 Sicherheitstechnische Anforderungen an den Telearbeitsrechner [IT-Betrieb, Leiter IT]

Die sicherheitstechnischen Anforderungen an die Telearbeitsrechner richten sich nach dem Schutzbedarf der zu bearbeitenden Daten am Telearbeitsplatz und der Daten, auf die die Telearbeiter über den Kommunikationsrechner der Institution zugreifen können. Je höher der Schutzbedarf, desto mehr Maßnahmen müssen ergriffen werden, um diesen Schutz zu gewährleisten.

Allgemeine Sicherheitsziele für Telearbeitsrechner sind:

- Telearbeitsrechner dürfen nur von autorisierten Personen benutzt werden. Damit wird sichergestellt, dass nur autorisierte Personen auf Daten und Programme zugreifen können, die auf einem Telearbeitsrechner gespeichert sind. Gleiches gilt für Informationen und Daten, die über den Telearbeitsrechner erreichbar wären (zum Beispiel mittels VPN). Autorisierte Personen sind der Administrator des Telearbeitsrechners und der Telearbeiter nebst seinem Stellvertreter.
- Telearbeitsrechner dürfen nur für autorisierte Zwecke benutzt werden. Beispielsweise sollte der Benutzer keine ungenehmigten Programme installieren dürfen. Dadurch wird Schäden durch Fehlbedienung und Missbrauch vorgebeugt.
- Schäden aufgrund eines Diebstahls oder Defektes eines Telearbeitsrechners müssen tolerabel sein. Telearbeitsrechner werden üblicherweise in einer wenig gesicherten Umgebung eingesetzt, sodass ein Diebstahl oder Defekt wahrscheinlicher ist als in der geschützten Betriebsumgebung einer Institution. Darunter kann nicht nur die Verfügbarkeit, sondern auch die Vertraulichkeit der gespeicherten Daten leiden. Um die Schäden bei Diebstählen gering zu halten, sollten die Daten zum Beispiel nur verschlüsselt gespeichert werden. Um Schäden durch Defekte zu begrenzen, eignen sich zum Beispiel regelmäßig durchgeführte Datensicherungen.
- Telearbeiter sollten wenigstens offensichtliche versuchte oder erfolgte Manipulationen am Telearbeitsrechner erkennen können. Damit wird sichergestellt, dass der Telearbeitsrechner in einem integren Zustand verbleibt, auch wenn Manipulationsversuche nicht ausgeschlossen sind.

Aus dem Schutzbedarf der zu bearbeitenden Daten am Telearbeitsplatz leiten sich die Sicherheitsziele und damit die sicherheitstechnischen Anforderungen an die Telearbeitsrechner ab. Es ist zu dokumentieren, welche der nachfolgend beschriebenen sicherheitsrelevanten Funktionalitäten ein Telearbeitsrechner aufweisen muss und wie diese umgesetzt werden.

Für einen Telearbeitsrechner sind folgende Funktionalitäten sinnvoll:

- Der Telearbeitsrechner muss über einen I**dentifizierungs- und Authentisierungsmechanismus** verfügen. Insbesondere sind dabei folgende Punkte sicherzustellen:
    - Sicherheitskritische Parameter, wie Passwörter oder Benutzer-Kennung müssen sicher verwaltet werden. Passwörter dürfen nie unverschlüsselt auf dem Telearbeitsrechner gespeichert werden.
    - Das Zugangsverfahren muss definiert auf Fehleingaben reagieren. Erfolgt zum Beispiel dreimal hintereinander eine fehlerhafte Authentisierung, ist der Zugang zum Telearbeitsrechner zu sperren oder es sind die zeitlichen Abstände sukzessiv zu vergrößern, nach denen ein weiterer Zugangsversuch erlaubt wird.
    - Es muss möglich sein, Minimalvorgaben für die sicherheitskritischen Parameter vorzugeben.
    - Nach zeitweiser Inaktivität der Tastatur oder Maus, muss automatisch eine Bildschirmsperre aktiviert werden, die erst nach erneuter Identifikation und Authentisierung deaktiviert wird.
- Der Telearbeitsrechner muss über eine **Zugriffskontrolle** verfügen. Insbesondere sind folgende Anforderungen umzusetzen:
    - Der Telearbeitsrechner muss verschiedene Benutzer unterscheiden können. Es muss möglich sein, mindestens zwei getrennte Rollen auf dem Telearbeitsrechner einzurichten, nämlich Administrator und Telearbeiter.
    - Mittels einer differenzierten Rechtestruktur (zum Beispiel lesen, schreiben, ausführen) muss der Zugriff auf Dateien und Programme regelbar sein. Bei mobilen Endgeräten ist eine differenzierte Rechtestruktur nicht immer möglich. Gerade Smartphones und Tablets verfügen häufig über keine derartige Differenzierung. Es sollte daher geprüft werden, ob sich die Geräte für den vorliegenden Schutzbedarf eignen.
- Telearbeitsrechner sollten über eine **Protokollierung** verfügen. Es ist sinnvoll, folgende Anforderungen umzusetzen:
    - Der Mindestumfang, den der Telearbeitsrechner protokollieren soll, sollte parametrisierbar sein. Beispielsweise sollten folgende Aktionen inklusive der aufgetretenen Fehlerfälle protokollierbar sein:
        - bei Authentisierung: zum Beispiel Benutzer-Kennung, Datum und Uhrzeit, Ergebnis des Anmeldeversuchs bei der Zugriffskontrolle, Art des Zugriffs, was wurde wie geändert, gelesen, geschrieben
        - Durchführung von Administrator-Tätigkeiten,
        - Auftreten von funktionalen Fehlern.
    - für Unberechtigte darf keine Möglichkeit bestehen, die Protokollierung zu deaktivieren. Die Protokolle selbst dürfen für Unberechtigte weder lesbar noch modifizierbar sein.
    - Die Protokollierung muss übersichtlich, vollständig und korrekt sein.
- Soll der Telearbeitsrechner über eine **Protokollauswertung** verfügen, können folgende Anforderungen sinnvoll sein:
    - Eine Auswertefunktion muss nach den bei der Protokollierung geforderten Datenarten unterscheiden können (zum Beispiel Filtern aller unberechtigten Zugriffe auf alle Ressourcen in einem vorgegebenen Zeitraum).
    - Die Auswertefunktion muss auswertbare (lesbare) Berichte erzeugen, sodass keine sicherheitskritischen Aktivitäten übersehen werden.
- Telearbeitsrechner sollten über Funktionen zur **Datensicherung** verfügen. Diese sollten unter anderem folgende Anforderungen erfüllen:
    - Die Datensicherung für die Telearbeit sollte den Rahmenbedingungen zur Datensicherung der Institution entsprechen und diese einhalten
    - Das Datensicherungsprogramm muss benutzerfreundlich und schnell arbeiten. Es sollte automatisierbar sein.
    - Es muss konfigurierbar sein, welche Daten wann gesichert werden.
    - Es muss eine Option existieren, um beliebige Datensicherungen wieder einzuspielen.
    - Die Funktion muss ermöglichen, mehrere Generationen zu sichern.
    - Datensicherungen von Zwischenergebnissen aus der laufenden Anwendung sollen möglich sein.
- Telearbeitsrechner sollten über eine **Verschlüsselungskomponente** verfügen. Hierfür ist zunächst zu überlegen, welche Funktionalität benötigt wird:
    - die Verschlüsselung ausgewählter Daten (offline) oder
    - automatisch der gesamten Festplatte (online).

  Grundsätzlich sollte die automatische Verschlüsselung aller Datenträger vorgezogen werden, da dies benutzerfreundlicher und effizienter ist. Das setzt voraus, dass ein geeignetes Verschlüsselungsprodukt eingesetzt wird und dass ein Datenverlust bei Fehlfunktion (Stromausfall, Abbruch

Aus den obigen Funktionalitäten sind diejenigen auszuwählen, die aufgrund der Sicherheitsanforderungen an die Telearbeitsrechner benötigt werden und entsprechend dem Schutzbedarf möglich sind. Anhand dieser Funktionalitäten muss dann ein geeignetes Betriebssystem als Plattform ausgewählt werden. Wenn dieses nicht alle benötigten Funktionalitäten unterstützt, müssen dazu Zusatzprodukte eingesetzt werden. Dabei sollten möglichst alle Telearbeitsrechner einer Institution gleich ausgestattet sein, um die Betreuung und Wartung zu erleichtern und gleichartige Systeme als Client-Gruppen zusammenführen zu können. Das Gesamtsystem ist durch die Administratoren so zu konfigurieren, dass maximale Sicherheit erreicht werden kann.

Weitere Anforderungen zu den einzelnen Client-Systemen werden in der Bausteinschicht SYS.2 *Desktop-Systeme* aufgeführt. Diese sollten entsprechend der eingesetzten Client-Lösung für den Telearbeitsrechner umgesetzt werden.

OPS.1.2.4.M3 Sicherheitstechnische Anforderungen an die Kommunikationsverbindung [IT-Betrieb, Leiter IT, Telearbeiter]

Erfolgt im Rahmen der Telearbeit eine Datenübertragung zwischen einem Telearbeitsrechner und einem Rechner der Institution, werden dabei dienstliche Informationen üblicherweise über öffentliche Kommunikationsnetze übertragen. Da weder die Institution noch die Telearbeiter Einfluss darauf haben, ob die Vertraulichkeit, Integrität und Verfügbarkeit in einem öffentlichen Kommunikationsnetz gewahrt werden, sind zusätzliche Sicherheitsmaßnahmen erforderlich.

Generell muss die Datenübertragung zwischen Telearbeitsrechner und Institution folgende Sicherheitsanforderungen erfüllen:

- **Sicherstellung der Vertraulichkeit der übertragenen Daten:** Durch eine ausreichend sichere Verschlüsselung muss erreicht werden, dass auch wenn Angreifer die Kommunikation zwischen Telearbeitsrechner und dem Rechner der Institution abhören, keine Rückschlüsse auf die Inhalte der Daten möglich sind. Zur Sicherstellung der Vertraulichkeit der übertragenen Daten gehört neben einem geeigneten Verschlüsselungsverfahren auch ein angepasstes Schlüsselmanagement mit periodischem Schlüsselwechsel.
- **Sicherstellung der Integrität der übertragenen Daten:** Die eingesetzten Übertragungsprotokolle müssen eine zufällige Veränderung übertragener Daten erkennen und beheben. Um absichtliche Manipulationen während der Datenübertragung detektieren zu können, sollten die Daten signiert und/oder verschlüsselt werden.
- **Sicherstellung der Verfügbarkeit der Datenübertragung:** Falls zeitliche Verzögerungen bei der Telearbeit nur schwer zu tolerieren sind, sollte ein redundant ausgelegtes öffentliches Kommunikationsnetz als Übertragungsweg ausgewählt werden, sodass ein Ausfall einzelner Verbindungsstrecken nicht den Totalausfall der Kommunikation bedeutet. Auf eine redundante Netzanbindung an den Telearbeitsrechner und die Schnittstelle der Institution kann gegebenenfalls verzichtet werden.
- **Sicherstellung der Authentizität der Daten:** Wenn Daten zwischen Telearbeitsrechner und Institution übertragen werden, muss sichergestellt sein, dass die Kommunikation zwischen den richtigen Teilnehmern stattfindet. Das bedeutet sicher zu stellen, dass Daten mit Absender Telearbeitsrechner auch tatsächlich von dort stammen. Ebenso muss der Ursprung von Institutionsdaten zweifelsfrei auf die Institution zurückgeführt werden können.
- **Sicherstellung der Nachvollziehbarkeit der Datenübertragung:** Um eine Kommunikation nachvollziehbar zu machen, können Protokollierungsfunktionen eingesetzt werden.
- **Sicherstellung des Datenempfangs:** Ist es für die Telearbeit wichtig, dass Daten korrekt empfangen wurden, können Quittungsmechanismen eingesetzt werden, aus denen hervorgeht, ob der Empfänger die Daten korrekt empfangen hat.

OPS.1.2.4.M4 Datensicherung bei der Telearbeit [IT-Betrieb, Telearbeiter]

Bei der Telearbeit können Daten auf verschiedenen IT-Systemen und an verschiedenen Orten verarbeitet werden. Beispielsweise kann die Verarbeitung auf Servern und Clients in der Institution, aber auch auf Clients am Telearbeitsplatz stattfinden. Um die Verfügbarkeit der Daten sicherzustellen, müssen diese regelmäßig gesichert werden.

Eine Datensicherung aller relevanten Daten am Telearbeitsplatz muss generell erfolgen und den allgemeinen Regeln zur Datensicherung der Institution entsprechen. Das Datensicherungskonzept der Institution muss auch die Telearbeitsplätze miteinbeziehen. Generell bieten sich folgende Verfahren zur Datensicherung am Telearbeitsplatz an:

- Datensicherung auf externen DatenträgernHierfür müssen die Telearbeitsplätze über die notwendige technische Ausstattung verfügen. Dazu gehören neben den erforderlichen externen Datenträgern die notwendige Hard- und Software des Rechners. Außerdem müssen die Telearbeiter geschult sein, um die Datensicherungen selbstständig anfertigen zu können.
- Datensicherung über NetzDie Sicherung der lokalen Daten kann auch über die Anbindung an das Netz der Institution erfolgen. Vorteilhaft ist hierbei, dass zum einen die Datensicherung nicht von den Telearbeitern selbstständig durchgeführt werden muss und zum anderen die Telearbeiter auch keine Datenträger verwalten müssen. Entscheidend bei der Datensicherung über eine Netzverbindung ist, dass deren Übertragungskapazität für das Volumen der zu sichernden Daten ausreichend ist. Je nach Datensicherungsprogramm besteht die Möglichkeit, nur die Änderungen des Datenbestands seit der letzten Datensicherung zu übertragen (inkrementelle Datensicherung). In vielen Fällen kann hierdurch das zu transportierende Datenvolumen stark reduziert werden. Eine wichtige Anforderung an das Backup-Programm ist, dass unerwartete Verbindungsabbrüche erkannt und ordnungsgemäß behandelt werden.

Bei beiden Verfahren zur Datensicherung ist es wünschenswert, das Volumen der zu sichernden Daten zu minimieren. Neben verlustfreien Kompressionsverfahren, die in viele Datensicherungsprogrammen integriert sind, können auch inkrementelle oder differentielle Sicherungsverfahren eingesetzt werden. Hierdurch erhöht sich jedoch unter Umständen der Aufwand für die Wiederherstellung einer Datensicherung.

Die Datensicherung sollte möglichst automatisiert ablaufen, sodass die Telearbeiter nur wenige Aktionen selbst durchführen müssen. Wenn die Mitarbeit der Benutzer erforderlich ist, sollten sie dazu verpflichtet werden, die Datensicherung regelmäßig durchzuführen. Schließlich sollte sporadisch geprüft werden, ob angelegte Datensicherungen wiederhergestellt werden können.

Aufbewahrung der Backup-Datenträger

Falls Datensicherungen am Telearbeitsplatz durchgeführt werden, müssen Backup-Datenträger dort verschlossen aufbewahrt werden. Es ist sicherzustellen, dass nur der Telearbeiter und sein Vertreter darauf zugreifen können.

Jeweils eine Generation der Backup-Datenträger sollte jedoch in der Institution aufbewahrt werden, damit im Katastrophenfall der Vertreter auf die Backup-Datenträger zugreifen kann.

OPS.1.2.4.M5 Sensibilisierung und Schulung der Telearbeiter [Leiter IT, Vorgesetzte]

Anhand eines Merkzettels für Telearbeit müssen die Telearbeiter in die entsprechenden Sicherheitsmaßnahmen der Institution eingewiesen werden. Dabei sind insbesondere folgende Punkte zu berücksichtigen:

- Dienstliche Unterlagen müssen am Telearbeitsplatz sicher aufbewahrt werden, also zum Beispiel in Schränke weggeschlossen werden.
- Fenster und nach außen gehende Türen (Balkone, Terrassen) sind abzuschließen, wenn der Telearbeitsplatz verlassen wird.
- Strukturelle und sicherheitsrelevante Änderungen an der Telearbeitsplatz-IT dürfen nur durch die Administratoren der Institution vorgenommen werden.
- Der Telearbeitsrechner darf nur über den dafür vorgesehenen Anschluss an öffentliche Kommunikationsnetze angebunden sein.
- Beim Datenaustausch mittels Datenträgern zwischen IT-Systemen der Institution und dem Arbeitsplatz-PC am Telearbeitsplatz dürfen nur die von der Institution beschafften Datenträger benutzt werden. Datenträger sollten nur verschlüsselt transportiert werden. Dienstliche und private IT-Systeme oder Datenträger sollten sorgfältig getrennt bleiben.
- Der unbefugte Zugriff auf die IT der Telearbeiter ist durch Zugriffssperren zu verhindern, zum Beispiel Boot- und Bildschirm-Sperren. Passwörter sind generell geheim zu halten.

Darüber hinaus sind die Telearbeiter soweit im Umgang mit den Telearbeitsrechnern zu schulen, dass sie einfache Fehlerkorrekturen (zum Beispiel Druckerpatrone wechseln) vornehmen beziehungsweise einfache Probleme selbstständig beheben können.

Für das geordnete und strukturierte Vorgehen bei sicherheitstechnischen Einweisungen der Telearbeiter sollten auch die Anforderungen des Bausteins ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit* beachtet werden.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Telearbeit".

OPS.1.2.4.M6 Erstellen eines Sicherheitskonzeptes für Telearbeit [Leiter IT, Leiter Organisation, Vorgesetzte]

Es sollte ein Sicherheitskonzept für Telearbeit erstellt werden, in dem die Sicherheitsziele, der Schutzbedarf der bei der Telearbeit zu bearbeitenden Informationen sowie die Risiken und Sicherheitsmaßnahmen aufgezeigt werden.

Bei der Telearbeit werden Informationen meist außerhalb der geschützten Betriebsumgebung verarbeitet. Daher ist im Vorfeld eine Schutzbedarfsfeststellung der betroffenen Informationen, Geschäftsprozesse, Anwendungen, IT-Systeme, Kommunikationsverbindungen und Räume (vor allem der Telearbeitsplätze) bezüglich Vertraulichkeit, Integrität und Verfügbarkeit durchzuführen. Aus dem Schutzbedarf der zu bearbeitenden Daten am Telearbeitsplatz leiten sich die Sicherheitsziele und damit die sicherheitstechnischen Anforderungen an die Telearbeiter, die Telearbeitsrechner und die Telearbeitsplätze ab.

Neben einem Überblick über die Gefährdungslage und den organisatorischen, infrastrukturellen und personellen Sicherheitsmaßnahmen können Maßnahmen aus folgenden Bereichen sinnvoll sein:

- Umgang mit Daten und schützenswerten Betriebsmitteln wie Dokumenten und Speichermedien, insbesondere Regelungen zum Anfertigen von Kopien und zum Löschen beziehungsweise Vernichten von Datenträgern,
- Absicherung der Kommunikation (zum Beispiel durch Verschlüsselung, elektronische Signatur) zwischen Institution und Telearbeitsplatz,
- Authentisierungsmechanismen,
- Regelungen für weitere Netzanbindungen,
- Regelungen für den Datenaustausch,
- Datensicherung.

Zur Ausgestaltung der Telearbeit sind zusätzlich diverse Gesetze und Vorschriften zu beachten (siehe OPS.1.2.4.M1 *Regelungen für Telearbeit*).

Die Anforderungen, Ziele und die zu ergreifenden Maßnahmen zur Sicherheit bei Telearbeit sind zu dokumentieren. Das Sicherheitskonzept zur Telearbeit ist mit dem übergreifenden Sicherheitskonzept der Institution abzustimmen und zu harmonisieren. Außerdem muss es regelmäßig aktualisiert werden und ist an Änderungen in der Institution oder der Technik anzupassen.

Die von den Telearbeitern umzusetzenden Sicherheitsmaßnahmen sind in einer Sicherheitsrichtlinie zur Telearbeit zielgruppengerecht zusammenzufassen.

OPS.1.2.4.M7 Geregelte Nutzung der Kommunikationsmöglichkeiten bei Telearbeit [IT-Betrieb, Telearbeiter]

Für die Telearbeit werden typischerweise verschiedene Kommunikationsmöglichkeiten, wie Telefon-, Fax- und Internet-Anbindung, aber auch Postaustausch sowie Akten- und Datenträgertransport benötigt.

Es muss geregelt werden, auf welche Weise die vorhandenen Kommunikationsmöglichkeiten genutzt werden dürfen. Auch der Postaustausch sowie der Akten- und Datenträger-Transport zwischen Institution und Telearbeitsplatz müssen dabei betrachtet werden. Ebenso sollte die private Benutzung der Kommunikationsmöglichkeiten klar geregelt werden, z. B. des Internetanschlusses. Alle Regelungen sind schriftlich zu fixieren (siehe *OPS.1.2.4*.M1 *Regelungen für Telearbeit*) und den Telearbeitern auszuhändigen.

Zu klären sind dabei zumindest folgende Punkte:

Datenflusskontrolle

Der Austausch von Informationen zwischen dem Telearbeitsplatz und der Institution muss so geregelt sein, dass die Sicherheit der Informationen gewährleistet ist.

- Welche Dienste dürfen zum Informationsaustausch und zur Datenübertragung genutzt werden?
- Welche Informationen dürfen dabei an wen weitergegeben werden?
- Welche Dienste dürfen explizit nicht genutzt werden?
- Welcher Schriftverkehr darf über E-Mail abgewickelt werden? Ist eine Unterschriftenregelung für die Kommunikation vorgesehen?
- Welche Authentisierungsverfahren werden für den Schriftverkehr und für den Datenaustausch genutzt?
- Werden digitale Signaturen eingesetzt?

ZugriffsberechtigungenMuss der Telearbeiter auf die IT der Institution (zum Beispiel auf einen Server) zugreifen können, sollte zuvor festgelegt werden, welche Objekte (zum Beispiel Daten oder IT) er tatsächlich für seine Aufgaben benötigt. Die benötigten Zugangs- und Zugriffsrechte sollten nach den festgelegten Vorgaben der Institution vergeben werden.

Sicherheitsmaßnahmen beim Informationsaustausch Der Informationsaustausch bei der Telearbeit muss angemessen abgesichert werden. Vertrauliche Informationen müssen sicher transportiert werden. Dazu sind mindestens folgende Fragen zu beantworten:

- Für welche Datenträger soll welche Versandart eingesetzt werden (zum Beispiel Kurierdienst)? Welche Art der Transportsicherung ist angemessen (zum Beispiel Umschläge mit Sicherheitsetiketten)?
- Für welche Daten sollen welche Verschlüsselungsverfahren eingesetzt werden? Daten sollten bei der Datenübertragung und auf Datenträgern möglichst immer verschlüsselt werden, damit Transportverluste höchstens deren Verfügbarkeit und nicht deren Vertraulichkeit gefährden.
- Werden von zu übertragenden Daten, die nur zum Zweck der Datenübertragung erstellt beziehungsweise zusammengestellt worden sind, Sicherungskopien vorgehalten?
- Für welche Daten ist eine Löschung nach erfolgreicher Übertragung notwendig? Das kann beispielsweise für personenbezogene Daten gelten.
- Von welchen Daten soll trotz der erfolgreichen Übertragung eine Kopie der Daten auf dem Telearbeitsrechner verbleiben?
- Wird vor Versand und nach Erhalt von Daten ein Malware-Check der Daten durchgeführt?
- Für welche Datenübertragungen sollte eine Protokollierung erfolgen? Falls eine automatische Protokollierung von Datenübertragungen nicht möglich sein sollte, ist festzulegen, ob und in welchem Umfang eine handschriftliche Protokollierung vorzusehen ist.

Internet-Nutzung Es ist zu regeln, ob über den Telearbeitsrechner Internet-Dienste genutzt werden dürfen. Dabei ist auch zu klären, ob eine private Nutzung erlaubt wird. Dabei zu klärende Fragen:

- Wird die Nutzung von Internet-Diensten generell verboten?
- Welche Internet-Dienste dürfen genutzt werden?
- Dürfen Daten aus dem Internet geladen werden? Bei Daten von fremden Servern besteht die Gefahr, dass sie Schadsoftware enthalten.
- Welche Rahmenbedingungen und technischen Sicherheitsmaßnahmen müssen bei der Internet-Nutzung beachtet werden? Welche Sicherheitsmechanismen sollen beispielsweise im Browser aktiviert werden?
- Dürfen sich Telearbeiter am Informationsaustausch über Internet-Plattformen, Newsgruppen, Blogs oder Ähnlichem beteiligen? Ist hierfür ein Pseudonym erforderlich?

OPS.1.2.4.M8 Informationsfluss zwischen Telearbeiter und Institution [Telearbeiter, Vorgesetzte]

Damit Telearbeiter nicht vom betrieblichen Geschehen ausgeschlossen werden, muss ein regelmäßiger Informationsaustausch zwischen den Telearbeitern und den Arbeitskollegen der Institution erfolgen. Hierfür sind sowohl die Vorgesetzten, als auch die Telearbeiter selber verantwortlich. Die jeweiligen Vorgesetzten müssen sicherstellen, dass die Telearbeiter alle notwendigen Informationen für ihre Arbeitsbereiche erhalten. Die Telearbeiter müssen jedoch auch selbstständig nach Informationen und Neuigkeiten fragen. Der regelmäßige Informationsaustausch ist wichtig, damit die Telearbeiter über Planungen und Zielsetzungen in ihrem Arbeitsbereich informiert sind.

Die Telearbeiter sollten an den Umlaufverfahren für Hausmitteilungen, einschlägige Informationen und Zeitschriften beteiligt werden. Dies stellt ein Problem dar, wenn Telearbeiter ausschließlich zu Hause arbeiten. Eine Lösungsmöglichkeit ist, wichtige Schriftstücke einzuscannen, um sie den Telearbeitern per E-Mail zuzustellen. Die Telearbeiter müssen auf jeden Fall zeitnah über geänderte Sicherheitsmaßnahmen und andere sicherheitsrelevante Aspekte unterrichtet werden.

Die Arbeitskollegen in der Institution müssen über die Anwesenheits- und Erreichbarkeitszeiten der Telearbeiter in Kenntnis gesetzt werden. Die entsprechenden E-Mail-Adressen und Telefonnummern sollten allen Kollegen bekannt sein. Außerdem sollte eine Anrufweiterleitung vom Telefonanschluss des Mitarbeiters in der Institution zum Telefon am Telearbeitsplatz eingerichtet werden.

Folgende Punkte müssen darüber hinaus bei der Telearbeit geklärt werden:

- Wer ist Ansprechpartner bei technischen und/oder organisatorischen Problemen bei der Telearbeit?
- Wem müssen Sicherheitsvorkommnisse mitgeteilt werden?
- Wie erfolgt die Aufgabenzuteilung?
- Wie erfolgt die Übergabe der Arbeitsergebnisse?

Treten technisch-organisatorische Probleme auf, müssen diese vom Telearbeiter unverzüglich der Institution gemeldet werden.

OPS.1.2.4.M9 Betreuungs- und Wartungskonzept für Telearbeitsplätze [IT-Betrieb, Leiter IT, Telearbeiter]

Für Telearbeitsplätze sollte ein spezielles Betreuungs- und Wartungskonzept erstellt werden, das folgende Punkte vorsieht:

- **Benennen von Ansprechpartnern für den Benutzerservice:** An diese Stelle können sich Telearbeiter bei Software- und Hardware-Problemen wenden. Der Benutzerservice versucht (auch telefonisch) kurzfristig Hilfe zu leisten beziehungsweise leitet Wartungs- und Reparaturarbeiten ein. Dazu sollte dem Benutzerservice die Konfiguration der Telearbeitsrechner bekannt sein.
- **Wartungstermine:** Die Termine für Wartungsarbeiten an den Telearbeitsgeräten sollten frühzeitig bekannt gegeben werden, damit die Telearbeiter zu diesen Zeiten den Wartungstechnikern Zutritt zum Telearbeitsplatz oder den Zugriff auf Telearbeitsrechner gewähren oder zu wartende IT-Geräte in die Institution bringen können.
- **Einführung von Standard-Telearbeitsrechnern:** Die IT-Ausstattung aller Telearbeiter einer Institution sollte standardisiert sein, damit der Benutzerservice schnell bei Problemen helfen kann. Auch wird dadurch der konzeptionelle und administrative Aufwand für den Aufbau eines sicheren Telearbeitsrechners vermindert.
- **Fernwartung:** Falls der Telearbeitsrechner über Fernwartung administriert und gewartet werden kann, sind die notwendigen Sicherheitsmaßnahmen zu klären. Außerdem ist mit den betroffenen Telearbeitern der Zeitpunkt für einen Online-Zugriff zur Wartung zu vereinbaren. Damit der Fernwartungszugang nicht missbraucht werden kann, müssen angemessene Sicherungsverfahren festgelegt werden.
- **Transport der IT:** Es sollte aus Gründen der Haftung festgelegt werden, wer autorisiert ist, IT-Geräte und andere Ausstattung für die Telearbeitsplätze zwischen der Institution und den Telearbeitsplätzen zu transportieren. Dabei muss auch der Schutz der Geräte beachtet werden. Ein Laptop kann beispielsweise vom Telearbeiter persönlich transportiert werden, sollte aber mit einer Diebstahlsicherung versehen sein. Die Informationen sollten verschlüsselt sein.

OPS.1.2.4.M10 Durchführung einer Anforderungsanalyse für den Telearbeitsplatz [IT-Betrieb, Leiter IT]

Bevor ein Telearbeitsplatz eingerichtet wird, sollte eine Anforderungsanalyse durchgeführt werden. Sinn dieser Anforderungsanalyse ist es, alle infrage kommenden Einsatzszenarien zu bestimmen, um daraus die benötigten Hard- und Software-Komponenten abzuleiten. Die Ergebnisse einer solchen Anforderungsanalyse müssen dokumentiert und mit den IT-Verantwortlichen abgestimmt werden.

Im Rahmen dieser Anforderungsanalyse sind unter anderem folgende Fragen zu klären:

- Bis zu welchem Vertraulichkeitsanspruch dürfen Daten am Telearbeitsplatz bearbeitet werden?
- Zu welchem Zweck wird der Zugang zur Institution genutzt (Abfragen von Informationen, Einstellen von Informationen, Programmnutzung)?
- Wie hoch ist der Datenverkehr zwischen dem Telearbeitsplatz und der Institution?
- Muss der Telearbeiter auf das Intranet der Institution zugreifen? Wenn ja, muss er auf das gesamte Intranet, das heißt auf alle dort verfügbaren Daten und Dienste oder nur auf Teilbereiche des Intranets zugreifen können?
- Ist für die Telearbeiter die Nutzung des Internets vorgesehen? Wenn ja, bekommt der Telearbeiter einen eigenen Internet-Zugang oder wird dieser Zugang über das Intranet der Institution realisiert?

Je nach Vertraulichkeit der Daten kann es erforderlich sein, bestimmte Übertragungswege von der Institution zum Telearbeitsplatz festzulegen. Dabei kann es sinnvoll sein, einzelne Übertragungswege auszuschließen oder Mindestanforderungen dafür festzulegen. Beispielsweise könnte es vorgeschrieben sein, Papierdokumente mit vertraulichen Informationen nur auf direktem Weg von der Institution zum Telearbeitsplatz in verschlossenen Transportbehältern zu transportieren. Ebenso könnten für verschiedene Vertraulichkeitsgrade unterschiedliche Verschlüsselungsverfahren für die Datenübertragung vorgesehen sein.

Ähnliche Überlegungen sollten angestellt werden, wenn die im Rahmen der Telearbeit zu verarbeitenden Informationen besonders vor Manipulation geschützt werden müssen.

3 Weiterführende Informationen

3.1 Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Telearbeit" finden sich unter anderem in folgenden Veröffentlichungen:

[27001A6.2.1] ISO/IEC 27001:2013

Information technology - Security techniques - Information security management systems - Requirements, insbesondere Annex A, A.6.2.1 Mobile device policy, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/SC 27, Oktober 2013

[ISFPA2] Standard of Good Practice for Information Security

Area PA2 Mobile Computing, Information Security Forum (ISF), June 2018

[NIST80046] Guide to Enterprise Telework, Remote Access and Bring Your Own Device (BYOD) Security

NIST Special Publication 800-46, Revision 2, Juli 2016, http://dx.doi.org/10.6028/NIST.SP.800-46r2, zuletzt abgerufen am 05.10.2018

OPS.2: IT-Betrieb von Dritten

Umsetzungshinweise zum Baustein OPS.2.1 Outsourcing für Kunden

1 Beschreibung

1.1 Einleitung

Immer mehr Institutionen entscheiden sich heutzutage, bestimmte Prozesse und Aktivitäten nicht mehr vollständig selbst zu erbringen, sondern diese an einen Dritten – einen externen Dienstleister – auszulagern. Diese Entscheidung wird in der Regel aufgrund der vielfältigen Möglichkeiten getroffen, die ein solches Outsourcing-Vorhaben mit sich bringen kann. So können unter anderem erhebliche Kosten gespart, externe Ressourcen flexibel genutzt oder Ressourcen entlastet werden, um sich stärker auf die eigenen Kernkompetenzen zu konzentrieren. Diese Chancen gehen jedoch stets mit zum Teil erheblichen Risiken einher (hohe Abhängigkeit von externen Dienstleistern, Verlust von Kontroll- und Steuerungsmöglichkeiten, Risiken für die Informationssicherheit), die das Outsourcing-Vorhaben nicht nur scheitern lassen, sondern im schlechtesten Fall auch die Existenz der auslagernden Institution gefährden können. Ein Beispiel hierfür wäre die unautorisierte Veröffentlichung streng vertraulicher Geschäftsstrategien der auslagernden Institution durch Mitarbeiter des Dienstleisters von Outsourcing-Dienstleistungen. Umso wichtiger ist es, allen mit dem Outsourcing-Vorhaben einhergehenden Risiken ausreichend zu begegnen. Um dieses Ziel zu erreichen, werden nachfolgend Maßnahmen beschrieben, die der Outsourcing-Kunde im Rahmen jeder Phase eines Outsourcing-Vorhabens beachten bzw. umsetzen sollte.

1.2 Lebenszyklus

Beginnend mit der Erstellung eines Grobkonzepts und einer Strategie für das Outsourcing-Vorhaben über die Wahl des passenden Dienstleisters und die anschließende Vertragsgestaltung bis hin zur sicheren Migration und dem Regelbetrieb ist im Rahmen eines Outsourcing-Projekts einer Vielzahl von Sicherheitsrisiken zu begegnen. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die im Zuge dessen beachtet werden müssen, sind im Folgenden beschrieben.

Planung und Konzeption

Damit ein Outsourcing-Vorhaben erfolgreich umgesetzt werden kann, sollten bereits im Vorfeld der eigentlichen Auslagerung alle notwendigen Rahmenbedingungen für das Projekt festgelegt werden.

Hierzu gehören strategische Überlegungen, wie das Abwägen von Chancen und Risiken. Zudem muss eine Entscheidung hinsichtlich des Outsourcing-Modells getroffen werden, das die Realisierung der mit dem Outsourcing-Vorhaben verbundenen Erwartungen stützt (OPS.2.1.M5 Festlegung einer Outsourcing-Strategie). Des Weiteren sind im Vorhinein Sicherheitsstandards zu definieren, die für das Outsourcing-Vorhaben gelten sollen. Diese werden gegenüber einem potenziellen Outsourcing-Partner zu Sicherheitsanforderungen (OPS.2.1.M1 Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben). Mitarbeiter und deren Vertretung sind ebenso rechtzeitig über das Outsourcing-Vorhaben zu informieren (OPS.2.1.M2 Rechtzeitige Beteiligung der Personalvertretung). Zudem sind bereits im Rahmen der Planung Regelungen festzulegen, wie der sichere Einsatz von Fremdpersonal im Zuge der Kooperation mit dem Dienstleister gewährleistet wird (siehe OPS.3 Outsourcing für Dienstleister).

Umsetzung

Neben den Sicherheitsanforderungen sind auch alle anderen Voraussetzungen, die ein Outsourcing-Partner erfüllen muss, für jedes Outsourcing-Projekt individuell zu definieren, um objektive Vergleiche zu ermöglichen und einen optimalen Outsourcing-Partner zu identifizieren (OPS.2.1.M3 Auswahl eines geeigneten Outsourcing-Dienstleisters).

Um die gesetzten Outsourcing-Ziele zu erreichen, sollten alle dafür notwendigen Leistungen, die durch den Outsourcing-Dienstleister erbracht werden müssen, vertraglich fixiert werden (OPS.2.1.M4 Vertragsgestaltung mit dem Outsourcing-Dienstleister). Für jedes Outsourcing-Vorhaben sollte ein Sicherheitskonzept erarbeitet werden, das der Individualität der Kombination von Kunden, Dienstleister und dem ausgelagertem Prozess Rechnung trägt (OPS.2.1.M6 Erstellung eines Sicherheitskonzeptes für das Outsourcing-Vorhaben). Nachdem das Sicherheitskonzept erstellt wurde, ist sicherzustellen, dass Maßnahmen zur Aufrechterhaltung der Informationssicherheit (OPS.2.1.M11 Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb) umgesetzt werden, damit ein Sicherheitskonzept tatsächlich wirkt und nicht veraltet.

Ebenso werden in dieser Phase die Kommunikationswege und die sichere Migration von Prozessen und Aufgaben definiert (OPS.2.1.M7 Festlegung der möglichen Kommunikationspartner; OPS.2.1.M13 Sichere Migration bei Outsourcing-Vorhaben).

Hinsichtlich der Netzanbindung und dem Datenaustausch mit dem Outsourcing-Dienstleister sind Regelungen zu treffen, da normalerweise viele Prozesse hiervon abhängig sind. Die Dienstleister sind aber eigenständig und als Dritte nicht direkt im Einflussbereich des Kunden (siehe OPS.2.1.M9 Vereinbarungen über die Anbindung an Netze der Outsourcing-Partner und OPS.2.1.M10 Vereinbarungen über Datenaustausch zwischen den Outsourcing-Partnern).

Betrieb und Aussonderung

Im laufenden Betrieb sollten regelmäßig alle vereinbarten Parameter geprüft werden. Hierzu gehört neben der Überwachung definierter Leistungskennzahlen die Kontrolle von Maßnahmen zur Aufrechterhaltung der Informationssicherheit des Outsourcing-Dienstleisters (OPS.2.1.M11 Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb).

Sollte im Rahmen eines Outsourcing-Vorhabens von einer der Parteien eine Änderung gewünscht werden, sollte diese nach einem definierten Prozess umgesetzt werden (OPS.2.1.M12 Änderungsmanagement). Eine Änderung der Outsourcing-Beziehung kann auch deren Beendigung sein. Für diesen Fall sollten vertragliche Abmachungen und Vorkehrungen getroffen werden. Insbesondere bei einem unerwarteten Ende des Outsourcing-Vorhabens (z. B. aufgrund einer Insolvenz des Outsoucing-Dienstleisters) kann das Fehlen solcher Vorkehrungen zu erheblichen wirtschaftlichen Schäden führen (OPS.2.1.M15 Geordnete Beendigung eines Outsourcing- Verhältnisses).

Notfallvorsorge

Im Rahmen der Notfallvorsorge sollten auch die vereinbarten Parameter kontrolliert werden (OPS.2.1.M14 Notfallvorsorge beim Outsourcing).

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Outsourcing für Kunden" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

OPS.2.1.M1 Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben

Im Rahmen eines Outsourcing-Vorhabens müssen Sicherheitsanforderungen festgelegt werden, die im Einklang mit der Outsourcing-Strategie stehen. Diese sollten als Grundlage für die Auswahl eines Outsourcing-Dienstleisters und die anschließende Vertragsgestaltung dienen (OPS.2.1.M3 Auswahl eines geeigneten Outsourcing-Dienstleisters, OPS.2.1.M4 Vertragsgestaltung mit dem Outsourcing-Dienstleister und OPS.2.1.M11 Planung und Aufrechterhaltung der Informationssicherheit).

Die Sicherheitsanforderungen können beispielsweise auf Basis von IT-Grundschutz festgelegt werden.

Um das erforderliche Sicherheitsniveau zu erreichen, sollten von Outsourcing-Kunden und Outsourcing-Dienstleister gemeinsam Sicherheitsziele und darauf aufbauend Sicherheitsanforderungen entwickelt werden, die der Individualität des jeweiligen Outsourcing-Vorhabens Rechnung tragen.

In diese Betrachtungen müssen alle Schnittstellen zwischen Outsourcing-Kunden und Outsourcing-Dienstleister mit den jeweiligen Sicherheitsanforderungen mit einbezogen werden. Hierbei sollten alle Aspekte des Identitäts- und Berechtigungsmanagements berücksichtigt werden. Hierfür können z. B. alle beteiligten Benutzer bestimmten Gruppen (Administrator, Kontrolleur, Mitarbeiter etc.) zugeordnet werden, wobei jede Gruppe bestimmte Rechte erhält, die sie im Rahmen ihrer Tätigkeit zwingend benötigt. Eine weitere Möglichkeit ist die Definition bestimmter Rollen, d. h. die Zusammenfassung bestimmter Rechte. Benutzer, die im Rahmen ihrer Tätigkeit in dem Outsourcing-Vorhaben eine oder mehrere bestimmte Rollen ausfüllen, erhalten dann die erforderlichen Rechten.

In jedem Fall sollte bei der Rechtevergabe das *Least-Privilege-Prinzip* beachtet werden. So erhalten alle Benutzer nur die unbedingt notwendigen Rechte. Die Gefahr vorsätzlich oder fahrlässig verursachter Sicherheitsvorfälle kann so reduziert werden (siehe hierzu auch OPS.2.1.M6 Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben).

Um Zugriffsrechte adäquat vergeben zu können, ist es notwendig, alle Daten und Informationen zu klassifizieren. Die Klassifizierung muss entsprechend der strategischen Bedeutung vorgenommen werden.

Es ist zu bedenken, dass das Festlegen von Sicherheitsanforderungen ein iterativer Prozess ist:

- Zunächst werden die gewünschten Sicherheitsanforderungen durch den Kunden spezifiziert.
- Danach wird in der Angebotsphase abgeglichen, wie und ob die gewünschten Sicherheitsanforderungen durch die anbietenden Dienstleister geleistet werden können.
- Ist ein Dienstleister ausgewählt, so muss mit diesem die weitere Verfeinerung der Sicherheitsanforderungen (z. B. basierend auf den eingesetzten Betriebssystemen oder Sicherheitsmechanismen) erarbeitet werden. In der Endphase dieses Abstimmungsprozesses müssen dann auch die Sicherheitsanforderungen für die konkrete Umsetzung definiert werden.

Generell ergeben sich für Outsourcing-Szenarien folgende Mindestsicherheitsanforderungen:

- Die Umsetzung des IT-Grundschutzes oder eines vergleicbaren Schutzniveaus ist eine Minimalforderung an beide Outsourcing-Parteien. Zusätzlich müssen sowohl Outsourcing-Dienstleister als auch der Outsourcing-Kunde selbst ein Sicherheitskonzept besitzen und dieses umgesetzt haben.
- Es ist wichtig, die relevanten IT-Verbünde genau abzugrenzen (z. B. nach Fachaufgabe, Geschäftsprozess, IT-Systemen), so dass alle Schnittstellen identifiziert werden können. An die Schnittstellen können dann entsprechende technische Sicherheitsanforderungen gestellt werden.
- Es muss eine Ist-Strukturanalyse von IT-Systemen und Anwendungen erfolgen.
- Es muss eine Schutzbedarfsfeststellung (z. B. von Anwendungen, Systemen, Kommunikationsverbindungen, Räumen) bezüglich Vertraulichkeit, Integrität und Verfügbarkeit erfolgen.

Natürlich sind auch relevante Gesetze und Vorschriften zu beachten. Dies kann besonders in Fällen, in denen Kunden oder Dienstleister länderübergreifend oder weltweit operieren, aufwendig sein.

Im Rahmen der Sicherheitsanforderungen ist festzulegen, welche Rechte (z. B. Zutrittsrechte, Zugriffsrechte auf Daten und Systeme) dem Outsourcing-Dienstleister vom Kunden eingeräumt werden.

Die Anforderungen an Infrastruktur, Organisation, Personal und Technik müssen beschrieben werden. Es genügt hier oftmals die Verpflichtung auf ein Sicherheitsniveau, das IT-Grundschutz entspricht. Sollten darüber hinausgehende Anforderungen bestehen, müssen diese detailliert beschrieben werden. Dies hängt entscheidend von der Sicherheitsstrategie und bereits vorhandenen Systemen und Anwendungen ab. Beispielsweise könnten folgende Punkte in Abhängigkeit vom Outsourcing-Vorhaben detailliert werden:

Organisatorische Regelungen und Prozesse

- Anforderungen an sicherheitskritische organisatorische Prozesse (z. B. Zeitrestriktionen für den Alarmierungsplan) können spezifiziert werden.
- Spezielle Anforderungen an bestimmte Rollen können festgelegt werden. Es kann beispielsweise gefordert werden, dass ein ISB mit speziellen Kenntnissen (z. B. Host-Kenntnissen) beim Outsourcing-Dienstleister benannt werden muss.

Hard-/Software

- Der Einsatz zertifizierter Produkte (z. B. gemäß Common Criteria oder ITSEC) beim Outsourcing-Dienstleister kann gefordert werden.
- Anforderungen an die Verfügbarkeit von Diensten und IT-Systemen können gestellt werden. Beispielsweise kann in diesem Zusammenhang der Grad und die Methode der Lastverteilung (z. B. für Web-Server mit Kundenzugriff bei sehr vielen Kunden) vorgegeben werden.
- Vorgaben an die Mandantenfähigkeit sowie die diesbezügliche Trennung von Hard- und Software können formuliert werden. Beispielsweise kann festgelegt werden, dass keine IT-Systeme des Kunden in Räumen untergebracht werden dürfen, in denen bereits Systeme anderer Mandanten des Dienstleisters stehen.

Kommunikation

- Spezielle Verfahren zur Absicherung der Kommunikation zwischen Dienstleister und Auftraggeber wie Einsatz von Verschlüsselungs- und Signaturverfahren können fest vorgegeben werden.

Kontrollen und QS

- Allgemeine Anforderungen bezüglich Kontrolle und Messung von Sicherheit, Qualität oder auch Abläufen und organisatorischen Regelungen können festgelegt werden, z. B. Zeitintervalle, Zuständigkeiten.
- Gewünschte Verfahren oder Mechanismen für die Kontrolle und Überwachung, wie unangekündigte Kontrollen vor Ort, Audits (unter Umständen durch unabhängige Dritte) können spezifiziert werden.
- Anforderungen an die Protokollierung und Auswertung von Protokolldateien können festgelegt werden.

Generell bilden die festgelegten IT-Sicherheitsanforderungen eine der Grundlagen für die Wahl eines geeigneten Outsourcing-Dienstleisters. Spezielle IT-Sicherheitsanforderungen müssen jedoch eventuell an das von Dienstleistern umsetzbare IT-Sicherheitsniveau angepasst werden.

Bei Ausschreibungen oder bei der Auswahl eines Outsourcing-Dienstleisters sollte immer eine Leistungsbeschreibung oder ein Pflichtenheft erstellt werden mit den folgenden Inhalten:

- Beschreibung des Outsourcing-Vorhabens (Aufgabenbeschreibung und Aufgabenteilung) sowie
- Beschreibungen zum geforderten Qualitätsniveau, welches nicht zwangsläufig dem Niveau des Auftraggebers entsprechen muss,
- Anforderungen an die Informationssicherheit und
- Kriterien zur Messung von Servicequalität und Sicherheit.

In Einzelfällen kann es notwendig sein, die Detailanforderungen bezüglich Sicherheit nur gegen eine Vertraulichkeitsvereinbarung (Non-Disclosure Agreement) an Dienstleister herauszugeben, da sich daraus Hinweise auf existierende oder geplante Sicherheitsmechanismen ableiten lassen.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Outsourcing für Kunden".

OPS.2.1.M2 Rechtzeitige Beteiligung der Personalvertretung [Leiter Organisation]

Die rechtzeitige und umfassende Information der Personalvertretung empfiehlt sich grundsätzlich bei allen Projekten, die die betrieblichen Interessen der Beschäftigten berühren. Hierzu gehören im Allgemeinen auch Outsourcing-Vorhaben. Eine frühzeitige Einbindung der Personalvertretung des Outsourcing-Kunden ist empfehlenswert, möglichst schon in der Planungsphase des Outsourcing. Dies kann zum Gelingen des Projekts beitragen. Die frühzeitige Einbeziehung kann Zeitverzögerungen bei der Umsetzung von Maßnahmen verhindern und die Akzeptanz für das Outsourcing-Vorhaben erhöhen. Wechselbereitschaft der Mitarbeiter, Motivation, Arbeitszufriedenheit und zügige Projektabwicklung können durch Kooperation aller Beteiligten positiv beeinflusst werden. Zudem ist die Expertise jener Mitarbeiter, die später im Rahmen der konkreten Prozesse rund um das Outsourcing-Vorhaben arbeiten, ein nicht zu unterschätzender Erfolgsfaktor bei der Umsetzung.

Rechtliche Grundlage der Beteiligung der Personalvertretung sind in Deutschland die Betriebsverfassungs- und Personalvertretungsgesetze von Bund und Ländern sowie einzelne Vorschriften des Bürgerlichen Gesetzbuchs (BGB).

Mit Outsourcing-Vorhaben gehen oft Maßnahmen einher, die prinzipiell die Verhaltens- oder Leistungsüberwachung von Mitarbeitern ermöglichen. Dies bedarf z. B. der Mitbestimmung der Personalvertretung.

Die Übertragung von Aufgaben oder Prozessen einer Institution an einen Dritten führt in der Regel auch zu Veränderungen in der Personalstruktur, was ebenfalls die Einbindung der Personalvertretung notwendig macht. Dies kann auch bedeuten, dass Mitarbeiter nach der Umsetzung eines Outsourcing-Vorhabens vom Outsourcing-Kunden zum Dienstleister wechseln müssen. Für den Kunden, also den ursprünglichen Arbeitgeber, besteht in diesem Fall eine Informationspflicht. Die Arbeitnehmer sind vor dem Betriebsübergang schriftlich zu unterrichten. Die Mitarbeiter müssen nicht individuell unterrichtet werden, es ist jedoch empfehlenswert, auf die speziellen Auswirkungen für spezifische Arbeitnehmergruppen individuell einzugehen. Inhalte der Unterrichtung werden in § 613a Abs. 5 BGB festgeschrieben.

Auch die Folgen für die Betriebsverfassungsorgane selbst müssen im Rahmen eines Outsourcing-Vorhabens geprüft werden. Hierzu ist es empfehlenswert, eine professionelle Rechtsberatung hinzuzuziehen.

OPS.2.1.M3 Auswahl eines geeigneten Outsourcing-Dienstleisters

Da die Auswahl des Outsourcing-Dienstleisters eine weitreichende und risikobehaftete Entscheidung ist, sollten für jedes Outsourcing-Vorhaben klare Auswahl-Kriterien festgelegt werden. Im Folgenden sind beispielhafte Bewertungskriterien beschrieben, die bei der Entscheidung für einen Outsourcing-Dienstleister berücksichtigt werden sollten.

Transparenz

Der Outsourcing-Dienstleister sollte die für seine Leistungserbringung grundlegenden Prozesse, so transparent darstellen können, dass zweifelsfrei von einer Vertragserfüllung durch ihn ausgegangen werden kann. Dem Outsourcing-Kunden sollten zudem die Sicherheitsvorkehrungen, die der Outsourcing-Dienstleister für das spezielle Outsourcing-Vorhaben getroffen hat, soweit nötig bekannt sein. Dies soll insbesondere ein reibungsloses Zusammenspiel der Sicherheitsmechanismen zwischen den Outsourcing-Partnern ermöglicht.

Prüfung der Sicherheitsanforderungen

Der Outsourcing-Kunde muss sich über die Sicherheitsanforderungen auf Seiten des Outsourcing-Dienstleisters insofern befassen, dass der Outsourcing-Dienstleister mindestens das gewünschte Sicherheitsniveau des Outsourcing-Kunden abdeckt. Fordert der Outsourcing-Kunde beispielsweise einen hohen Schutzbedarf, muss der Outsourcing-Dienstleister mindestens die Anforderungen für einen hohen Schutzbedarf erfüllen.

Reputation

Die Reputation eines Dienstleisters am Markt lässt sich quantitativ nicht erfassen. Erfahrungsberichte anderer Kunden, Medienberichte und auch die aktive öffentliche Präsenz des Dienstleisters können hier qualitativ betrachtet werden.

Referenzen

Der Dienstleister sollte Referenzen für ähnliche Outsourcing-Vorhaben aufweisen können. Dabei ist auf Interessenskonflikte durch Geschäftsbeziehungen zu Konkurrenten des Kunden zu achten.

Die angegebenen Referenzen sollten zumindest stichprobenartig hinterfragt werden. So können bestehende oder ehemalige Kunden des potenziellen Dienstleisters zu ihren Projekterfahrungen mit dem Dienstleister befragt werden.

Je nach Bedarf sollte der Dienstleister einschlägige Sicherheitsstandards umsetzen, z. B. ISO 27001 auf Basis von BSI IT-Grundschutz. Bei bestehenden Zertifizierungen muss der Outsorcing-Kunde darauf achten, dass der im Zertifikat enthaltene Geltungsbereich und Schutzbedarf den vom Outsourcing-Kunden benötigten Einsatzbereich umfasst. Hierzu ist eine Prüfung des zertifizierten Geltungsbereichs erforderlich.

Business Fit/Unternehmenskultur

Bei ausländischen Dienstleistern müssen besondere Aspekte bedacht werden. Dazu gehören beispielsweise: fremde Gesetzgebung, andere Haftungsregelungen, Spionagerisiken, andere Sicherheitskultur, im Partnerunternehmen oder durch die landesspezifische Gesetzgebung zugelassene und verwendbare Sicherheitsmechanismen.

Zudem sollte die Organisationsform des Dienstleisters betrachtet werden, da diese z. B. die Haftungsgrenzen beeinflussen kann. Weiterhin sollte die Eigentümerstruktur recherchiert werden, um mögliche Einflussfaktoren im Vorfeld abzuklären.

Abschließend sollte überprüft werden, inwieweit die beschriebenen Aspekte mit der Situation bzw. den Vorstellungen des Kunden vereinbar sind.

Anforderungen an Mitarbeiter

Auch an die Mitarbeiter eines Outsourcing-Dienstleisters sind Anforderungen zu stellen.

Der Outsourcing-Kunde sollte überprüfen, inwieweit die Mitarbeiter des Outsourcing-Dienstleisters über die notwendigen Qualifikationen verfügen. Zudem sollte die Anzahl der verfügbaren qualifizierten Mitarbeiter, die für den Outsourcing-Kunden zur Verfügung stehen, bewertet werden. Dabei sollten auch Vertretungsregelungen und Arbeitszeiten hinterfragt werden.

Bei der Wahl ausländischer Partner muss eine gemeinsame Sprache für die Kommunikation zwischen den eigenen Mitarbeitern und denen des Dienstleisters festgelegt werden. Hierbei sollte auch hinterfragt werden, ob die vorhandenen Sprachkenntnisse für die Klärung von Detailproblemen ausreichen. Hier sind zudem Aspekte wie unterschiedliche Zeitzonen oder rechtliche Besonderheiten zu beachten.

Abhängig von dem notwendigen Sicherheitsniveau für das Outsourcing-Vorhaben sollte falls erforderlich geprüft werden, ob eine Sicherheitsüberprüfung der Mitarbeiter vorliegt bzw. eine solche komplikationslos durchgeführt werden kann.

OPS.2.1.M4 Vertragsgestaltung mit dem Outsourcing-Dienstleister

Outsourcing-Verträge sind nicht, wie Kauf-, Werk- oder Dienstverträge, im Bürgerlichen Gesetzbuch (BGB) geregelt. Es ist demzufolge darauf zu achten, alle Aspekte eines Outsourcing-Projekts bei der Vertragsgestaltung schriftlich zu vereinbaren. Das Vertragswerk sollte dabei sowohl die erforderlichen Rechte und Pflichten der Outsourcing-Partner festschreiben. Die Art, der Umfang und der Detaillierungsgrad der vertraglichen Regelungen sollten dabei individuell an das Outsourcing-Vorhaben angepasst werden. Vertragliche Regelungen im Vorfeld sind insbesondere deshalb wichtig, weil viele Risiken für den Outsourcing-Kunden dadurch vorab reduziert bzw. vermieden werden können. Die folgenden Aspekte sind daher aus Sicht des Outsourcing-Kunden im Zuge jeder Vertragsgestaltung zu berücksichtigen.

Klare Spezifizierung und Abgrenzung der Leistung

Eine ungenaue Definition der Leistungserbringung führt oftmals zu nachträglichen und unvorhersehbaren Mehrkosten für den Outsourcing-Kunden, da dieser beispielsweise eine vermeintliche "Mehrleistung" des Outsourcing-Dienstleisters in Anspruch nehmen muss. Ansprüche des Dienstleisters auf eine Abgeltung bei zusätzlich erbrachten Leistungen können besser bewertet werden, wenn die zu erbringende Leistung klar definiert wurde. Es ist daher empfehlenswert, auch "selbstverständliche" Leistungen zu spezifizieren. Entsprechende Diskussionen beziehungsweise Meinungsverschiedenheiten, die das Geschäftsverhältnis zwischen den Vertragsparteien nachhaltig schädigen könnten, werden dadurch im Vorfeld bestmöglich vermieden. Zudem kann dem Risiko des Verlusts der Kontroll- und Steuerungsmöglichkeiten entgegengewirkt werden, wenn die auslagernde Institution mittels einer klaren Leistungsabgrenzung Abweichungen leichter erkennen bzw. nachweisen kann. In diesem Zusammenhang schafft der Outsourcing-Kunde zudem eine vertragsrechtliche Grundlage für mögliche Sanktionen oder Schadensersatzforderungen bei Schlecht- oder Nichterfüllung der Leistung.

Datenschutz und Datensicherheit

Weiterhin sollten Regelungen zur Einhaltung datenschutzrechtlicher Bestimmungen festgelegt werden. Dazu zählen u. a. Sicherheitsvorkehrungen, die der Outsourcing-Dienstleister im Zuge der Datenverarbeitung zu beachten hat. Dadurch soll gewährleistet werden, dass die Outsourcing-Partner die gesetzlichen Bestimmungen des Bundesdatenschutzgesetzes (BDSG) bzw. die EU-Datenschutz-Grundverordnung (EU -DSGVO) und andere Regelungen wie Sozialgesetzbuch (SGB) einhält und die Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Informationen schützt. Der Vertrag sollte die notwendigen organisatorischen Maßnahmen festlegen, die von dem Outsourcing-Dienstleister ergriffen werden müssen, um einen unbefugten Zugriff auf die Daten des Outsourcing-Kunden zu verhindern. Dabei sollten insbesondere der Schutz der Systeme gegen unbefugte oder zufällige Vernichtung, den zufälligen Verlust, technische Fehler, Fälschung, Diebstahl, widerrechtliche Verwendung, unbefugtes Ändern, Kopieren oder Zugreifen im Fokus stehen. Zudem sollte festgelegt werden, in welcher Weise die Vertraulichkeit der Daten durch technische, personelle und organisatorische Maßnahmen geschützt werden soll. Falls erforderlich sind zusätzliche Vereinbarungen zur Wahrung des Geschäftsgeheimnisses des Kunden vertraglich zu regeln.

Infrastruktur

- Umfang der gemeinsam genutzten Infrastruktur
- Anforderungen des Outsourcing-Kunden an die Absicherung der gemeinsam genutzten Infrastruktur
- Verbleib der Eigentumsrechte aller Bestandteile der Infrastruktur

Organisatorische Regelungen / Prozesse

- Vertraulichkeitsvereinbarungen (Non-Disclosure Agreements) sind vertraglich zu fixieren. Dies sollte bereits in der Phase der Vertragsgestaltung selbst berücksichtigt werden, da Sicherheitsanforderungen des Outsourcing-Kunden unter Umständen Schlüsse auf die vorhandenen Sicherheitssysteme zulassen.
- Festlegung von Kommunikationswegen und Ansprechpartnern
- Festlegung von Prozessen, Arbeitsabläufen und Zuständigkeiten
- Integration der Dienstleistung in den Wertschöpfungsprozess des Outsourcing-Kunden
- Arbeitsteilung bei der Serviceerbringung / Mitwirkungspflichten des Outsourcing-Kunden
- Verfahren zur Behebung von Problemen, Benennung von Ansprechpartnern mit den nötigen Befugnissen bei beiden Vertragsparteien
- Regelmäßige Abstimmungsrunden
- Vorgehensweise bei der Leistungsanpassung
- Archivierung und Löschung von Datenbeständen (insbesondere bei Beendigung des Vertragsverhältnisses)
- Zugriffsmöglichkeiten des Outsourcing-Dienstleisters auf IT-Ressourcen des Outsourcing-Kunden: Wer greift wie auf welches System zu? Wie sind die Zuständigkeiten und Rechte?
- Zutritts- und Zugriffsberechtigungen für Mitarbeiter des Outsourcing-Dienstleisters zu den Räumlichkeiten und IT-Systemen des Outsourcing-Kunden
- Zutritts- und Zugriffsberechtigungen für Mitarbeiter des Outsourcing-Kunden zu den Räumlichkeiten und IT-Systemen des Outsourcing-Dienstleisters
- physischer Aufbewahrungsort von Daten

Personal

- Gestaltung der Arbeitsplätze von Mitarbeitern des Outsourcing-Dienstleisters, die zum Outsourcing-Kunden entsandt werden (z. B. die Einhaltung der Bildschirmarbeitsplatzrichtlinie)
- Festlegung und Abstimmung von Vertretungsregelungen bei beiden Vertragspartnern
- Verpflichtung zu Fortbildungsmaßnahmen

Regelungen im Rahmen der

Im Rahmen der Notfallvorsorge sollten zumindest die folgenden Aspekte geregelt werden, um eine kontinuierliche Fortführung des Geschäftsbetriebs zu gewährleisten:

- Kategorien zur Einteilung von Fehlern und Störfällen nach Art, Schwere und Dringlichkeit
- Erforderliche Maßnahmen beim Eintreten eines Störfalls
- Reaktionszeiten und Eskalationsstufen
- Mitwirkungspflicht des Outsourcing-Dienstleisters bei der Behebung von Notfällen
- Art der Einbindung und zeitliche Abfolge von Notfallübungen beim Outsourcing-Dienstleister
- Anforderungen des Outsourcing-Kunden an die Art und den Umfang der Datensicherung
- Vereinbarung, ob bzw. welche Systeme redundant ausgelegt sein müssen

Von besonderer Bedeutung können Regelungen im Fall höherer Gewalt sein. Des Weiteren sollte beispielsweise geklärt sein, wie bei einem Streik des Personals des Outsourcing-Dienstleisters die Verfügbarkeit von Daten und Systemen sichergestellt wird. Besonders wenn Outsourcing-Dienstleister und Outsourcing-Kunden unterschiedlichen Branchen angehören oder ihren Sitz in verschiedenen Ländern haben, kann der Kunde von derartigen Vorkommnissen gänzlich überrascht werden.

Weiterverlagerungen

Es muss geregelt werden, wie Dritte, Subunternehmer und Unterauftragnehmern durch den Outsourcing-Dienstleister eingebunden werden. Allgemein empfiehlt es sich, dies nicht grundsätzlich auszuschließen, sondern sinnvolle Bedingungen festzulegen. Grundsätzlich sollte jede Weiterverlagerung nur zulässig sein, wenn alle Anforderungen erfüllt werden, die im Rahmen der bestehenden Outsourcing-Beziehungen an den Dienstleister gestellt werden. Der Outsourcing-Kunde sollte sich eine Zustimmung zur Weiterverlagerung vorbehalten.

Mandanten

Im Rahmen der Mandantentrennung muss der Outsourcing-Dienstleister sicherstellen, dass Störungen oder Notfälle bei anderen Mandanten nicht die Abläufe und Systeme des Outsourcing-Kunden beeinträchtigen. Zudem dürfen die Daten des Outsourcing-Kunden unter keinen Umständen anderen Mandanten zugänglich werden.

Der Outsourcing-Dienstleister sollte daher vertraglich verpflichtet werden, ein Mandantenkonzept zu erstellen, in dem beschrieben ist, auf welche Weise die IT-Systeme und Anwendungen mandantenfähig betrieben werden. Falls notwendig, muss eine physikalische Trennung, d. h. dedizierte Hardware, vereinbart werden. Weiterhin kann festgelegt werden, dass die vom Outsourcing-Dienstleister eingesetzten Mitarbeiter nicht für andere Outsourcing-Kunden eingesetzt werden.

Änderungsmanagement und Testverfahren

Es müssen vertragliche Regelungen festgelegt werden, die es dem Outsourcing-Kunden jederzeit ermöglichen, sich neuen Anforderungen anzupassen. Dies gilt insbesondere, wenn sich beispielsweise gesetzliche Vorgaben ändern. Es ist festzulegen, wie auf Systemerweiterungen, gestiegene Anforderungen oder knapp werdende Ressourcen reagiert wird.

In diesem Zusammenhang ist auch die Betreuung und Weiterentwicklung bereits vorhandener Systeme zu regeln. Nicht selten übernimmt der Outsourcing-Dienstleister selbst entwickelte Systeme oder Software vom Outsourcing-Kunden, der diese damit nicht mehr in seinem Sinne weiterentwickeln kann. Der Evolutionspfad von Systemen sollte daher ebenfalls vertraglich geregelt werden.

Eine kontinuierliche Verbesserung der Dienstleistungsqualität und des Sicherheitsniveaus sollte möglichst präzise in den Service/Security Level Agreements (SLA) festgeschrieben werden. Dies gilt sowohl für den jeweiligen Zeitrahmen zur Behebung von Fehlern als auch für die Nachverfolgung der Sicherheitsanforderungen.

Des Weiteren sollten Testverfahren für neue Hard- und Software festgelegt werden. Dabei sind folgende Punkte einzubeziehen:

- Regelungen für Updates und Systemanpassungen
- Trennung von Test- und Produktionssystemen
- Zuständigkeiten bei der Erstellung von Testkonzepten
- Festlegen von zu benutzenden Testmodellen und Testdaten
- Zuständigkeiten von Outsourcing-Kunden und Outsourcing-Dienstleitern bei der Durchführung von Tests (z. B. Mitarbeit oder Hilfestellung des Outsourcing-Kunden, Abnahme- und Freigabeprozeduren)
- Informationspflicht und Absprache vor wichtigen Eingriffen in ein System (Negativbeispiel: Der Outsourcing-Dienstleister spielt eine neue Version des Betriebssystems auf dem Server ein. Durch unerwartete Fehler werden wichtige Anwendungen gestört, ohne dass der Outsourcing-Kunde sich vorbereiten konnte.)
- Genehmigungsverfahren für die Durchführung von Tests
- Festlegung zumutbarer Qualitätseinbußen während der Testphase (z. B. Verfügbarkeit und Kapazität)

Kontroll-

Die Qualität der Leistungserbringung muss regelmäßig kontrolliert werden. Dem Outsourcing-Kunden müssen die dazu notwendigen Auskunfts-, Einsichts-, Zutritts- und Zugangsrechte zu den von ihm genutzten Räumlichkeiten vertraglich zugesichert werden. Wenn unabhängige Dritte Audits oder Benchmark-Tests durchführen sollen, muss dies ebenfalls im Vertrag geregelt werden.

Allen Institutionen, die bei dem Outsourcing-Kunden Prüfungen durchführen müssen (z. B. Aufsichtsbehörden), müssen auch bei dem Outsourcing-Dienstleister die entsprechenden Kontrollmöglichkeiten (z. B. Zutrittsrechte, Dateneinsicht) wahrnehmen können.

Um die Prüfungs- und Kontrollmöglichkeiten zu gewährleisten, sollte der Outsourcing-Vertrag eine entsprechende Erklärung des Outsourcing-Dienstleisters enthalten, dass dieser eine, falls erforderlich auch unangekündigte, Prüfung des durch den Outsourcing-Kunden ausgelagerten Bereichs duldet.

Informationspflichten und Kommunikation

Der Dienstleister sollte vertraglich dazu verpflichtet werden, über alle Entwicklungen zu berichten, die einen Einfluss auf die Leistungserbringung haben könnten. Dadurch soll es dem Outsourcing-Kunden ermöglicht werden, rechtzeitig zu reagieren. Zudem sollte gewährleistet sein, dass der Outsourcing-Dienstleister regelmäßig über aktuelle (Sicherheits-)Vorkommnisse bzw. Probleme hinsichtlich interner Arbeitsabläufe berichtet. In dieser Hinsicht sind z. B. Ergebnisse von Revisionen relevant.

Um einen angemessenen Informationsfluss zu gewährleisten, sollten z. B. die Art der Information, die zu nutzenden Kommunikationswege und die jeweiligen Ansprechpartner (Rollen), an die bestimmte Informationen weitergeleitet werden sollen, vertraglich festgelegt werden.

Es sollten Regelungen für das Ende der Outsourcing-Beziehung spezifiziert werden. So sollten in jedem Fall Kündigungsfristen vereinbart und ausreichend dimensioniert werden. In Hinsicht auf die Dimensionierung der Kündigungsfristen ist darauf zu achten, dass dem Outsourcing-Kunden genügend Zeit bleibt, um die ausgelagerten Aktivitäten und Prozesse wieder zu integrieren oder auf einen anderen Outsourcing-Dienstleister zu übertragen.

Zudem kann der Outsourcing-Dienstleister falls erforderlich darauf verpflichtet werden, im Zuge einer Rückintegration oder einer Übertragung der Leistungserbringung auf einen anderen Outsourcing-Dienstleister auch nach dem Ende der Outsourcing-Beziehung unterstützend zur Verfügung zu stehen.

Des Weiteren ist der Outsourcing-Dienstleister vertraglich darauf zu verpflichten, nach Beendigung der Outsourcing-Beziehung alle Hard- und Software inklusive der darauf gespeicherten Daten, die sich ursprünglich im Besitz des Outsourcing-Kunden befanden, zurückzugeben oder zu vernichten.

OPS.2.1.M5 Festlegung einer Outsourcing-Strategie

Outsourcing-Vorhaben sind oftmals mit vielen Vorteilen verbunden. Diesen Vorteilen stehen jedoch einige Risiken gegenüber, die dazu führen können, dass die erwünschten Ziele nicht erreicht werden können. Zudem erfolgt die Bindung an einen Outsourcing-Dienstleister normalerweise für längere Zeit. Eine strategische Planung des Outsourcing-Vorhabens ist daher von großer Bedeutung.

Hierbei sollten wirtschaftliche, technische und organisatorische Aspekte bedacht werden. Zudem spielen sicherheitsrelevante Aspekte eine wichtige Rolle. Die Informationssicherheit muss bereits bei Beginn der Planungen mit betrachtet werden, da ihr eine zentrale Bedeutung in Outsourcing-Vorhaben zukommt.

Festlegung der Outsourcing-Ziele

In jeder Outsourcing-Strategie sollten die Ziele des Vorhabens genau definiert werden. Dabei sollte stets die Konformität mit der Sicherheitsleitlinie gewahrt werden. So dürfen die Outsourcing-Ziele den übergeordneten Zielen der Institution sowie den daraus abgeleiteten Sicherheitszielen nicht widersprechen. Folgende Gesichtspunkte sollten betrachtet werden:

- Sicherheitsleitlinie (Flexibilität, Abhängigkeiten, zukünftige Planungen),
- Machbarkeitsstudie mit Zusammenstellung der Rahmenbedingungen und
- betriebswirtschaftliche Aspekte mit Kosten-Nutzen-Abschätzung.

Nach ersten strategischen Überlegungen muss zunächst geklärt werden, welche Geschäftsprozesse, Aufgaben oder Anwendungen generell für ein Outsourcing in Frage kommen.

Dabei darf die Bedeutung der rechtlichen Rahmenbedingungen nicht unterschätzt werden. Gesetze könnten beispielsweise das Auslagern bestimmter Kernaufgaben einer Institution generell verbieten oder zumindest weitreichende Auflagen enthalten und die Beteiligung von Aufsichtsbehörden vorschreiben. In der Regel bleibt der Auftraggeber weiterhin gegenüber seinen Kunden oder staatlichen Stellen voll verantwortlich für Dienstleistungen oder Produkte, unabhängig davon, ob einzelne Aufgabenbereiche ausgelagert wurden.

Die Informationssicherheit wird leider häufig zu Beginn der Planung vernachlässigt, obwohl ihr eine zentrale Bedeutung zukommt. Dies gilt sowohl für technische als auch organisatorische Sicherheitsaspekte, denen im Outsourcing-Szenario eine entscheidende Rolle zukommt. Generell ist nämlich zu bedenken:

- Die Entscheidung zum Outsourcing ist in der Regel nicht einfach zu revidieren. Die Bindung an den Dienstleister erfolgt unter Umständen sehr langfristig.
- Ein Dienstleister hat häufig Zugriff auf Daten und IT-Ressourcen des Kunden. Der Outsourcing-Kunde verliert dadurch die alleinige und vollständige Kontrolle über Daten und Ressourcen. Je nach Outsourcing-Vorhaben betrifft dies dann auch Daten mit hohem Schutzbedarf.

- Für die technische Umsetzung des Outsourcing-Vorhabens ist es notwendig, dass zwischen Kunden und Dienstleister Daten übertragen werden. Dadurch ergibt sich automatisch ein erhöhtes Gefahrenpotential.
- In der Regel ist es erforderlich, dass Mitarbeiter oder Subunternehmer des Outsourcing-Dienstleisters (und damit Betriebsfremde) zeitweise in den Räumlichkeiten des Kunden arbeiten müssen. Auch dadurch ergibt sich ein erhöhtes Gefahrenpotential.
- Im Rahmen eines Outsourcing-Vorhabens müssen neue Prozesse und Arbeitsabläufe entworfen, eingeführt und durchgeführt werden. Die Folgen der notwendigen Umstellungen müssen geklärt und abgeschätzt werden.

- Für jeden Outsourcing-Dienstleister besteht ein nicht zu unterschätzender Interessenskonflikt: Einerseits muss er die Dienstleistung möglichst kostengünstig erbringen, um seinen Gewinn zu maximieren, andererseits erwartet der Outsourcing-Kunde hohe Dienstleistungsqualität, Flexibilität und kundenfreundliches Verhalten. Dieser Punkt ist erfahrungsgemäß der am häufigsten unterschätzte. Während IT-Manager in der Regel sehr kritisch und kostenbewusst sind und Versprechungen von Herstellern und Beratern mit großer Skepsis begegnen, ist beim Outsourcing leider oft das Gegenteil zu beobachten. Allzu leicht verfällt hier der Kunde den Werbeaussagen der Dienstleister in der frohen Erwartung, seine IT-Kosten signifikant senken zu können. Die Praxis lehrt jedoch, dass höchstens die Dienstleistungen in der Zukunft erbracht werden, die von Anfang an vertraglich fixiert worden sind. Stellt sich heraus, dass die Dienstleistungsqualität unzureichend ist, weil der Kunde Leistungen erwartet, die er – im Gegensatz zum Outsourcing-Dienstleister – als selbstverständlich erachtet, sind Nachbesserungen in der Regel ohne hohe zusätzliche Kosten nicht zu erwarten. Jeder IT-Manager, der über Outsourcing nachdenkt, sollte sich im Vorfeld die Mühe machen, nachzurechnen, zu welchen Kosten ein Dienstleister die vereinbarte Leistung erbringen muss, damit Kunde und Dienstleister beide von dem Vertragsverhältnis profitieren. Bei dieser Rechnung stellt sich vielleicht heraus, dass eine seriöse Leistungserbringung zu den versprochenen niedrigen Kosten höchst unwahrscheinlich ist.

Um die Outsourcing-Strategie festzulegen, muss daher immer eine individuelle Sicherheitsanalyse durchgeführt werden. Nur so kann letztendlich festgestellt werden, wie bestehende Geschäftsprozesse oder Informationsverbünde abgegrenzt und getrennt werden können, damit Teile davon ausgelagert werden können. In dieser frühen Projektphase wird das Sicherheitskonzept naturgemäß nur Rahmenbedingungen beschreiben und keine detaillierten Maßnahmen enthalten. Die Sicherheitsanalyse sollte nach der in der IT-Grundschutz-Vorgehensweise beschriebenen Methodik durchgeführt werden:

- Es sollte zunächst eine Strukturanalyse durchgeführt werden, um den aktuellen Ist-Zustand zu ermitteln.
- Danach erfolgt eine Schutzbedarfsfeststellung.
- Darauf aufbauend müssen geeignete Sicherheitsmaßnahmen ausgewählt und auf die jeweiligen Rahmenbedingungen des Outsourcing-Vorhabens angepasst werden. Dabei sind auch der Handlungsbedarf, die Prioritäten sowie die Kosten für die umzusetzenden Maßnahmen zu identifizieren. Die Ergebnisse können dann insbesondere in die Betrachtung der Wirtschaftlichkeit des Outsourcing-Vorhabens mit einbezogen werden.

Wenn der Schutzbedarf wichtiger Systeme oder Anwendungen hoch ist oder die Modellierung des Informationsverbunds nach IT-Grundschutz nicht möglich ist, muss eine ergänzende Sicherheitsanalyse (z. B. Risikoanalyse) durchgeführt werden. Sind die sicherheitsrelevanten Gefährdungen analysiert worden, kann festgelegt werden, ob und wie diesen begegnet werden soll.

Schlussendlich wird dennoch ein gewisses Restrisiko durch den Outsourcing-Kunden zu tragen sein. Die Ergebnisse der Sicherheitsanalyse gehen unmittelbar in die Kosten-Nutzen-Abschätzung ein.

Das Management darf bei der Entwicklung einer erfolgversprechenden, langfristigen Outsourcing-Strategie den Blick nicht nur auf die Einsparung von Kosten richten. Die Auswirkungen eines Outsourcing-Vorhabens auf die Aufgabenerfüllung, das Geschäftsmodell und das Dienstleistungs- oder Produktportfolio müssen ebenfalls berücksichtigt werden. Sollen Standardabläufe oder Kerngeschäftsprozesse ausgelagert werden? Wichtig ist in diesem Zusammenhang, dass die Fähigkeit, Anforderungen an die IT selbst zu bestimmen und zu kontrollieren, in ausreichendem Maße erhalten wird. Insbesondere an die Weiterentwicklung und Pflege selbstentwickelter IT-Systeme und Anwendungen sollte gedacht werden.

Folgende Chancen, die grundsätzlich mit einem Outsourcing-Projekt verbunden sind, können als Ziele für den Outsourcing-Kunden formuliert werden:

- Kostenvorteile: Die Reduzierung der Kosten bei der Leistungserbringung und die damit verbundene Steigerung der Produktivität stellen nach wie vor das Hauptmotiv aus Sicht von Outsourcing-Kunden dar. Kostenersparnisse können dabei z. B. durch Personaleinsparungen erzielt werden. Sowohl Löhne und Gehälter als auch Kosten für Qualifizierung und Weiterbildung entfallen auf den Outsourcing-Dienstleister. Fixe Personalkosten können so zu variablen Dienstleistungskosten umgewandelt werden, die je nach Bedarf zeitnah angepasst werden können. Auch Bedarfe an Ressourcen, wie z. B. die IT-Infrastruktur, können schnell angepasst werden, ohne dadurch das Investitionsrisiko zu erhöhen.
- Konzentration auf Kernkompetenzen: Die Auslagerung bestimmter Prozesse kann zu einer Entlastung des Managements, des IT-Betriebs oder anderen Fachbereichen führen, so dass sich diese auf ihre Kernkompetenzen konzentrieren können. Auf diese Weise werden Personalkapazitäten frei, die anderweitig eingesetzt werden können.
- Verbesserung des Sicherheitsniveaus: Im Idealfall kann durch das Outsourcing-Vorhaben ein besseres Sicherheitsniveau erreicht werden. Der Outsourcing-Dienstleister ist auf seinem Leistungsgebiet in der Regel durch einen hohen Spezialisierungsgrad gekennzeichnet. Gerade in der Informationssicherheit ist einschlägiges Know-how erforderlich, um regelmäßig die aktuellen Sicherheitshinweise, Security-Bulletins, Updatemeldungen und Bug-Reports auszuwerten, ihre Relevanz zu erkennen und bei Bedarf rasch die richtigen Schritte einzuleiten. Outsourcing-Dienstleister können zudem das Einspielen von Sicherheitspatches oder sicherheitsrelevanten Systemkonfigurationen zeitlich auf die Produktion des Outsourcing-Kunden anpassen, so dass der Betrieb durch diese Vorgänge nicht gestört wird.
- Kompetenzinseln: Interne IT-Abteilungen wachsen oft nicht im gleichen Maße wie die Organisation, für die sie zuständig sind. Ein Flickenteppich aus Workarounds und anderen provisorischen Sicherheitslösungen kann die Folge sein. Zusätzlich sind nur wenige, wenn nicht nur ein einziger Mitarbeiter in der Lage, die komplette IT-Infrastruktur zu überblicken. Fallen diese Mitarbeiter aus oder verlassen sie die Organisation des Outsourcing-Kunden, ergeben sich gravierende Sicherheitsmängel, da die Kompetenz zur Pflege der IT-Infrastruktur nicht mehr vorhanden ist. Die Outsourcing-Dienstleister können hingegen in der Regel auf mehrere gleich qualifizierte Experten zurückgreifen, die sich gegenseitig vertreten können. Zusätzlich verfügen sie über eine homogene IT-Infrastruktur, die aufgrund ihres hohen Standardisierungsgrads insbesondere aus sicherheitstechnischer Sicht leichter zu pflegen ist und eine höhere Resilienz aufweist. Hierbei ist jedoch sicherzustellen, dass der Outsourcing-Kunde weiterhin den Überblick über seine Gesamtstruktur hat.
- Nutzung von externem Know-how und Verbesserung des Leistungsangebots: Ein weiteres Outsourcing-Motiv kann die Nutzung von externem Know-how sein, ohne dies selbst vorhalten oder entwickeln zu müssen. Hierdurch ergeben sich wiederum Kosteneinsparungspotenziale. Zudem kann die Qualität der Leistungserbringung durch die Nutzung des Spezialwissens des Outsourcing-Dienstleisters gesteigert werden. Eine effizientere Prozessgestaltung und risikoarme Diversifikation kann zudem durch die Verringerung der Fertigungstiefe realisiert werden. Outsourcing-Kunden können ihre Kompetenzen auf schlanke Wertschöpfungsprozesse konzentrieren, die durch spezialisierte Outsourcing-Dienstleister unterstützt werden.Auch in diesem Zusammenhang kann die Unterstützung eines Outsourcing-Dienstleisters möglicherweise dazu beitragen, das allgemeine Sicherheitsniveau zu verbessern. Outsourcing-Dienstleister werden aufgrund ihrer Spezialisierung häufig besser geeignet sein, dynamische Sicherheitslagen auszuwerten und unmittelbar notwendige Schritte einzuleiten. Insbesondere mit Blick auf neue IT-Lösungen und die damit einhergehende steigende Komplexität kann ein spezialisierter Dienstleister nützlich sein, der die Balance zwischen Sicherheit und einem erweiterten Leistungsangebot bzw. mehr Funktionalität halten kann.
- Risikoverlagerung: Neben der bereits erwähnten Übertragung von Investitionsrisiken ist ein weiterer Vorteil die Auslagerung weiterer Risiken, z. B. Fehlverhalten von Mitarbeitern, Softwarefehler oder das Eintreten von Katastrophen. Ausfälle dieser Art treffen allerdings nicht allein den Outsourcing-Dienstleister, sondern können immer auch auf den Outsourcing-Kunden zurückfallen. Selbst bei einer vertraglich vereinbarten kompletten Übertragung der Risiken auf den Outsourcing-Dienstleister bleibt fraglich, inwiefern dieser im Haftungsfall zahlungsfähig ist. Mögliche Imageschäden hingehen treffen meist den Outsourcing-Kunden allein.

Risiken und Herausforderungen

Den Outsourcing-Zielen stehen eine Reihe vielseitiger Outsourcing-Risiken gegenüber. Diese Risiken sollten in der Outsourcing-Strategie beschrieben und in Folge dessen im Rahmen jedes Outsourcing-Projekts berücksichtigt werden. Im Folgenden werden mögliche Risiken eines Outsourcing-Vorhabens beschrieben.

- Versteckte Kosten: Ein Outsourcing-Vorhaben ist nicht nur mit Kosteneinsparungen verbunden. Die damit einhergehenden Kosten sollten im Vorhinein genau analysiert und abgewogen werden. So sind z. B. Kosten für die Steuerung des Outsourcing-Vorhabens und das Vertragsmanagement einzukalkulieren. Während einer Outsourcing-Beziehung kommt es auf der Seite des Outsourcing-Kunden möglicherweise zu unerwarteten Kommunikations- und Koordinationskosten.Wurde zu Beginn des Outsourcing-Vorhabens ein zu geringer Leistungsumfang definiert, werden im Laufe der Vertragsbeziehung eventuelle Anpassungen notwendig. Solche Vertragsänderungen können teilweise erhebliche Zusatzkosten nach sich ziehen.Zudem können einmalige Kosten entstehen. Hierzu zählen beispielsweise Abfindungen oder Kosten für Neueinstellungen, die im Zuge personeller Umstrukturierungen anfallen.
- Verlust von Know-how: Die Vorteile durch die Nutzung externen Know-hows bringen auch Risiken mit sich. So bewirkt die dauerhafte Nutzung des Fachwissens von Dritten in der Regel nach und nach den Verlust des eigenen Know-hows. Die Mitarbeiter des Outsourcing-Kunden geben ihr Fachwissen im Zuge eines Outsourcing-Projekts oftmals ab oder auf bzw. erhalten dieses nicht weiter aufrecht. Die Kompetenz für die ausgelagerten Funktionen liegt letztendlich nicht mehr in den Händen des Outsourcing-Kunden.Besonders kritisch ist eine solche Situation, wenn das Know-how der Mitarbeiter des Outsourcing-Dienstleisters nicht mehr angemessen ist und somit gravierende Sicherheitslücken entstehen, diese jedoch nicht entdeckt werden können, weil das benötigte Fachwissen beim Outsourcing-Kunden nicht mehr vorhanden ist. Der Verlust des eigenen Know-hows steigert demnach zwangsläufig die Abhängigkeit von dem Outsourcing-Dienstleisters.
- Abhängigkeit vom Outsourcing-Dienstleister: Die Abhängigkeit des Outsourcing-Kunden vom Outsourcing-Dienstleister steigt insbesondere mit der Komplexität des ausgelagerten Prozesses und mit der Dauer der Outsourcing-Beziehung. Für den Outsourcing-Kunden besteht stets das Risiko einer Preisanhebung durch den Outsourcing-Dienstleister, nachdem das Outsourcing-Vorhaben weit fortgeschritten ist und eine Rückintegration nicht wirtschaftlich oder zu risikobehaftet wäre. Infolgedessen müssen die Kostenerhöhungen häufig akzeptiert werden, wodurch die Wirtschaftlichkeit des Outsourcing-Vorhabens im Nachhinein stark beeinflusst werden kann. Die dadurch notwendig gewordenen Kosteneinsparungen führen wiederum oftmals zu Einsparungen im Sicherheitsbereich und haben entsprechende Auswirkungen auf das Sicherheitsniveau.
- Ansehens- und Vertrauensverlust: Die aus Leistungsdefiziten des Outsourcing-Dienstleisters resultierenden Auswirkungen auf Outsourcing-Kunden können zu weitreichenden Konsequenzen führen. Entsprechende Folgen, wie z. B. ein Ansehens- oder Vertrauensverlust, treffen den Outsourcing-Kunden selbst, ganz gleich, ob die Schuld ursprünglich bei dem Outsourcing-Dienstleister liegt.
- Verlust von Kontroll- und Steuerungsmöglichkeiten: Der Outsourcing-Kunde besitzt gegenüber dem Outsourcing-Dienstleister in der Regel nur eingeschränkte Befugnisse in Bezug auf Anordnungen. Daraus resultieren eingeschränkte Steuerungsmöglichkeiten und ein erhöhter Abstimmungsbedarf im Vergleich mit einer Eigenerbringung. Auch die Kontrollmöglichkeiten des Outsourcing-Kunden sind eingeschränkt. Trotz vereinbarter Zugangsrechte wird der Outsourcing-Kunde nicht über alle Informationen hinsichtlich Organisation und Abläufe des Outsourcing-Dienstleisters verfügen.
- Einblicke Dritter in interne Betriebsabläufe und Daten: In Abhängigkeit von der Art des Outsourcing-Vorhabens kann der Outsourcing-Dienstleister Informationen über interne Betriebsabläufe und möglicherweise auch über Geschäftsverbindungen des Outsourcing-Kunden erhalten. So ist für letzteren eine alleinige Kontrolle über diese Informationen nicht mehr sichergestellt. Zudem ist es eventuell notwendig, dass die Mitarbeiter des Outsourcing-Dienstleisters zumindest vorübergehend in den Räumlichkeiten der Outsourcing-Kunden arbeiten, wodurch ihnen der Zugang zu Daten und Ressourcen erleichtert wird. Handelt es sich bei einer Offenlegung von Informationen um personenbezogene Daten, sind zusätzlich die einschlägigen Datenschutz-Gesetze zu beachten.
- Risiken für die Sicherheit der Daten: Die Sicherheit der Daten ist ein wesentlicher Aspekt im Rahmen einer Auslagerung. Besonders Risiken, die aus dem Verlust der Verfügbarkeit von Systemen und Daten resultieren, z. B. bei einem Systemausfall einer IT-Auslagerung, sind zu betrachten. Generell wird bei Einbeziehung eines Outsourcing-Dienstleisters die Anzahl der Übertragungswege und somit auch das Gefahrenpotenzial erhöht. Typische Bedrohungen sind Hacker-Angriffe, Schadprogramme, Ausfälle aufgrund technischen Versagens bei der Soft- und Hardware und weitere Schadensszenarien, z. B. durch Strom- oder Klimaanlagenausfälle. Die IT-Risiken des Dienstleisters wirken sich direkt auf den Outsourcing-Kunden aus. Schon kleinere bzw. Teilausfälle führen zu inkonsistenter oder fehlerhafter Datenverarbeitung.

Beschreibung der Vorgehensweise im Rahmen des Outsourcing-Projekts

Nachdem die Outsourcing-Ziele sowie die zu berücksichtigenden Outsourcing-Risiken in der Outsourcing-Strategie dargelegt wurden, sollte eine strukturierte Vorgehensweise für das Management eines Outsourcing-Vorhabens skizziert werden. Ausführliche Vorgaben zur Durchführung können in nachgelagerten Dokumenten (z. B. einer Rahmenanweisung für das Outsourcing) beschrieben werden. Mittels der beschriebenen Vorgehensweise sollen die Outsourcing-Risiken behandelt und somit die Erreichung der gesetzten Ziele gewährleistet werden. Im Rahmen der beschriebenen Vorgehensweise sollten die folgenden Phasen des Outsourcing-Vorhabens berücksichtigt werden:

- Selektion möglicher Outsourcing-Bereiche: Welche Prozesse und/oder Aktivitäten dürfen aufgrund gesetzlicher Vorgaben oder aus strategischen Gründen (Kernkompetenzen) nicht ausgelagert werden? Zudem ist im Rahmen dieser Phase eine Kosten-Nutzen-Analyse durchzuführen, auf deren Grundlage die Wirtschaftlichkeit des geplanten Outsourcing-Vorhabens beurteilt werden kann.
- Erfassung und Beurteilung des Outsourcing-Sachverhalts: Welche individuellen Risiken bestehen für den betrachteten Sachverhalt, wie ist diesen zu begegnen bzw. welche Anforderungen sind aufgrund dessen an einen potenziellen Outsourcing-Dienstleister zu stellen?
- Auswahl eines passenden Outsourcing-Dienstleisters: Die Auswahl sollte aufgrund der zuvor ermittelten Risiken und der daraus abgeleiteten (Sicherheits-)Anforderungen getroffen werden.
- Vertragsgestaltung: Welche Aspekte sind vertraglich zu regeln?
- Überführung in den Regelbetrieb: Welche (Sicherheits-)Maßnahmen sind im Zuge der Übertragung der Leistungserbringung auf den Outsourcing-Dienstleister zu ergreifen?
- Regelbetrieb und Beendigung: Welche Steuerungs-, Überwachungs-, Kontroll- und Abstimmungsmaßnahmen sind im laufenden Betrieb zu ergreifen und welche Vorsorgemaßnahmen sind für eine erwartete bzw. unerwartete Beendigung des Outsourcing-Vorhabens zu treffen?

OPS.2.1.M6 Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben

Für jedes Outsourcing-Vorhaben muss ein Sicherheitskonzept existieren, das auf den Sicherheitsanforderungen des Outsourcing-Kunden basiert (OPS.2.1.M1 Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben).

Das Gesamt-Sicherheitskonzept sollte nach Beauftragung eines Outsourcing-Dienstleisters erstellt werden. Outsourcing-Projekte sind dadurch gekennzeichnet, dass sich viele technische und organisatorische Details erst im Laufe der Planung und bei Migration der Systeme ergeben. Das Sicherheitskonzept wird daher in den wenigsten Fällen von Beginn an vollständig und endgültig sein und muss während der Migrations- und der Betriebsphase von allen Beteiligten stetig weiterentwickelt und konkretisiert werden. Spezielle Anforderungen an das Sicherheitskonzept für die Migrationsphase (als Teil des Gesamt-Sicherheitskonzepts) sind in OPS.2.1.M13 Sichere Migration bei Outsourcing-Vorhaben beschrieben.

Generell unterscheiden sich Sicherheitskonzepte für Outsourcing-Vorhaben nur wenig von Sicherheitskonzepten für selbst betriebene IT-Systeme. Zu berücksichtigen ist jedoch, dass bei einem Outsourcing-Vorhaben weitere Parteien involviert sein können. Dies können neben dem Outsourcing-Dienstleister beispielsweise Netzprovider und Unterauftragnehmer des Dienstleisters sein. Auch durch diese dürfen die vereinbarten Sicherheitsziele nicht beeinträchtigt werden. Die erforderlichen Sicherheitsanforderungen für deren Aufgabengebiete müssen entweder im Sicherheitskonzept des Dienstleisters integriert oder in eigenständigen Sicherheitskonzepten beschrieben sein, die dem Outsourcing-Kunden vorzulegen sind.

Jede am Outsourcing-Vorhaben beteiligte Partei muss ein eigenes Sicherheitskonzept erstellen und umsetzen, welches auch das spezielle Outsourcing-Vorhaben umfasst. Damit sind Sicherheitskonzepte erforderlich:

- für den Einflussbereich des Outsourcing-Kunden,
- für den Einflussbereich des Outsourcing-Dienstleisters sowie
- für die Schnittstellen und die Kommunikation zwischen diesen Bereichen.

Der Outsourcing-Kunde sollte hierauf aufbauend ein Sicherheitskonzept für das Gesamtsystem erstellen, welches die Sicherheit im Zusammenspiel der Einzelsysteme betrachtet.

Die verschiedenen Teil-Konzepte müssen zwischen Outsourcing-Kunden und Outsourcing-Dienstleister abgestimmt werden. Dabei ist der Outsourcing-Kunde am Sicherheitskonzept des Outsourcing-Dienstleisters nicht direkt beteiligt, sollte aber in einem Audit prüfen, ob es vorhanden und ausreichend ist. Für das Audit kann der Outsourcing-Kunde dabei auch auf externe Dritte zurückgreifen. Im Verlauf des Vorhabens sollten alle Teil-Konzepte kontinuierlich auf Aktualität und Korrektheit geprüft werden.

Das Gesamt-Sicherheitskonzept sollte alle relevanten Risiken berücksichtigen, die mit dem Outsourcing-Vorhaben einhergehen. Mögliche Risiken werden in OPS.2.1.M5 Festlegung einer Outsourcing-Strategie beschrieben.

Die in OPS.2.1.M1 Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben und OPS.2.1.M4 Vertragsgestaltung mit dem Outsourcing-Dienstleister genannten Sicherheitsanforderungen bilden die Basis für das Gesamt-Sicherheitskonzept. Aufbauend auf den dort beschriebenen grundlegenden Anforderungen muss im Sicherheitskonzept die detaillierte Ausgestaltung erfolgen, wobei beispielsweise die Maßnahmen konkretisiert und Ansprechpartner namentlich festgelegt werden.

Erfahrungsgemäß ist der Übergang (Migration) von Aufgaben und IT-Systemen vom Kunden zum Outsourcing-Dienstleister eine Projektphase, in der verstärkt mit Sicherheitsvorfällen zu rechnen ist. Aus diesem Grund müssen im Sicherheitskonzept Regelungen und Maßnahmen zur Migration behandelt werden, die in OPS.2.1.M13 Sichere Migration bei Outsourcing-Vorhaben genauer behandelt werden.

Im Folgenden sind einige Aspekte und Themen aufgelistet, die im Sicherheitskonzept im Detail beschrieben werden sollten. Da die Details eines Sicherheitskonzeptes direkt vom Outsourcing-Vorhaben abhängen, ist die Liste als Anregung zu verstehen und erhebt keinen Anspruch auf Vollständigkeit. Neben einem Überblick über die Gefährdungslage, die der Motivation der Sicherheitsmaßnahmen dient, und den infrastrukturellen und personellen Sicherheitsmaßnahmen können Maßnahmen aus folgenden Bereichen sinnvoll sein:

Organisation

- Umgang mit Daten und schützenswerten Betriebsmitteln wie Druckerpapier und Speichermedien, insbesondere Regelungen zum Anfertigen von Kopien und Löschen/Vernichten
- Festlegung von Aktionen, für die das "Vier-Augen-Prinzip" anzuwenden ist
- Vertretungsregelungen

Hard-/Software

- Einsatz gehärteter Betriebssysteme, um Angriffe möglichst zu erschweren
- Einsatz von Intrusion-Detection-Systemen (IDS), um Angriffe frühzeitig zu erkennen
- Einsatz von Prüfungssystemen für Datei-Integrität, um Veränderungen z. B. nach erfolgreichen Angriffen zu erkennen
- Einsatz von Syslog- und Timeservern, um eine möglichst umfassende Protokollierung zu ermöglichen
- Einsatz kaskadierter Firewall-Systeme zur Erhöhung des Perimeterschutzes auf Seiten des Dienstleisters
- sorgfältige Vergabe von Benutzer-Kennungen, Verbot von Gruppen-IDs für Personal des Dienstleisters

Kommunikation

- Absicherung der Kommunikation (z. B. durch Verschlüsselung, elektronische Signatur) zwischen Dienstleister und Kunde, um sensitive Daten zu schützen
- Authentisierungsmechanismen
- Detailregelungen für weitere Netzanbindungen
- Detailregelungen für den Datenaustausch

Kontrollen und QS

- Detailregelungen (z. B. unangekündigte Kontrollen vor Ort, Zeitintervalle, Zuständigkeiten, Detailgrad) für Kontrollen und Messung von Sicherheit, Dienstqualität, Abläufen und organisatorische Regelungen

Notfallvorsorge

- Outsourcing-Kunden und -Dienstleister müssen aufeinander abgestimmte Notfallkonzepte haben, siehe auch OPS.2.1.M14 Kontrolle der Notfallvorsorge beim Outsourcing.

OPS.2.1.M7 Festlegung der möglichen Kommunikationspartner

Im Rahmen eines Outsourcing-Vorhabens werden vom Outsourcing-Kunden viele Informationen zu externen Kommunikationspartnern übertragen. Hierbei muss sichergestellt werden, dass die jeweiligen Empfänger die notwendigen Berechtigungen zum Weiterverarbeiten dieser Informationen besitzen. Werden Informationen zwischen mehreren kommunizierenden Stellen ausgetauscht, sollte für alle Beteiligten ersichtlich sein, wer diese Informationen ebenfalls erhalten hat beziehungsweise erhalten wird.

Um die oben genannten Kriterien zu erfüllen, muss festgelegt werden, welche Kommunikationspartner welche Informationen erhalten dürfen, sowohl aufseiten des Outsourcing-Kunden als auch aufseiten des Outsourcing-Dienstleisters sowie für alle weiteren Beteiligten. Hierfür ist es erforderlich, dass alle Informationen entsprechend ihrer strategischen Bedeutung für die auslagernde Institution klassifiziert sind (OPS.2.1 M1 Festlegung der Sicherheitsanforderungen für Outsourcing?Vorhaben).

Die Empfänger sind darauf hinzuweisen, dass die übermittelten Daten nur zu dem Zweck benutzt werden dürfen, zu dem sie weitergegeben wurden. Auch aus Datenschutzgründen (siehe z. B. BDSG, Weitergabekontrolle) sollte eine Übersicht erstellt werden, welche Empfänger berechtigt sind, Informationen, insbesondere personenbezogene Daten, per Datenübertragung oder Datenträgeraustausch zu erhalten. Diese Übersicht muss aktuell und korrekt sein.

Zu diesem Zweck sind den Verantwortlichkeiten bestimmte Rollen zuzuweisen, die diese Aufgaben übernehmen und die Einhaltung der getroffenen Regelungen regelmäßig aufseiten des Outsoucing-Kunden wie auch des Outsourcing-Dienstleisters überprüfen.

OPS.2.1.M8 Regelungen für den Einsatz des Personals des Outsourcing-Dienstleiters

Im Rahmen von Outsourcing-Projekten werden die Mitarbeiter des Outsourcing-Dienstleisters eventuell auch in Räumlichkeiten des Outsourcing-Kunden eingesetzt. Dies kann auf Dauer dazu führen, dass die Mitarbeiter des Outsourcing-Kunden nicht immer genau wissen, ob es sich um eigene oder externe Mitarbeiter handelt.

Personal des Outsourcing-Dienstleisters, das über einen längeren Zeitraum innerhalb der Räumlichkeiten des Outsourcing-Kunden tätig sind und eventuell Zugang zu vertraulichen Unterlagen und Daten bekommen, sind schriftlich auf die Einhaltung der geltenden einschlägigen Gesetze, Vorschriften und internen Regelungen zu verpflichten.

Weiterhin sollte sichergestellt werden, dass die Mitarbeiter des Outsourcing-Dienstleisters – ähnlich wie eigene Mitarbeiter – in ihre Aufgaben eingewiesen werden. Soweit es zur Erfüllung ihrer Aufgaben und Verpflichtungen erforderlich ist, sind sie über hausinterne Regelungen und Vorschriften zur Informationssicherheit sowie die institutionsweite Sicherheitsvorgaben zu unterrichten. Dies gilt in besonderem Maß, wenn sie in den Räumlichkeiten des Outsourcing-Kunden arbeiten.

Zudem sollte sichergestellt sein, dass auch für die Mitarbeiter des Outsourcing-Dienstleisters angemessene Vertretungsregelungen existieren. Auch die jeweiligen Vertreter müssen ordnungsgemäß eingewiesen und auf die Einhaltung der geltenden Gesetze, Vorschriften und internen Regelungen verpflichtet werden.

Außerdem muss geregelt sein, wie mit Personalveränderungen beim Outsourcing-Dienstleister umgegangen wird. Diese müssen dem Outsourcing-Kunden rechtzeitig mitgeteilt werden.

Bei Beendigung des Outsourcing-Verhältnisses muss eine geregelte Übergabe der Arbeitsergebnisse und der erhaltenen Unterlagen und Betriebsmittel erfolgen. Den Mitarbeitern des Outsourcing-Dienstleisters sind zudem sämtliche Zugangsberechtigungen und Zugriffsrechte zu entziehen.

Sollten Mitarbeiter des Outsourcing-Dienstleister lediglich kurzfristig oder einmalig vor Ort eingesetzt werden, sollten diese wie Besucher behandelt werden und sich dementsprechend beispielsweise nur in Begleitung von Mitarbeitern des Outsourcing-Kunden in dessen Räumlichkeiten aufhalten dürfen.

OPS.2.1.M9 Vereinbarung über die Anbindung an Netze der Outsourcing-Partner

Vor der Anbindung des Netzes des Outsourcing-Kunden an das Netz des Outsourcing-Dienstleisters sollte eine detaillierte Vereinbarung (Data Connection Agreement, DCA) geschlossen werden. In dieser muss genau definiert sein, wer Zugriff auf das Netz des Outsourcing-Kunden erhält und unter welchen Bedingungen dies geschehen soll. Analog muss geregelt sein, wer aus dem Netz des Outsourcing-Kunden mit welchen Zugriffsrechten und zu welchen Bedingungen Zugriff auf das Netz des Outsourcing-Dienstleisters erhalten soll. Eine solche Vereinbarung sollte folgende Bestandteile umfassen:

- Eine Beschreibung dessen, was die Vereinbarung insgesamt umfasst, inklusive einer Beschreibung der betroffenen Informationsverbünde
- Eine Abstimmung über den jeweiligen Schutzbedarf und die Klassifikation von Daten (es muss ein gemeinsames Verständnis erzielt werden)
- Eine Festlegung der Verantwortlichen (Wer trägt die Verantwortung für die Einhaltung der Vertragsbedingungen?)
- Die Benennung von Ansprechpartnern sowohl für organisatorische als auch technische Probleme und insbesondere für sicherheitsrelevante Ereignisse
- Die erforderlichen Informationen zur Klassifizierung organisatorischer und technischer Probleme als solche sowie sicherheitsrelevanter Ereignisse
- Informationen und Festlegungen zur netzinternen Verschlüsselung
- Welche Dienste (z. B. SSH, HTTPS) zur Verfügung gestellt werden und welche nicht
- Welche IT-Plattformen, Anwendungen und Datenformate eingesetzt werden
- Ob sich aus der Netzanbindung Anforderungen an die Verfügbarkeit von Netz- oder IT-Komponenten beim jeweiligen Partner ergeben (Performance, maximale Ausfallrate)
- Wer was protokollieren darf bzw. muss, wo die Protokolldaten abgelegt werden und wer auf die Protokolldaten zugreifen darf (dies kann insbesondere in Notsituationen wichtig sein)
- Inwieweit ein regelmäßiger Austausch von Protokolldaten erfolgen soll
- Welche Sicherheitsmaßnahmen gewährleistet werden müssen und wie deren Einhaltung überprüft wird
- Eine Vertraulichkeitsvereinbarung (Non-Disclosure Agreement), d. h. eine Vereinbarung darüber, dass Informationen, die einer der Beteiligten im Rahmen der Zusammenarbeit erhalten hat, nicht an Außenstehende weitergegeben werden
- Eine Haftungs- bzw. Schadensersatzregelung (hierin sollten unter anderem die Bedingungen für die Trennung der Netzanbindung, Haftung bei Schadprogrammen oder Hackerangriffen, Vertragsstrafen bei nicht erfüllter Leistung bzw. Haftungsübernahme bei Inanspruchnahme für fremde Inhalte geklärt sein)
- Eine Regelung über Auskunftspflichten bei aufgetretenen Sicherheitslücken
- Eine Festlegung, welche Daten zu welchen Zwecken genutzt werden dürfen (z. B. bei der Weiterverwendung von Arbeitsergebnissen)
- Eine Beschreibung, inwieweit weitere Vertragspartner in die Vereinbarung eingebunden werden, z. B. durch gemeinsame Nutzung von Applikationen oder als Dienstleister für einen der Vertragspartner
- Die Laufzeit sowie Anpassungsmöglichkeiten der Vereinbarung (Technik entwickelt sich schnell weiter, d. h. auch die Vereinbarungen über deren Nutzung müssen ständig angepasst werden)

Die Vereinbarung sollte durch jene Personen abgeschlossen werden, welche die Verantwortung für die Einhaltung der Vereinbarungen tragen. Dafür ist zunächst zu klären, wer die Verantwortung für die Netzanbindung tragen sollte, da hier üblicherweise unterschiedliche Bereiche einer Institution involviert sind. Sinnvollerweise sollte hierzu ein Team gebildet werden, zu dem zumindest der Informationssicherheitsbeauftragte, der IT-Leiter, die Fachverantwortlichen der betroffenen Bereiche und der Datenschutzbeauftragte gehören. Bei kritischen Entscheidungen sollten alle genannten Personen beteiligt werden, da sich deren Interessen erfahrungsgemäß stark voneinander unterscheiden können.

Bevor eine Netzanbindung aktiviert wird, sollten alle Sicherheitsmängel auf beiden Seiten ausgeräumt worden sein. Hier sollte auch ein Weg gefunden werden, wie sich der Outsourcing-Kunden von dem Sicherheitsniveau des Outsourcing-Dienstleisters oder sonstiger Dritter überzeugen kann, beispielsweise durch Basis-Sicherheitschecks oder Stichproben vor Ort. Auf keinen Fall darf die Beseitigung von Sicherheitslücken in den Echtbetrieb verschoben werden, da dies erfahrungsgemäß niedriger priorisiert wird als reine Probleme in Bezug auf die Verfügbarkeit.

Dem Outsourcing-Dienstleister sollten nur die Dienste zur Verfügung gestellt werden, die vertraglich vereinbart wurden und unbedingt erforderlich sind. Bei ausländischen Outsourcing-Dienstleistern müssen unbedingt deren nationale Gesetze berücksichtigt werden, z. B. in den Bereichen Kryptographie, Datenschutz und Urheberrecht.

Falls durch die Netzanbindung Sicherheitsvorfälle auftreten, muss klar definiert sein, wer wann die Verbindung trennen darf, wer darüber zu informieren ist und welche Eskalationsschritte vorzusehen sind.

OPS.2.1.M10 Vereinbarung über Datenaustausch zwischen den Outsourcing-Partnern

Datenaustausch zwischen dem Outsourcing-Kunden und dem Outsourcing-Dienstleister kann über verschiedene Wege erfolgen, neben Netzanbindung (siehe OPS.2.1.M9 Vereinbarung über die Anbindung an Netze Dritter) z. B. über Datenträgeraustausch oder per E-Mail. Neben den Sicherheitsmaßnahmen, die bereits beim sporadischen Datenaustausch zu beachten sind, sollten bei einem regelmäßigen Datenaustausch mit festen Kommunikationspartnern Vereinbarungen getroffen werden, um diesen möglichst reibungslos zu gestalten. Eine solche Vereinbarung sollte folgende Bestandteile umfassen:

- Benennung von Ansprechpartnern sowohl für organisatorische als auch für technische Probleme und insbesondere für sicherheitsrelevante Ereignisse
- die erforderlichen technischen Informationen, also Festlegungen darüber
  - welche Anwendungen und Datenformate unterstützt werden
  - welche Verfügbarkeit zu gewährleisten ist, also wie häufig beispielsweise E-Mails zu lesen und wie schnell sie zu beantworten sind
- welche Sicherheitsmaßnahmen beim Datenaustausch gewährleistet werden müssen, also z. B.
  - dass die Daten vor und nach dem Austausch auf Schadsoftware zu überprüfen sind
  - wie die Daten vor Transportschäden und unbefugtem Zugriff zu schützen sind (verschlossene Behältnisse, Checksummen, Verschlüsselung)
  - wie das Schlüsselmanagement geregelt ist
  - dass die Daten auf der Senderseite frühestens nach Bestätigung des korrekten Empfangs gelöscht werden dürfen, falls eine Löschung erforderlich ist
- eine Vertraulichkeitsvereinbarung
- eine Festlegung, welche Daten zu welchen Zwecken genutzt werden dürfen (z. B. bei der Weiterverwendung von Arbeitsergebnissen)
- eine Verpflichtung auf die Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen, also z. B. Datenschutz- und Urheberrechtsgesetze bzw. LizenzregelungenWeitere Punkte, die in eine solche Vereinbarung aufgenommen werden sollten, finden sich in Baustein OPS.1.2.3 Datenträgertausch und Baustein APP.1 E-Mail/Groupware/Kommunikation.

OPS.2.1.M11 Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb

Nachdem die Übertragung der Leistungserbringung auf den Outsourcing-Dienstleister erfolgt ist, muss die Informationssicherheit auch im laufenden Betrieb gewährleistet werden. Dabei unterscheiden sich die IT-bezogenen Einzelaufgaben generell nicht von denen, die zu planen und durchzuführen sind, wenn kein Outsourcing betrieben wird. Besonderheiten ergeben sich jedoch dadurch, dass die Aufgaben auf mehrere Parteien verteilt und daher zusätzliche Abstimmungs- und Kontrollmaßnahmen erforderlich sind. Im Rahmen dessen sind folgende Aspekte zu berücksichtigen:

- Dokumentationen und Richtlinien müssen regelmäßig aktualisiert werden.
- Die geltenden Sicherheitskonzepte aller Beteiligten müssen daraufhin geprüft werden, ob sie noch aufeinander abgestimmt sind und das gewünschte Sicherheitsniveau gewährleisten. Insbesondere sollte der Outsourcing-Dienstleister den Outsourcing-Kunden über wichtige Änderungen in seinem Einflussbereich informieren.
- Das Mandantenkonzept des Outsourcing-Dienstleisters sollte überprüft werden, ob es den Sicherheitsanforderungen des Kunden genügt.

- Regelmäßige Kontrollen zu folgenden Aspekten sind durchzuführen:
  - Durchführung der vereinbarten Audits
  - Umsetzungsstand der vereinbarten Sicherheitsmaßnahmen
  - Wartungszustand von Systemen und Anwendungen
  - Rechtezuweisung durch den Outsourcing-Dienstleister (Missbrauch von Rechten)
  - Einsatz von Mitarbeitern, die dem Outsourcing-Kunden nicht gemeldet wurden (z. B. bei Vertretungen)
  - Einhaltung der Anforderungen in Hinsicht auf Performance, Verfügbarkeit, Qualitätsniveau
  - Einhaltung der Anforderungen im Rahmen der Datensicherung
- Regelmäßige Abstimmungsrunden zu folgenden Punkten sind abzuhalten:
  - Informationsaustausch (z. B. Personalnachrichten, organisatorische Regelungen, Gesetzesänderungen, geplante Projekte, vorgesehene Tests und Systemänderungen, die zu Beeinträchtigungen der Dienstleistungsqualität führen können)
  - Informationen über Sicherheitsrisiken und den Umgang damit
  - Identifikation und Analyse von Problemen
  - gegenseitiges Feedback und Identifizierung von Verbesserungspotenzialen
  - Änderungsmanagement: Änderungswünsche (Hardware, Software, Ausweitung des Dienstleistungsportfolios, gestiegener Ressourcenbedarf etc.) sollten frühzeitig besprochen werden
- Es sollten regelmäßige Übungen und Tests zu folgenden Themen durchgeführt werden:
  - Reaktion auf Systemausfälle (Teilausfall, Totalausfall)
  - Wiedereinspielen von Datensicherungen
  - Beherrschung von Sicherheitsvorfällen

OPS.2.1.M12 Änderungsmanagement [IT-Betrieb, Änderungsmanager]

Bei der Komplexität heutiger IT-Systeme können bereits kleine Änderungen an laufenden Systemen zu Sicherheitsproblemen führen, z. B. durch unerwartetes Systemverhalten oder Systemausfälle.

In Bezug auf Informationssicherheit ist es Aufgabe des Änderungsmanagements, neue Sicherheitsanforderungen zu erkennen, die sich aus Änderungen an IT-Systemen ergeben. Sind signifikante Hardware- oder Software-Änderungen an einem IT-System geplant, sind die Auswirkungen auf die Sicherheit des Gesamtsystems zu untersuchen. Änderungen an einem IT-System dürfen nicht zu einer Verringerung der Effizienz einzelner Sicherheitsmaßnahmen und damit zu einer Gefährdung der Gesamtsicherheit führen.

Änderungen, die während eines Outsourcing-Vorhabens auf Seiten des Outsourcing-Dienstleisters vorgenommen werden, sind ebenso durch das Änderungsmanagement des Outsourcing-Kunden zu betrachten. Daher sollte mit dem Outsourcing-Dienstleister vertraglich geregelt werden, dass Sicherheitsaspekte bei der Planung und Durchführung von Änderungen an IT-Komponenten, Software oder Konfigurationsdaten berücksichtigt werden. Alle Änderungen an IT-Komponenten, Software oder Konfigurationsdaten sollten vom Outsourcing-Dienstleister geplant, getestet, genehmigt und dokumentiert werden. Vom Outsourcing-Dienstleister ist dafür Sorge zu tragen, dass auf alle sicherheitsrelevanten Änderungen angemessen reagiert wird. Dazu gehören zum Beispiel:

- Änderungen an IT-Systemen (neue Applikationen, neue Hardware, neue Netzverbindungen, Modifikationen an der eingesetzten Software, Einspielen von Sicherheitspatches, Aufrüstung der Hardware usw.)
- Änderungen in der Aufgabenstellung oder in der Wichtigkeit der Aufgabe für den Outsourcing-Kunden
- Änderungen in der Benutzerstruktur (neue, etwa externe oder anonyme Benutzergruppen)
- räumliche Änderungen, z. B. nach einem Umzug

Bevor Änderungen genehmigt und durchgeführt werden, muss durch Prüfung und Test der geplanten Aktionen sichergestellt werden, dass das Sicherheitsniveau während und nach der Änderung erhalten bleibt. Wenn Risiken, insbesondere für die Verfügbarkeit, nicht ausgeschlossen werden können, muss die Planung auch eine Rückfalllösung vorsehen und Kriterien vorgeben, wann diese zum Tragen kommen soll.

Alle Änderungen und die dazugehörigen Entscheidungsgrundlagen sind zu dokumentieren. Dies gilt sowohl in der Betriebs- als auch in einer Testumgebung.

Beim Änderungsmanagement ist das Berechtigungskonzept zur Durchführung von Änderungen ein wichtiger Punkt:

- Nur diejenigen, die Änderungen durchführen dürfen, sollten Zugriffsberechtigungen auf die dafür relevanten Systembereiche haben.
- Es sollte Mechanismen geben, die sicherstellen, dass alle wesentlichen Änderungen vorher abgestimmt wurden.

Hinweis: Bei der Durchführung von Änderungen sollte immer beachtet werden, dass Änderungen eines IT-Systems oder seiner Einsatzbedingungen

- Änderungen in der Umsetzung einzelner Sicherheitsmaßnahmen,
- die Erstellung eines neuen Sicherheitskonzepts oder
- die Überarbeitung der institutionsweiten Leitlinie zur Informationssicherheit erforderlich machen können.
- Bei größeren Änderungen sollte vereinbart werden, dass das Informationssicherheitsmanagement des Outsourcing-Kunden vom Outsourcing-Dienstleister schon im Vorfeld involviert werden muss. Eine Rückfalllösung sollte gemeinsam erarbeitet werden.

OPS.2.1.M13 Sichere Migration bei Outsourcing-Vorhaben

Nach Beauftragung des Outsourcing-Dienstleisters muss zunächst ein vorläufiges Sicherheitskonzept für die Migrationsphase entwickelt werden, in dem auch die Test- und Einführungsphase als Teilaspekt des Outsourcing-Vorhabens betrachtet wird (siehe OPS.2.1 M6 Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben). Zum einen sind in dieser Phase zahlreiche Betriebsfremde involviert, zum anderen müssen Abläufe etabliert, Aufgaben übertragen und Systeme neu eingerichtet bzw. angepasst werden. Ein sorgfältiger Testbetrieb ist deshalb überaus wichtig. Besonders zu Testzwecken und in Phasen großer Arbeitsbelastung werden gerne "flexible" und "unkomplizierte" Lösungen gewählt, die selten sehr sicher sind. Es ist daher beispielsweise sicherzustellen, dass produktive Daten nicht ohne besonderen Schutz als Testdaten verwendet werden. Dies muss durch das Sicherheitskonzept ausgeschlossen werden.

Vor der Erstellung eines Migrationskonzepts als Teil des Sicherheitskonzepts für ein Outsourcing-Vorhaben sollte ein Informationssicherheitsmanagement-Team speziell für die Migrationsphase beim Outsourcing-Kunden eingerichtet werden. Dieses muss während der Migrationsphase auf Sicherheitsbelange achten und durch geeignete Maßnahmen auch schon vor der Migration dafür sorgen, dass ein sicherer IT-Betrieb während der Migration gewährleistet ist. Die Größe des Informationssicherheitsmanagement-Teams hängt dabei von Art und Größe des Outsourcing-Vorhabens ab, als Minimum kann es aus einem Sicherheitsexperten von jedem Outsourcing-Partner bestehen.

Dem Informationssicherheitsmanagement-Team kommen dabei folgende Aufgaben zu, aus denen sich Regelungen und Vorgaben ableiten, die im Migrationskonzept zu erfassen sind:

- Es ist ein gemischtes Team aus Mitarbeitern des Outsourcing-Kunden und des Outsourcing-Dienstleisters zu bilden. Dieses kann auch durch externe Experten verstärkt werden, um spezielles Know-how verfügbar zu machen.
- Für die Migrationsphase muss eine Informationssicherheitskonzeption erstellt werden.
- Die Verantwortlichkeiten und Hierarchien für die Migrationsphase sind festzulegen. Dabei ist es wichtig, dass klare Führungsstrukturen geschaffen und auf beiden Seiten eindeutige Ansprechpartner definiert werden. Zusätzlich ist darauf zu achten, dass auf beiden Seiten Verantwortlichkeiten auch auf hohen Ebenen definiert werden. Nur so kann sichergestellt werden, dass im Zweifelsfall mit entsprechendem Nachdruck gehandelt werden kann.
- Die erforderlichen Tests müssen geplant und durchgeführt, Abnahmeprozeduren erarbeitet und die Inbetriebnahme der Dienstleistung geplant werden.
- Es sind geeignete Mitarbeiter auf beiden Seiten der Outsourcing-Partner für die Test- und Einführungsphase und für den späteren Betrieb auszuwählen. Vertraglich kann sich ein Outsourcing-Kunden natürlich auch ein Mitspracherecht bei der Personalauswahl des Outsourcing-Dienstleisters einräumen lassen.
- Die Mitarbeiter des Outsourcing-Kunden sind zum Verhalten während und nach der Migrationsphase zu schulen. In der Regel sind die Mitarbeiter dabei mit neuen und unbekannten Ansprechpartnern konfrontiert. Dies birgt die Gefahr des Social Engineerings (z. B. Anruf eines vermeintlichen Mitarbeiters des Sicherheitsteams des Outsourcing-Dienstleisters).
- Der Outsourcing-Dienstleister muss die relevanten Abläufe, Applikationen und IT-Systeme des Outsourcing-Kunden genau kennenlernen und dahingehend eingewiesen werden.
- Der störungsfreie Betrieb ist durch genaue Ressourcenplanung und Tests sicherzustellen. Die produktiven Systeme dürfen dabei nicht vernachlässigt werden. Dazu ist im Vorfeld zu überprüfen, ob die vorgesehenen Mitarbeiter zur Verfügung stehen. Zusätzlich müssen Störungen durch notwendige Tests einkalkuliert werden.
- Anwendungen und IT-Systeme, die der Outsourcing-Dienstleister übernehmen soll, sollten ausreichend dokumentiert sein. Die Prüfung der Dokumentation auf Vollständigkeit sollte dabei ebenso bedacht werden wie das Anpassen der vorhandenen Dokumentation auf die veränderten Randbedingungen durch das Outsourcing-Vorhaben. Die Dokumentation neuer Systeme oder Teilsysteme sollte dabei ebenfalls sichergestellt sein.
- Während der Migration sollte ständig überprüft werden, ob die SLAs oder die vorgesehenen Security Level Agreements angepasst werden müssen.

In der Einführungsphase des Outsourcing-Vorhabens und der ersten Zeit des Betriebs muss dem Notfallkonzept besondere Aufmerksamkeit geschenkt werden. Bis sich bei allen Beteiligten die notwendige Routine, beispielsweise in der Behandlung von Fehlfunktionen und sicherheitsrelevanten Vorkommnissen, eingestellt hat, sind verstärkt Mitarbeiter zu Bereitschaftsdiensten zu verpflichten.

Nach Abschluss der Migration muss sichergestellt werden, dass das Informationssicherheitskonzept aktualisiert wird, da sich erfahrungsgemäß während der Migrationsphase immer Änderungen ergeben. Dies bedeutet insbesondere:

- Alle Sicherheitsmaßnahmen müssen konkretisiert werden.
- Ansprechpartner und Zuständigkeiten werden mit Namen und notwendigen Kontaktdaten (Telefon, Zeiten der Erreichbarkeit, eventuell erforderliche Zuordnungsbegriffe wie Kundennummern) dokumentiert.
- Die Systemkonfigurationen sind zu dokumentieren, wobei auch die eingestellten sicherheitsrelevanten Parameter zu erfassen sind.
- Das Personal ist durch Schulungsmaßnahmen auf den Regelbetrieb vorzubereiten.
- Als letzte Aufgabe muss das Outsourcing-Vorhaben nach der Migrationsphase in den sicheren Regelbetrieb überführt werden. Dabei ist vor allem darauf zu achten, dass alle während der Migrationsphase notwendigen Ausnahmeregelungen, z. B. erweiterte Zugriffsrechte, aufgehoben werden.

OPS.2.1.M14 Notfallvorsorge beim Outsourcing [Notfallbeauftragter]

Für die Notfallvorsorge beim Outsourcing gelten grundsätzlich die gleichen Anforderungen wie beim nicht ausgelagerten Betrieb von Geschäftsprozessen oder IT-Systemen. Besonderheiten ergeben sich aber dadurch, dass die Notfallvorsorge von unterschiedlichen Parteien und dadurch auch für unterschiedlich verteilte Systeme gewährleistet werden muss.

Generell müssen Notfallvorsorgekonzepte für die Systeme beim Outsourcing-Kunden und beim Outsourcing-Dienstleister sowie für die Schnittstellen zwischen Outsourcing-Kunden und Outsourcing-Dienstleister (z. B. Netzverbindung, Router, Telekommunikationsprovider) existieren. In OPS.2.1.M4 Vertragsgestaltung mit dem Outsourcing-Dienstleister wird beschrieben, welche Aspekte bereits im Rahmen der Vertragsgestaltung geregelt werden sollten. Im Notfallvorsorgekonzept müssen diese Vorgaben im Detail beschrieben werden. Im Rahmen der Notfallvorsorge sollten zudem insbesondere die folgenden Aspekte berücksichtigt werden:

- Zuständigkeiten, Ansprechpartner und Abläufe sollten klar geregelt und vollständig dokumentiert werden.
- Es sollten detaillierte Arbeitsanweisungen für bestimmte Fehlersituationen erstellt werden.
- Es sollte ein Konzept für die Durchführung regelmäßiger Notfallübungen erarbeitet werden.

Die Informationssicherheit hängt in Notfällen entscheidend von der Qualität der Arbeitsanweisungen für das Personal des Outsourcing-Dienstleisters ab. Oftmals werden die Systeme des Outsourcing-Kunden vom Personal des Outsourcing-Dienstleisters betrieben, das keine Detailkenntnisse über die Anwendungen besitzt, die auf den IT-Systemen betrieben werden. Die Verantwortung für die Anwendung liegt dennoch ausschließlich beim Outsourcing-Kunden. Tritt ein Fehler in der Anwendung auf, muss der Outsourcing-Dienstleister unter Umständen eine Fehlerbehebung herbeiführen, ohne umfangreiche Kenntnisse über das Gesamtsystem zu besitzen. Durch das Notfallvorsorgekonzept müssen dem Outsourcing-Dienstleister daher genaue Anweisungen zur Verfügung gestellt werden. Im Zuge dessen kann es auch sinnvoll sein, Aktionen zu definieren, die explizit verboten sind (z. B. Reboot eines IT-Systems).

Ein Fehlverhalten einer Anwendung kann technische (z. B. voller Datenträger, Netzprobleme) oder anwendungsspezifische Ursachen haben (z. B. Verarbeitung eines falschen Datensatzes, Programmfehler, falsche Parametereinstellung). Bei technischen Fehlern ohne Auswirkungen auf andere Anwendungen wird der Outsourcing-Dienstleister den Fehler zwar selbst beheben können, eine Kooperation mit dem Outsourcing-Kunden ist meist aber dennoch notwendig, um unerwünschte Nebeneffekte auf Applikationsebene zu verhindern. Liegen anwendungsspezifische Probleme vor, benötigt der Outsourcing-Dienstleister detaillierte und umfangreiche Anweisungen sowie Listen mit Ansprechpartnern aufseiten des Outsourcing-Kunden, damit er richtig reagieren kann. Besonders bei Problemen mit komplizierten Anwendungen oder bei umfangreichen Patch-Prozessen sind häufig Kenntnisse erforderlich, die nur beim Kunden vorhanden sind.

Wichtig ist auch, dem Outsourcing-Dienstleister Informationen über den Schutzbedarf der betroffenen Daten und Systeme zur Verfügung zu stellen, damit er angemessen handeln kann.

Der Outsourcing-Kunde sollte regelmäßig überprüfen, wie effizient und effektiv die Notfallmaßnahmen des Outsourcing-Dienstleisters umgesetzt sind und wie gut diese mit den eigenen Notfallmaßnahmen abgestimmt sind. Daher sollten regelmäßig gemeinsame Notfallübungen von Outsourcing-Kunden und Outsourcing-Dienstleister durchgeführt werden.

OPS.2.1.M15 Geordnete Beendigung eines Outsourcing-Verhältnisses [Leiter Beschaffung]

Ein Outsourcing-Verhältnis endet entweder beabsichtigt und erwartet (z. B. nach dem Erreichen eines definierten Ziels nach dem Projektende oder aufgrund einer Übertragung der Leistungserbringung auf einen anderen Dienstleister) oder unbeabsichtigt und unerwartet (z. B. aufgrund einer Insolvenz des Outsourcing-Dienstleisters).

Um im Zuge einer beabsichtigten Beendigung ausreichend Zeit für die Rückintegration bzw. Übertragung der ausgelagerten Prozesse und Aktivitäten auf einen anderen Outsourcing-Dienstleister zu haben, sind ausreichende Kündigungsfristen zu vereinbaren (siehe OPS.2.1.M4 Vertragsgestaltung mit dem Outsourcing-Dienstleister). Die Einhaltung der vereinbarten Kündigungsfristen kann jedoch nicht immer gewährleistet werden. Aufgrund von Insolvenzen, technischen Störungen oder Naturkatastrophen kann die Leistungserbringung des Outsourcing-Dienstleisters kurzfristig ausfallen. Um diesem Risiko zu begegnen und in solchen Fällen die Kontinuität sowie die Qualität der Leistungserbringung aufrecht zu erhalten, sollte der Outsourcing-Kunde über angemessene Notfallkonzepte verfügen (siehe OPS.2.1.M14 Kontrolle der Notfallvorsorge beim Outsourcing). Dies gilt insbesondere für Outsourcing-Vorhaben, die zeitkritische Prozesse und Aktivitäten betreffen.

Sollte im Anschluss an die Beendigung der Outsourcing-Beziehung eine Übertragung der Leistungserbringung auf einen anderen Outsourcing-Dienstleister erfolgen, ist diese als neues Outsourcing-Vorhaben anzusehen. Demnach sind dafür alle Anforderungen des Bausteins erneut umzusetzen. Beim Insourcing, also der Wiedereinlagerung der Leistungserbringung in die eigene Institution, gilt dies analog. Für Strategie, Sicherheitskonzept für Insourcing, Migration und Notfallvorsorge gelten die gleichen Anforderungen wie bei einem "klassischen" Outsourcing-Vorhaben.

Folgende Gesichtspunkte sind zu beachten:

- Eigentumsrechte an Hard- und Software (Schnittstellenprogramme, Tools, Batchabläufe, Makros, Lizenzen, Backups) müssen geregelt werden.
- Die Weiterverwendung der vom Dienstleister eingesetzten Tools, Prozeduren, Skripte und anderer Software ist für den Fall der Beendigung des Dienstleistungsverhältnisses zu regeln.
- Die IT-Systeme, -Anwendungen und Arbeitsabläufe beim Outsourcing-Dienstleister müssen ausreichend dokumentiert sein.
- Alle notwendigen Daten müssen vom Dienstleister an den Kunden übertragen beziehungsweise übergeben werden.
- Alle Datenbestände beim Dienstleister müssen sicher gelöscht werden. Die Löschung der Datenbestände sollte sich der Outsourcing-Kunde schriftlich bestätigen lassen.
- Alle Berechtigungen, die im Rahmen des Outsourcing-Projekts eingerichtet wurden, sind zu überprüfen. Der Outsourcing-Kunde sollte alle Berechtigungen löschen, die für den Outsourcing-Dienstleister oder Dritte eingerichtet wurden.
- Interne oder externe Mitarbeiter, die Aufgaben des Dienstleisters übernehmen, müssen eingewiesen und geschult werden.
- Es ist empfehlenswert, vertraglich eine Übergangsfrist zu vereinbaren, in der der ehemalige Dienstleister noch für Rückfragen und Hilfestellungen zur Verfügung steht.
- Bei Beendigung des Outsourcing-Verhältnisses muss eine geregelte Übergabe der Arbeitsergebnisse und der erhaltenen Unterlagen und Betriebsmittel erfolgen. Den Mitarbeitern des Outsourcing-Dienstleisters sind zudem sämtliche Zugangsberechtigungen und Zugriffsrechte zu entziehen..

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

OPS.2.1.M16 Sicherheitsüberprüfung von Mitarbeitern (CI)

Der Outsourcing-Kunde sollte sich die Qualifikation, aber auch die Vertrauenswürdigkeit der Mitarbeiter des Outsourcing-Dienstleisters geeignet nachweisen lassen.

Die Möglichkeiten, die Vertrauenswürdigkeit von Personal überprüfen zu lassen, sind in Deutschland, aber auch in vielen anderen Ländern, rechtlich sehr eingeschränkt. Zudem sind die Ergebnisse meist wenig aussagekräftig, z. B. bei polizeilichen Führungszeugnissen. Grundsätzlich sollte aber vor der Übernahme neuer oder externer Mitarbeiter in Projekte überprüft werden, ob

- diese hinreichende Referenzen haben, z. B. aus anderen, ähnlichen Projekten
- der vorgelegte Lebenslauf des Bewerbers aussagekräftig und vollständig ist

Darüber hinaus kann es sinnvoll sein, sich akademische und berufliche Qualifikationen bestätigen zu lassen, beispielsweise durch Nachfragen bei der Universität oder früheren Arbeitgebern oder Kunden. Auch die Identität des Bewerbers sollte verifiziert werden, z. B. durch Vorlage von Ausweispapieren.

Wenn Personal auf Seiten des Outsourcing-Dienstleisters intern beim Kunden eingesetzt wird oder im Rahmen von Projekten, Kooperationen oder Outsourcing-Vorhaben auf interne Anwendungen und Daten zugreifen kann, sollten vergleichbare Überprüfungen wie für eigene Mitarbeiter durchgeführt werden. Bei der Vertragsgestaltung mit Outsourcing-Dienstleistern sollte vertraglich festgehalten werden, welche Seite solche Überprüfungen durchzuführen hat und in welcher Tiefe diese erfolgen.

3 Weiterführende Informationen

3.1 Wissenswertes

Hinweis zur Fußzeile: Das "zuletzt geprüft" kann auch weggelassen werden, solange die beiden Daten "zuletzt aktualisiert" und "zuletzt geprüft" übereinstimmen.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Outsourcing für Kunden" finden sich unter anderem in folgenden Veröffentlichungen:

[27001] ISO/IEC 27001:2013

Information technology-Security techniques-Information security management systems-Requirements, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/SC 27, Oktober 2013

[BVIT2005] Leitfaden Business Process Outsourcing

BPO als Chance für den Standort Deutschland, Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V. (Bitkom), Version 10.1, September 2005, https://www.bitkom.org/Bitkom/Publikationen/Leitfaden-Business-Process-Outsourcing.html, zuletzt abgerufen am 26.07.2018

[BVIT2008] Leitfaden Rechtliche Aspekte von Outsourcing in der Praxis

Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V. (Bitkom), Januar 2008, https://www.bitkom.org/Bitkom/Publikationen/Rechtliche-Aspekte-von-Outsourcing-in-der-Praxis.html, zuletzt abgerufen am 26.07.2018

[ISF] The Standard of Good Practice for Information Security:

Information Security Forum (ISF), June 2018

[NIST80053] Security and Privacy Controls for Federal Information Systems and Organizations

NIST Special Publication 800-53, Revision 4, April 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf , zuletzt abgerufen am 30.08.2018

Umsetzungshinweise zum Baustein OPS.2.2 Cloud-Nutzung

1 Beschreibung

1.1 Einleitung

Mithilfe von Cloud-Diensten können Institutionen IT-Infrastruktur (Rechenleistungen oder Speicherkapazitäten), IT-Plattformen (Datenbanken oder Applikations-Server) oder auch IT-Anwendungen (Auftragssteuerung und Groupware) nach spezifischen Bedürfnissen als Dienst über ein Datennetz beziehen. Dabei kann die Leistung sowohl in den Räumlichkeiten des Auftraggebers als auch bei einem externen Cloud-Diensteanbieter erbracht werden.

Cloud Computing bietet viele Vorteile: Die IT-Dienste können bedarfsgerecht, skalierbar und flexibel genutzt und je nach Funktionsumfang, Nutzungsdauer und Anzahl der Benutzer abgerechnet werden. In der Praxis zeigt sich jedoch häufig, dass sich die Vorteile, die sich Institutionen von der Cloud-Nutzung erwarten, nicht vollständig auswirken. Die Ursache dafür ist meistens, dass wichtige kritische Erfolgsfaktoren nicht ausreichend betrachtet wurden. Dazu gehören z. B. eine strategische Planung für Cloud-Dienste sowie die sorgfältige Definition und Vereinbarung von (Sicherheits-)Anforderungen, Verantwortungen und Schnittstellen. Auch das Bewusstsein für ein erforderliches geändertes Rollenverständnis, sowohl aufseiten des IT-Betriebs als auch der Benutzer, ist ein wichtiger Erfolgsfaktor.

Zusätzlich ist bei der Einführung von Cloud-Diensten eine Reihe von Governance-Themen wichtig. Beispiele hierfür sind die Vertragsgestaltung, die Umsetzung von Mandantenfähigkeit, die Sicherstellung von Portabilität unterschiedlicher Services, die Abrechnung genutzter Service-Leistungen, das Monitoring der Service-Erbringung, das Sicherheitsvorfallmanagement und zahlreiche Datenschutzaspekte.

1.2 Lebenszyklus

Planung und Konzeption

Die Entscheidung einer Institution, Cloud-Dienste zu nutzen, ist strategischer Natur. Daher müssen relevante wirtschaftliche, technische und organisatorische Randbedingungen sowie sicherheitsrelevante Aspekte betrachtet werden und in eine Cloud-Nutzungs-Strategie einfließen (siehe OPS.2.2.M1 *Erstellung einer Cloud-Nutzungs-Strategie*). Nachdem die Cloud-Nutzungs-Strategie festgelegt worden ist, ergeben sich konkrete Sicherheitsvorgaben für die Umsetzung innerhalb der Institution. Diese müssen in ausreichend detaillierter Form in einer Sicherheitsrichtlinie für die Cloud-Nutzung (siehe OPS.2.2.M2 *Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung*) dokumentiert werden.

Die ermittelten Sicherheitsanforderungen, die relevanten Schnittstellen sowie die benötigten Service-Level sollten die Grundlage für die Service-Definition des zu verwendenden Cloud-Dienstes bilden (siehe OPS.2.2.M3 *Service-Definition für Cloud-Dienste durch den Anwender* und OPS.2.2.M4 *Festlegung von Verantwortungsbereichen und Schnittstellen*).

Ist der zu nutzende Cloud-Dienst abschließend definiert, sollten in der Folge umfangreiche Planungsmaßnahmen durchgeführt werden, um einen sicheren, fortlaufenden Betrieb des Dienstes gewährleisten zu können. Besonders wichtig ist hierbei, die Migration (siehe OPS.2.2.M5 *Planung der sicheren Migration zu einem Cloud-Dienst*) und die Einbindung der Cloud-Dienste geeignet zu planen (siehe Maßnahme OPS.2.2.M6 *Planung der sicheren Einbindung von Cloud-Diensten*).

Auf der Basis der Cloud-Nutzungs-Strategie und der erarbeiteten Sicherheitsrichtlinie sollte zudem ein Sicherheitskonzept für die gesamte Cloud-Nutzung erarbeitet werden (siehe OPS.2.2.M7 *Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung*).

Sofern eine Institution höhere Anforderungen an einen Cloud-Dienst hat, sollten zusätzliche Sicherheitsanforderungen erfüllt werden. So sollten dann z. B. die Portabilität der Dienste sichergestellt (OPS.2.2.M15 *Portabilität von Cloud-Diensten*) und die Daten verschlüsselt werden (siehe OPS.2.2.M17 *Einsatz für die Verschlüsselung bei Cloud-Nutzung*.

Beschaffung

Voraussetzung für die Auswahl eines geeigneten Cloud-Diensteanbieters ist ein möglichst detailliertes Anforderungsprofil. Die zuvor ermittelten Sicherheitsanforderungen sowie die erfolgte Definition der Cloud-Dienste liefern, kombiniert mit einer Anforderungsanalyse, die Basis für ein Lastenheft. Dieses ist mit verfügbaren bzw. angeforderten Angeboten von Cloud-Diensteanbietern abzugleichen. Nähere Angaben zu einer geeigneten Vorgehensweise bei der Auswahl eines Cloud-Diensteanbieters finden sich in Maßnahme OPS.2.2.M8 *Sorgfältige Auswahl eines Cloud-Diensteanbieters*, in der auch mögliche Fallstricke vermerkt sind.

Umsetzung

Nachdem ein Cloud-Diensteanbieter ausgewählt wurde, sollten alle relevanten Aspekte des Cloud-Nutzungs-Vorhabens vertraglich festgehalten und geregelt werden. Der Vertrag sollte neben Aussagen zu Sicherheitsanforderungen und der erforderlichen Servicequalität auch Regelungen zu Auskunfts-, Mitwirkungs- und Revisionspflichten beinhalten (siehe OPS.2.2.M9 *Vertragsgestaltung mit dem Cloud-Dienstanbieter*).

Letztlich müssen alle notwendigen Prozesse und Daten sicher zum Cloud-Dienst migriert werden (siehe OPS.2.2.M10 *Sichere Migration zu einem Cloud-Dienst*). Für größere Cloud-Projekte wird hierfür ein Phasenmodell empfohlen.

Betrieb

Die Informationssicherheit muss im laufenden Betrieb aufrechterhalten werden. Dafür sind eine Reihe von Maßnahmen zu realisieren, z. B. Dokumentationen und Richtlinien aktualisieren, Kontrollen und Abstimmungsrunden durchführen sowie Übungen umsetzen (siehe OPS.2.2.M12 *Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb)*.

Häufig lassen sich nicht eingehaltene vertragliche Vereinbarungen (z. B. unvollständig umgesetzte Sicherheitsanforderungen) nur durch ein Audit aufdecken. Deswegen sollten Cloud-Diensteanbieter regelmäßig durch Dritte auditiert werden (siehe OPS.2.2.M13 *Nachweis einer ausreichenden Informationssicherheit bei der Cloud-Nutzung)*.

Aussonderung

Damit ein Cloud-Nutzungs-Verhältnis geordnet beendet werden kann, müssen Eigentumsrechte an Hard- und Software geklärt sein. Außerdem muss festgelegt sein, wie Datenbestände vom Dienstleister zurückgegeben werden. Ebenso müssen alle erforderlichen Informationen dokumentiert sein, die für die Weiterführung des Betriebs von IT-Systemen und Anwendungen nötig sind (siehe OPS.2.2.M14 *Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses*).

Notfallvorsorge

Für die Cloud-Nutzung muss ein Notfallkonzept erstellt werden (siehe OPS.2.2.M11 *Erstellung eines Notfallkonzeptes für einen Cloud-Dienst*). Darin sollten relevante organisatorische und technische Punkte thematisiert werden.

Stellt eine Institution fest, dass besondere Gegebenheiten eigens durchgeführte Datensicherungen erforderlich machen, sind die Vorgaben der Maßnahme OPS.2.2.M16 *Durchführung eigener Datensicherungen* umzusetzen.

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Cloud-Nutzung" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

OPS.2.2.M1 Erstellung einer Cloud-Nutzungs-Strategie

Die Entscheidung einer Institution, Cloud-Dienste zu verwenden, hat immer eine strategische Komponente, auch wenn der Umfang des Cloud-Dienstes gering ist. Letzteres kann dazu verleiten, die Konsequenzen dieses Outsourcings zu unterschätzen oder zu verleugnen, zumal es häufig der erste Fall von Outsourcing von IT-Dienstleistungen in der Institution ist. Oft unterscheidet sich Outsourcing von Cloud-Nutzung im Umfang, in der Vertragsdauer sowie in der Art und Weise, wie die Dienste erbracht werden. Trotz allem ist die Nutzung von Cloud-Diensten immer ein Outsourcing (zumindest, wenn ein externer Dienstleister beauftragt wird) und somit strategischer Natur. Deswegen müssen wirtschaftliche, technische und organisatorische Randbedingungen sowie sicherheitsrelevante Aspekte ausführlich betrachtet werden.

Die nachfolgend beschriebenen Gesichtspunkte sollten in einer Cloud-Nutzungs-Strategie betrachtet und dokumentiert werden.

Einbindung in die Institutionsstrategie

Es ist zu klären, wie die Institution strategisch mit dem Thema Cloud-Nutzung umgeht. Ausgehend von der grundsätzlichen Entscheidung für Cloud-Dienste ist dabei festzuhalten, in welchem Umfang klassische IT durch Cloud-Dienste abgelöst werden soll. Es ist zu erarbeiten, welche Dienste für eine Cloud-Nutzung grundsätzlich infrage kommen.

Ebenso sollte beantwortet werden, warum Cloud-Dienste überhaupt eingesetzt werden sollen. Darüber hinaus sind die Ziele zu definieren, die die Institution mit der Cloud-Nutzung erreichen will. Das können beispielsweise Kosteneinsparungen, ein flexiblerer Service, der Ersatz bisheriger Dienste oder die Nutzung neuer Dienste sein.

Die Ergebnisse sollten möglichst auch in die Institutionsstrategie eingebunden werden.

Machbarkeitsstudie mit Zusammenstellung aller Rahmenbedingungen

Es gibt unterschiedliche äußere Faktoren, die die Entscheidung zur Cloud-Nutzung beeinflussen können oder diese bedingen. Das sind sowohl

- rechtliche Rahmenbedingungen (beispielsweise Vorgaben des Datenschutzes,von Aufsichtsbehörden oder von anderen Vertragspartnern),
- organisatorische Rahmenbedingungen (beispielsweise Reife der Institution hinsichtlich Organisation und IT) als auch
- technische Anforderungen (beispielsweise Vorgaben bezüglich des benötigten Datennetzes, Leistungsfähigkeit der Internetanbindung, Verfügbarkeit der Datennetze und der IT-Systeme).

Die Ergebnisse dieser Untersuchung sind in einer Machbarkeitsstudie zu dokumentieren, die aussagt, ob der untersuchte Cloud-Dienst überhaupt benutzt werden kann.

Betriebswirtschaftliche Aspekte mit erster Kosten-Nutzen-Abschätzung

Da durch Cloud Computing oft Geld gespart werden soll, stehen Kosten und Nutzen besonders im Fokus. Die Kosten-Nutzen-Abschätzung ergibt eine erste Indikation, ob aus einem Cloud-Dienst wirtschaftliche Vorteile gezogen werden können.

Hier sind auf der Kostenseite nicht nur die reinen Betriebskosten des Cloud-Dienstes zu berücksichtigen, sondern auch die Kosten für die Migration, die Schulung der Mitarbeiter und Administratoren, gegebenenfalls für neue Hardware und den Ausbau der Netzkapazitäten.

Bei der Kosten-Nutzen-Abschätzung sollte die Institution auch den strategischen Wert der Ressourcen Know-how, Mitarbeiter, IT-Systeme und Anwendungen berücksichtigen. Denn diese Ressourcen können durch die Nutzung von Cloud Computing teilweise verloren gehen. Auf der Nutzenseite könnte stehen, dass vielleicht obsolet gewordene Hardware mitsamt Lizenzen und Administration nicht ersetzt werden muss, bessere und schneller anpassbare IT und eventuelle Sicherheitsgewinne.

Sobald der Cloud-Dienst genauer definiert ist und erste konkrete Angebote einzelner Cloud-Diensteanbieter vorliegen, erfolgt eine detaillierte Kosten-Nutzen-Analyse (siehe OPS.2.2.M8 *Sorgfältige Auswahl eines Cloud-Diensteanbieters*).

Auswahl der Dienste und des Bereitstellungsmodells

Nach diesen strategischen Überlegungen sollte festgehalten werden, welche konkreten Dienste zukünftig von einem Cloud-Diensteanbieter bezogen werden könnten. Daneben ist auf der Basis der erhobenen Anforderungen zu entscheiden, welches Bereitstellungsmodell (zum Beispiel Private, Public, Hybrid Cloud) geeignet erscheint. Dieser Schritt wird häufig auch als Sourcing bezeichnet.

Berücksichtigung von Sicherheitsaspekten von Anfang an

Die Institution muss sicherstellen, dass grundlegende technische und organisatorische Sicherheitsaspekte bereits zu Beginn der Planungsmaßnahmen zur Cloud-Nutzung ausreichend berücksichtigt werden. Insbesondere ist auch zu klären, ob und inwieweit das Cloud Computing in der Sicherheitsleitlinie abgedeckt ist. Dabei sollten sich die Verantwortlichen innerhalb einer Institution insbesondere folgender Cloud-Spezifika bewusst sein:

- Der Cloud-Diensteanbieter kann je nach Cloud-Nutzungs-Modell auf die Daten der beauftragenden Institution zugreifen. Davon können auch Daten mit erhöhtem Schutzbedarf betroffen sein.
- Es werden immer Daten zwischen beauftragender Institution und dem Cloud-Diensteanbieter übertragen. Das dadurch erhöhte Gefahrenpotenzial ist durch die Institution zu ermitteln und entsprechend zu bewerten.
- Die Einführung von Cloud-Diensten setzt neue Prozesse und Arbeitsabläufe voraus, die entworfen, eingeführt und umgesetzt werden müssen. Die Folgen der notwendigen Umstellungen sind zu ermitteln und abzuschätzen.

Im Rahmen der Nutzung von Cloud-Diensten sollten Vor- und Nachteile, die einen Bezug zur Informationssicherheit aufweisen, durch die Institution betrachtet, bewertet und dokumentiert werden.

Durchführung einer groben Sicherheitsanalyse

Zur Festlegung der Cloud-Strategie sollte eine grobe individuelle Sicherheitsanalyse für den geplanten Cloud-Dienst durchgeführt werden, die zu wiederholen ist, wenn sich wesentliche technische und organisatorische Rahmenbedingungen verändern. Nur so kann festgestellt werden, wie bestehende Geschäftsprozesse oder Informationsverbünde abgegrenzt und getrennt werden können, damit Teile davon als Cloud-Dienst genutzt werden können. In dieser frühen Projektphase wird das Sicherheitskonzept naturgemäß nur Rahmenbedingungen beschreiben und keine detaillierten Maßnahmen enthalten.

Die Ergebnisse der Sicherheitsanalyse sollten unmittelbar in die Kosten-Nutzen-Abschätzung einfließen, die nach der Sicherheitsanalyse eventuell wieder angepasst werden muss.

Erstellung einer Roadmap

Nachdem die strategischen und sicherheitsrelevanten Aspekte untersucht wurden, sollte überlegt werden, wie die Dienste geeignet technisch realisiert werden sollen. Sofern mehrere Cloud-Dienste geplant sind, hat es sich in der Praxis als hilfreich erwiesen, eine sogenannte Cloud-Roadmap zu erstellen. Diese stellt einen Fahrplan zur Nutzung der Cloud-Dienste dar und beschreibt, wie sie mithilfe eines Phasenmodells auszurollen sind. So kann die Akzeptanz der Cloud-Dienste durch den Benutzer erhöht werden, während gleichzeitig das Risiko technischer Probleme bei der späteren Umsetzung gemindert wird.

OPS.2.2.M2 Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung

Aus der Strategie zur Cloud-Nutzung (siehe OPS.2.2.M1 *Erstellung einer Cloud-Nutzungs-Strategie*) ergeben sich, je nach Detaillierungsgrad, bereits Sicherheitsvorgaben für die Nutzung von Cloud-Diensten. Diese müssen in der Sicherheitsrichtlinie weiter verfeinert werden, sodass damit ein gewünschter Cloud-Dienst definiert (siehe *OPS.2.2.M3 Service-Definition für Cloud-Dienste durch den Anwender und OPS.2.2.M4 Festlegung von Verantwortungsbereichen und Schnittstellen*) sowie ein geeigneter Cloud-Diensteanbieter ausgewählt werden kann (siehe *OPS.2.2.8 Sorgfältige Auswahl eines Cloud-Diensteanbieters*).

Grundsätzlich müssen in diesem Zusammenhang möglichst alle Sicherheitsanforderungen betrachtet werden, die sich aus den ermittelten Schnittstellen sowie den organisatorischen, technischen und rechtlichen Rahmenbedingungen ergeben. Neben den Sicherheitsanforderungen an die eingesetzte Technik, einschließlich der benötigten Kommunikationswege und -dienste, ist daher zum Beispiel auch notwendig Datenschutzaspekte sowie Aspekte zur Informationsklassifizierung für alle ausgelagerten Daten zu berücksichtigen. Auch organisatorische Auswirkungen wie beispielsweise notwendige Schulungsmaßnahmen für Administratoren und Benutzer sollten bereits in der Sicherheitsrichtlinie berücksichtigt werden.

Weiterhin sollten insbesondere die nachfolgend beschriebenen Aspekte in die Sicherheitsrichtlinie für die Cloud-Nutzung eingehen:

- **Sicherheitsanforderungen an den Cloud-Diensteanbieter** sollten die benötigte technische Verfügbarkeit des angebotenen Dienstes sowie Vorgaben zum Standort der Leistungserbringung des Cloud-Diensteanbieters berücksichtigen. Zudem sollten Anforderungen hinsichtlich bestehender organisatorischer Regelungen und gelebter Prozesse beim Cloud-Diensteanbieter (beispielsweise die Einhaltung des Vier-Augen-Prinzips bei der Administration) festgelegt sein. Auch Regelungen für den Einsatz von Fremdpersonal fallen unter mögliche Sicherheitsanforderungen an den Cloud-Diensteanbieter (siehe ORP.2 *Personal*). Weitere Beispiele für Sicherheitsanforderungen an den Cloud-Diensteanbieter sind konkrete Vorgaben zur Datenablage, Datenverarbeitung und Datenlöschung. Auch geforderte Zertifizierungen des Dienstleisters (vorzugsweise nach IT-Grundschutz) sollten bereits in der Sicherheitsrichtlinie dokumentiert werden.
- **Sicherheitsanforderungen in Abhängigkeit vom Bereitstellungsmodell.** Sollen Cloud-Dienste mithilfe einer Hybrid Cloud oder einer Private Cloud On-Premise erbracht werden, ist unter anderem festzulegen, welche Nutzungsrechte (zum Beispiel Zutrittsrechte, Zugangsrechte, Zugriffsrechte auf Daten und IT-Systeme) dem Cloud-Diensteanbieter vom Auftraggeber eingeräumt werden.
- **Sicherheitsanforderungen aus relevanten Gesetzen und Vorschriften.** Ein besonderes Augenmerk sollte hierbei auf länderübergreifende oder international agierende Cloud-Diensteanbieter gelegt werden, die unter Umständen andersartigen gesetzlichen Anforderungen und Bestimmungen unterliegen.

OPS.2.2.M3 Service-Definition für Cloud-Dienste durch den Anwender

Entscheidet sich eine Institution dafür Cloud-Dienste zu nutzen, muss eine entsprechende Service-Definition erarbeitet werden. Die IT Infrastructure Library (ITIL) definiert einen Service als die "Möglichkeit, einen Mehrwert für einen Auftraggeber zu generieren. Dazu soll die Erreichung der vom Auftraggeber angestrebten Ergebnisse erleichtert oder gefördert werden. Der Auftraggeber selbst hat dabei keine Verantwortung für bestimmte Kosten oder Risiken zu tragen."

Angewandt auf die Cloud-Nutzung bedeutet dies, dass ein Mehrwert durch einen beauftragten Diensteanbieter nur generiert werden kann, wenn die angestrebten Ergebnisse innerhalb der Institution auch tatsächlich bekannt und dokumentiert sind. Grundlage für die sorgfältige Definition der zu verwendenden Cloud-Dienste sind die Anforderungen aus der Cloud-Nutzungs-Strategie (siehe OPS.2.2.M1 *Erstellung einer Cloud-Nutzungs-Strategie)* und der definierten Sicherheitsrichtlinie (siehe OPS.2.2.M2 *Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung).* Es sollte eine einheitlich gestaltete Auflistung vorgenommen werden, in der alle vorgesehenen Cloud-Dienste übersichtlich dargestellt sind. Hierfür bietet es sich beispielsweise an, sogenannte Service-Templates nach ITIL zu erstellen. Mögliche Inhalte in diesem Zusammenhang sind:

- Servicekürzel und Servicename,
- Kurzbeschreibung,
- Kategorie,
- Sub- bzw. Sekundärservices,
- Varianten,
- technische Parameter,
- Service-Parameter/SLA,
- SLA-Messung,
- Gültigkeit des Services (Zeitraum),
- Service-Übergabe,
- Methoden der Kostenermittlung,
- Preis/Verrechnung,
- Ansprechpartner für den Service,
- Berechtigte und Anforderer und
- Voraussetzungen.

Im Rahmen der Service-Definition für Cloud-Dienste sollten durch die Institution auch die nachfolgenden, näher beschriebenen Aspekte thematisiert werden.

Auswahl sicherer Authentisierungsmethoden

Für Cloud-Dienste sollten sichere Authentisierungsmethoden ausgewählt und eingesetzt werden. Dabei sind starke Authentisierungsmechanismen (zum Beispiel Zwei-Faktor-Authentisierung) zumindest für die Administration der Cloud-Dienste einzusetzen. Wurde für den Cloud-Dienst jedoch ein hohes Schutzniveau identifiziert, sollten für alle Benutzer starke Authentisierungsmechanismen eingesetzt werden. Gleiches gilt für Cloud-Dienste über das Internet, falls kein VPN eingesetzt wird.

Bei Cloud-Diensten mit normalem Schutzniveau und beim Einsatz eines VPN ist hingegen in der Regel eine Ein-Faktor-Authentisierung ausreichend. Das dabei verwendete Passwort sollte dann den Regeln für sichere Passwörter der Institution unterliegen.

Berücksichtigung weiterer Sicherheitsaspekte

Neben den genannten Aspekten sind im Rahmen der Service-Definition für Cloud-Dienste auch Vorgaben zur Verschlüsselung von Informationen zu erstellen. Sofern weitere Sicherheitsvorgaben als notwendig angesehen werden, wie beispielsweise eigene Datensicherungen durchzuführen, sollten diese ebenfalls in die Service-Definition einfließen.

Definition von OLA und SLA

Es sind konkrete interne Anforderungen an die zu verwendenden Cloud-Dienste auszuarbeiten. Außerdem muss der Service-Level für die Anwender innerhalb der eigenen Institution definiert werden. Diese internen Regelungen, die auch als Operational Level Agreement (OLA) bezeichnet werden, sind die Basis für die Erarbeitung entsprechender Service Level Agreements (SLAs) mit einem externen Cloud-Diensteanbieter.

Nach abschließend erfolgter Service-Definition für den Cloud-Dienst muss er sicher in die Institution eingebunden werden (siehe OPS.2.2.M6 *Planung der sicheren Einbindung von Cloud-Diensten)*.

Ist der Cloud-Dienst definiert, muss ein geeigneter Anbieter gefunden (siehe OPS.2.2.M8 *Sorgfältige Auswahl eines Cloud-Diensteanbieters*) und ein Vertrag mit ihm abgeschlossen werden (siehe OPS.2.2.M9 *Vertragsgestaltung mit dem Cloud-Diensteanbieter*).

OPS.2.2.M4 Festlegung von Verantwortungsbereichen und Schnittstellen

Die Institution muss alle relevanten Schnittstellen und Verantwortlichkeiten für die Cloud-Nutzung identifizieren und dokumentieren. Eine wesentliche Anwendungskomponente und wichtige Schnittstelle des Cloud-Dienstes stellt die Client-Software dar, zum Beispiel zur Integration eines zusätzlichen Laufwerks bei Nutzung eines Online-Speicherdienstes. Daher ist deren Auswahl für die Cloud-Nutzung bedeutend. Die folgenden Fragen unterstützen dabei, geeignete Lösungen zu finden:

- Existiert eine definierte Rückfallebene, wenn die Client-Software ausfällt?
- Sind eventuelle Abhängigkeiten oder Inkompatibilitäten im Zusammenhang mit der vorhandenen IT-Infrastruktur zu erwarten?
- Kann die Client-Software ohne Weiteres in die bestehenden Prozesse des Änderungsmanagements integriert werden oder sind Anpassungen notwendig? Nähere Hinweise hierzu finden sich auch im Baustein OPS.1.1.3 *Patch- und Änderungsmanagement*.
- Erfüllt die Client-Software die Anforderungen der Institution hinsichtlich bestehender Test- und Freigabeprozesse?

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich *Cloud-Nutzung*.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Cloud-Nutzung".

OPS.2.2.M5 Planung der sicheren Migration zu einem Cloud-Dienst

Damit Cloud-Dienste sicher integriert und betrieben werden können, müssen vorher umfangreiche Planungsmaßnahmen ergriffen werden. Besonders wichtig ist hierbei, die Migration und Einbindung des Dienstes zu planen. Der Begriff Migration bezeichnet dabei entweder den technischen Wechsel von einem System auf ein anderes oder den Wechsel des Cloud-Diensteanbieters. Die Planung der sicheren Einbindung von Cloud-Diensten (siehe OPS.2.2.M6 *Planung der sicheren Einbindung von Cloud-Diensten*) konzentriert sich auf unterschiedliche Aspekte, die über die Migration hinaus betrachtet werden sollten.

Für die sichere Migration zu einem Cloud-Dienst muss die Institution ein Migrationskonzept erstellen, das als Teil des Sicherheitskonzeptes für die Cloud-Nutzung auszulegen ist (siehe OPS.2.2.M7 *Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung*).

Planung der Einführung eines Cloud-Dienstes in die Institution

Ein Cloud-Dienst wird meistens stufenweise eingeführt. Zu Beginn der Planung sollten zunächst organisatorische Regelungen wie hierarchische Strukturen, Rollen und Verantwortlichkeiten sowie die Aufgabenverteilung festgelegt werden.

Zusätzlich sollten geeignete Test- und Übergabeverfahren geplant werden, um sowohl eine reibungslose Migration als auch fortlaufend einen sicheren Betrieb gewährleisten zu können.

Im weiteren Verlauf der Migrationsplanungen sollte geprüft werden, ob das festgelegte Sicherheitsniveau und die Service Level eingehalten werden. Sofern vom definierten Sollzustand abgewichen wird, müssen eventuell Anpassungen vorgenommen werden.

Zudem empfiehlt es sich, weitere vertragliche Regelungen zwischen Institution, Cloud-Diensteanbieter und gegebenenfalls externen Migrations-Dienstleistern zu definieren. Beispielsweise sollte festgelegt werden, wann die Migration als abgeschlossen zu betrachten ist und wann die Dienste an den produktiven Betrieb übergeben werden. Auch der Zeitpunkt, ab dem eine Institution die vereinbarten SLAs einfordern kann, gilt als genau zu definieren. Es ist hilfreich, nach der abgenommenen Migrationen ein Review über die gesamte Migration vorzunehmen. Wichtig sind hier auch Nachweise, was der Migrations-Dienstleister an Konvertierungen von Daten und IT-Systemen vorgenommen hat.

Berücksichtigung der eigenen IT

Cloud-Dienste müssen meistens eng in die IT-Umgebung der Institution eingebunden werden. Die bestehende IT-Umgebung ist daher in besonderem Maße bei den Migrationsplanungen zu berücksichtigen. Hierbei sollten bereits vorhandene sowie zusätzlich benötigte Schnittstellen identifiziert und eventuell an veränderte Anforderungen angepasst werden.

Auswirkung auf Betriebsprozesse

Cloud-Dienste wirken sich meistens auf die Betriebsprozesse der Institution aus. Deswegen empfiehlt es sich, bestehende Prozesse zu überprüfen und an neue Gegebenheiten anzupassen. Dabei muss auch berücksichtigt werden, wie sich das auf die Mitarbeiter auswirkt. Eventuell müssen hier neue Aufgaben und damit einhergehende Verantwortungsbereiche eindeutig definiert und zusätzlicher Schulungsbedarf identifiziert werden.

OPS.2.2.M6 Planung der sicheren Einbindung von Cloud-Diensten

Nachdem die Migrationsplanung abgeschlossen ist (siehe OPS.2.2.M5 *Planung der sicheren Migration zu einem Cloud-Dienst),* muss überlegt werden, wie Cloud-Dienste sicher in die IT einzubinden sind. Dabei sind einige Aspekte zu betrachten, die über die Migrationsplanung hinausgehen.

Basierend auf den ermittelten Anforderungen für die Cloud-Nutzung (siehe OPS.2.2.M1 *Erstellung einer Cloud-Nutzungs-Strategie*) sind notwendige Anpassungen mindestens in den nachfolgend beschriebenen Bereichen der Institution zu prüfen und zu planen. Die Ergebnisse der Prüfung sind dabei zu dokumentieren und für den Fall sich verändernder Anforderungen entsprechend anzupassen. Sofern sich aus den ermittelten Ergebnissen Handlungsbedarf ergibt, ist dieser ebenfalls zu dokumentieren und als Grundlage für weitere Maßnahmen im Rahmen der Umsetzung oder für die Durchführung von Kosten-Nutzen-Analysen anzusehen.

Anpassung der Schnittstellensysteme

Als Schnittstellensysteme sollten auf jeden Fall betrachtet werden: Loadbalancer, Proxys, Router, Sicherheitsgateways und Federation-Systeme.

Folgende Fragen helfen dabei, den Anpassungsbedarf an bestehenden Schnittstellensystemen sowie den Bedarf an potenziellen Neuanschaffungen in diesem Bereich zu ermitteln:

- Besteht ein Bedarf an der Bereitstellung neuer Schnittstellensysteme?
- Sind alle benötigten Schnittstellensysteme mit dem betrachteten Cloud-Dienst interoperabel?
- Können die vorhandenen Schnittstellensysteme auf allen Ebenen mit dem jeweiligen Cloud-Dienst umgehen? Kann beispielsweise der vorhandene Proxy den Applikationsverkehr angemessen inspizieren?
- Welche Performance beziehungsweise welchen Datendurchsatz müssen geeignete Schnittstellensysteme zur Verfügung stellen können?
- Müssen Schnittstellensysteme redundant ausgelegt sein und wenn ja, wie wird dies umgesetzt?

Sofern ein Cloud-Dienst über eine Schnittstelle (API - Application Programming Interface) eingebunden wird, sind zusätzlich die entsprechenden Anforderungen des Bausteins APP.3.5 *Webservices* umzusetzen.

Anpassung der Netzanbindung

Um zu ermitteln, ob die vorhandene Netzanbindung angepasst werden muss, sollten folgende Punkte geklärt werden:

- Ist die bestehende Bandbreite der Netzanbindung ausreichend oder muss sie für die Cloud-Nutzung angepasst werden?
- Stellen die zu nutzenden Cloud-Dienste spezielle Anforderungen an die Latenz der Netzanbindung?
- Sollen Cloud-Dienste redundant angebunden werden? Wie kann in diesem Fall die redundante Anbindung umgesetzt werden?
- Muss der Netzverkehr unterschiedlich priorisiert werden (Quality of Service – QoS), um beispielsweise Videoinformationen oder Sprache qualitativ hochwertig übertragen zu können?
- Welche Vorkehrungen wurden hinsichtlich der Ausfallsicherheit der Netzanbindung getroffen? Müssen in diesem Zusammenhang weitere Maßnahmen umgesetzt werden?

Anpassung des Administrationsmodells

Um notwendige Anpassungen des Administrationsmodells zu identifizieren, sollten nachfolgende Fragen beantwortet werden:

- Wurde die Administration von Cloud-Diensten sorgfältig geplant?
- Existiert ein Rollen- und Berechtigungskonzept, das eine Trennung von Administratoren (Customer Cloud Service Administrator, oft auch lediglich als Service-Administrator bezeichnet) und Benutzern für die Cloud-Nutzung vorsieht?

Anpassung des Datenmanagementmodells

Je nach gewähltem Bereitstellungsmodell befinden sich gegebenenfalls eigene Daten nicht mehr ausschließlich in der administrativen Hoheit der eigenen Institution. Es ist daher zu planen, ob und wie sich die Datensicherungs- und Datenaufbewahrungs-Strategien durch Cloud-Dienste verändern.

OPS.2.2.M7 Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung

Für Cloud-Dienste sollte, wenn möglich, auf der Basis der IT-Grundschutz-Vorgehensweise ein Sicherheitskonzept erstellt werden. Solche Konzepte unterscheiden sich dabei oft nur wenig von Sicherheitskonzepten für Informationsverbünde, die durch die Institution selbst betrieben werden.

Eine der wenigen Besonderheiten bei Cloud-Diensten ist, dass mehrere Parteien beteiligt sind. Das ist auch im Sicherheitskonzept zu berücksichtigen. In der Regel sind mindestens die nachfolgenden drei Parteien an einem Cloud-Nutzungs-Vorhaben beteiligt:

- Auftraggeber der Cloud-Dienste (nutzende Institution),
- Anbieter von Cloud-Diensten (Cloud-Diensteanbieter) sowie
- ein (oder mehrere) Netzprovider.

Grundsätzlich muss jede genannte Partei ein Sicherheitskonzept erstellen. Sofern der Bedarf nach einem Sicherheitskonzept des Netzproviders besteht, sind hierzu in der Regel vorab entsprechende Vereinbarungen mit ihm zu treffen.

Das Sicherheitskonzept dokumentiert die notwendigen Sicherheitsmaßnahmen im Zusammenhang mit der Nutzung von Cloud-Diensten. Die Grundlage für diese Dokumentation bilden dabei jene Anforderungen, die sich aus der Sicherheitsrichtlinie zur Cloud-Nutzung (siehe OPS.2.2.M2 *Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung*) für einen konkreten Anwendungsfall beziehungsweise einen konkreten Cloud-Dienst ableiten lassen.

Das Sicherheitskonzept für einen Cloud-Dienst sollte sich an den Sicherheitsanforderungen für einen klassischen IT-Service orientieren. Die sich hieraus ergebenden Anforderungen sollten die Basis für die Betrachtung des Cloud-Dienstes darstellen.

Im Sicherheitskonzept für die Cloud-Nutzung sollte zusätzlich die besondere Gefährdungslage durch Cloud-Dienste beschrieben werden. Hierbei sollten insbesondere folgende Punkte betrachtet werden:

- Vorzeitige oder zwangsweise Vertragsbeendigung,
- Fehlende Portabilität von Daten (insbesondere bei Software as a Service), Anwendungen (insbesondere bei Platform as a Service) und IT-Systemen (insbesondere bei Infrastructure as a Service) für den Fall, dass der gewählte Cloud-Dienst von etablierten Standards abweicht,
- Abhängigkeit von einem Cloud-Diensteanbieter durch fehlende Möglichkeit, den Anbieter zu wechseln (Vendor-Lock-in),
- Nutzung proprietärer Datenformate, die die Integrität der Informationen gefährden und den Wechsel des Anbieters erschweren,
- Gemeinsame Nutzung der Cloud-Infrastruktur durch mehrere Institutionen (multi-tenancy),
- Fehlende Kenntnis über den Speicherort von Informationen,
- In der Regel hohe Mobilität der Informationen sowie
- Unbefugter Zugriff auf Informationen, zum Beispiel durch Administratoren des Cloud-Diensteanbieters oder Dritte.

Abgeleitet aus diesen spezifischen Gefährdungen für den jeweiligen Cloud-Dienst müssen konkrete Sicherheitsanforderungen festgelegt werden. Diese sollten in jedem Fall im Rahmen der Vertragsgestaltung mit dem Cloud-Diensteanbieter verbindlich vereinbart werden. Hierbei sollten insbesondere folgende Punkte betrachtet werden:

- Vorgaben zur sicheren Administration des Cloud-Dienstes (zum Beispiel 4-Augen-Prinzip für bestimmte, besonders kritische administrative Tätigkeiten wie das Kopieren einzelner Datenbestände oder IT-Systeme),

- Vorgaben zu Betriebsprozessen und Prozessen im Sicherheitsmanagement (Schnittstellen zum Beispiel für das Change-, Incident-, Sicherheitsvorfalls- und Risikomanagement),
- Regelungen zur Überwachung der Service-Erbringung und zum Berichtswesen,
- Verschlüsselung der Informationen,
- Vergabe und Entzug von Berechtigungen sowie
- Durchführung von Datensicherungen, sowohl durch den Cloud-Diensteanbieter als auch durch die Institution.

Durch unabhängige Dritte sollte regelmäßig kontrolliert werden, ob das Sicherheitskonzept aufseiten des Cloud-Diensteanbieters existiert und korrekt umgesetzt wird.

OPS.2.2.M8 Sorgfältige Auswahl eines Cloud-Diensteanbieters

Nach der Planungs- und Konzeptionsphase ist durch die Institution ein geeigneter Anbieter für den definierten Cloud-Dienst auszuwählen. Dazu sollte ein möglichst detailliertes Anforderungsprofil erstellt werden. Neben der Definition des einzusetzenden Cloud-Dienstes finden sich in OPS.2.2.M3 *Service-Definition für Cloud-Dienste durch den Anwender* und OPS.2.2.M4 *Festlegung von Verantwortungsbereichen und Schnittstellen* weitere Aspekte, die für das Anforderungsprofil für den Cloud-Diensteanbieter relevant sind. Weitere Sicherheitsanforderungen sind aus den Maßnahmen OPS.2.2.M2 *Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung* und OPS.2.2.M7 *Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung* einzubeziehen. Daneben sollte eine Anforderungsanalyse durchgeführt werden, die den dokumentierten Vorgaben eine Gewichtung beziehungsweise Bewertung zuordnet.

Aus allen ermittelten Anforderungen ist ein Leistungskatalog bzw. ein Lastenheft zu generieren. Auf dieser Basis kann die Institution individuelle Angebote einholen oder verfügbare Standard-Angebote der Cloud-Diensteanbieter vergleichen.

Beschaffung und Auswertung weitergehender Informationen

Darüber hinaus sind bei der Auswahl eines geeigneten Cloud-Diensteanbieters weitere Aspekte zu betrachten. Als Bewertungsmethode hat sich in der Praxis eine Punkte-Matrix (zum Beispiel Balanced Scorecard) bewährt.

Nachfolgend beschriebene Aspekte sollten für die Auswahl eines geeigneten Cloud-Diensteanbieters herangezogen werden.

- **Reputation des Anbieters** Sofern Informationen hierüber verfügbar sind, sollte eine Institution auch die Reputation eines Cloud-Diensteanbieters in ihre Entscheidung einbeziehen. Dabei ist zusätzlich zu klären, ob es innerhalb der eigenen Institution bereits Erfahrungen mit einem Cloud-Diensteanbieter gibt oder ob auf Erfahrungen anderer Kunden mit ähnlichen Anforderungen zugegriffen werden kann. Eventuell sind Informationen darüber verfügbar, inwieweit der Service gegenüber anderen Kunden vertragstreu erbracht wurde.
- **Kerngeschäft des Anbieters** Es sollte kritisch hinterfragt werden, ob Cloud-Dienste das Kerngeschäft des Dienstleisters sind. Daneben sollte geprüft werden, inwieweit der Cloud-Diensteanbieter bereits eine gewisse Historie aufzuweisen hat, die auch auf eine möglichst hohe Zukunftssicherheit schließen lässt. Ein Cloud-Diensteanbieter, der erst seit kurzer Zeit am Markt ist und für den Cloud-Dienste nicht das Kerngeschäft sind, birgt unter Umständen ein erhöhtes Risikopotenzial. Die Gefahr, dass ein solcher Anbieter seine Dienstleistungen kurzfristig einstellt, sich stark verändert oder komplett vom Markt verschwindet, ist größer einzuschätzen als bei ausgewiesenen Cloud-Dienstleistern, die ihr Service-Angebot bereits über einen längeren Zeitraum aufrechterhalten und immer weiter ausbauen.
- **Öffentlich verfügbare Rankings oder Bewertungsmatrizen**Auch öffentlich verfügbare Rankings oder Bewertungsmatrizen, die von (unabhängigen) Dritten erstellt wurden, können zur Auswahl eines geeigneten Cloud-Diensteanbieters beitragen. Dabei ist darauf zu achten, dass die Bewertung möglichst objektiv und neutral erfolgt. Hier empfehlen sich Marktanalysen, die beschreiben, welcher Cloud-Diensteanbieter für welche Kundensituation am geeignetsten erscheint. In diesem Zusammenhang werden häufig Sicherheitsaspekte oder Kosten bewertet.
- **Due-Diligence-Prüfung**Bei entsprechendem Bedarf und sofern möglich, ist eine Due-Diligence-Prüfung (due diligence - gebotene Sorgfalt) ratsam. Hierbei sollten alle relevanten Parameter im Zusammenhang mit der Nutzung von Cloud-Diensten (zum Beispiel Sicherheitsaspekte, eingesetzte Technik, Schnittstellen und Prozesse) geprüft werden. Ziel der Prüfung ist, die Leistungsfähigkeit des Diensteanbieters zu ermitteln und zu klären, ob der Cloud-Diensteanbieter die Voraussetzungen für den gewünschten Service erfüllt.
- **Zugriffe durch den Diensteanbieter oder Dritte**Ein weiteres Auswahlkriterium für einen geeigneten Cloud-Diensteanbieter kann dessen Möglichkeit zum Zugriff auf Daten oder Verfahren der Institution darstellen. Unter Umständen will sich der Diensteanbieter ein solches Zugriffsrecht für sich oder Dritte einräumen lassen, was in der Regel aber den Anforderungen an den Cloud-Dienst widerspricht. Darüber hinaus ist zu beobachten, dass Diensteanbieter Subunternehmer beauftragen, die in der Folge auf Kundendaten zugreifen können.
- **Installation bestimmter Softwarelösungen**In einigen Fällen wird die vorherige Installation einer bestimmten Software-Lösung auf den IT-Systemen der Institution vorausgesetzt, um den Clound-Dienst zu nutzen. Hier empfiehlt es sich zu hinterfragen, welche potenziellen Sicherheitsrisiken bzw. -erfordernisse damit einhergehen. Möglicherweise ergeben sich Kompatibilitätsprobleme oder es entstehen zusätzliche Kosten, die nicht auf den ersten Blick ersichtlich sind. Zudem entsteht eine weitere Abhängigkeit vom Cloud-Diensteanbieter.
- **Standorte des Cloud-Diensteanbieters**Auch der Sitz des Cloud-Diensteanbieters (und die damit einhergehende Jurisdiktion), die Standorte der von ihm betriebenen oder genutzten Rechenzentren sowie die Sitze und Standorte für den Service beauftragen Subunternehmen können für eine Institution von entscheidender Bedeutung sein. Der mögliche Ort der Leistung kann durch Compliance-Vorgaben eingeschränkt sein. Abhängig von der Standortwahl des Diensteanbieters unterliegt dieser gegebenenfalls staatlichen Eingriffs- und Einsichtsrechten. Denkbar sind hier ebenfalls existierende Prüfpflichten zu gespeicherten Daten, denen der Diensteanbieter nachkommen muss, oder auch gerichtlich einklagbare Einsichtsrechte Dritter.
- **Subunternehmen zur Service-Erbringung**Häufig wird ein Cloud-Dienst mithilfe von Subunternehmen betrieben. Unstimmigkeiten zwischen den Vertragspartnern oder unzuverlässige Subunternehmer können sich nachteilig auf die Leistungsfähigkeit des Cloud-Diensteanbieters auswirken. In der Regel ist die Beteiligung von Subunternehmen wesentlich stärker ausgeprägt, als dies beispielsweise beim Outsourcing der Fall ist. Bei der Auswahl eines Cloud-Diensteanbieters sollten daher auch die Subunternehmen betrachtet werden.
- **Berücksichtigung vertraglicher Regelungen**Bereits bei der Auswahl eines Cloud-Diensteanbieters sollten dessen vertragliche Regelungen berücksichtigt werden. Besteht ein Cloud-Diensteanbieter beispielsweise auf Vertragsbestandteilen, die durch die nutzende Institution nicht zu akzeptieren sind, sollte der entsprechende Cloud-Diensteanbieter als potenzieller Vertragspartner ausscheiden. Weitere Informationen zu vertraglichen Regelungen sind in OPS.2.2.M9 *Vertragsgestaltung mit dem Cloud-Diensteanbieter* beschrieben.

Durchführung einer Kosten-Nutzen-Analyse

Die konkreten Angebote einiger Cloud-Diensteanbieter ermöglichen es, eine Kosten-Nutzen-Analyse durchzuführen. Sie ist für jeden definierten Cloud-Dienst zu realisieren. Der Fokus sollte dabei auf der Ermittlung der realistischen Kosten liegen. In der Praxis ist zu beobachten, dass im Verlauf der Service-Definition die gestellten Anforderungen an den zu nutzenden Cloud-Dienst, beispielsweise in Form konkreter SLAs, stetig wachsen. Häufig wird dabei jedoch der Einfluss solcher Leistungsmerkmale auf die Kosten eines Services unterschätzt oder gänzlich aus den Augen verloren.

Die Kosten-Nutzen-Analyse liefert einer Institution in diesem Fall Aufschlüsse über ein sinnvolles Verhältnis zwischen dem potenziellen Mehrwert zusätzlicher Anforderungen und den sich daraus ergebenden Kosten. Sind bei dem definierten Cloud-Dienst die Kosten höher als der Nutzen, sollte die Service-Definition überdacht und eventuell angepasst oder auf den Cloud-Dienst verzichtet werden.

Bei den Kosten ist zwischen Investitionskosten (Capex - capital expenditure) und Kosten für den operativen Geschäftsbetrieb (Opex - operational expenditure) zu unterscheiden. Bei der Nutzung von Cloud-Diensten entstehen zunächst zusätzliche Kosten, da der Aufwand für vorhandene Services und die dafür benötigte Infrastruktur nicht sofort wegfällt. So übernehmen beispielsweise die Mitarbeiter einer Institution neue Aufgaben, für die sie zusätzlich geschult werden müssen. Auch sind weitere organisatorische Anpassungen innerhalb der nutzenden Institution notwendig. Diese Kosten müssen ebenso in die Analyse des Kosten-Nutzen-Verhältnisses einbezogen werden, wie die in der Regel verbrauchsorientierten Nutzungskosten für einen Cloud-Dienst.

Auf diesem Weg soll sichergestellt werden, dass die potenzielle Ersparnis durch Cloud-Dienste realistisch betrachtet wird.

Mögliche Fallstricke bei der Auswahl eines Cloud-Diensteanbieters

In der Praxis zeigt sich oft, dass Anwender zwar über ein grundsätzliches Verständnis von Maßnahmen zur geeigneten Auswahl eines Cloud-Diensteanbieters verfügen, sie aber dennoch an häufig wiederkehrenden Fallstricken scheitern. Auf die nachfolgend beschriebenen Aspekte sollte daher, abhängig von den Anforderungen der Institution, ein besonderes Augenmerk gelegt werden. Sie sind allerdings nur unterstützende Hinweise für den Anwender, eine vollständige Umsetzung ist nicht notwendig.

Prüfung der vertraglichen Grundlagen

Die Nutzungsbedingungen, Geschäftsbedingungen oder sonstige vertragliche Grundlagen des Cloud-Diensteanbieters, die bereits vor dem eigentlichen Vertragsabschluss vorliegen, sollten umfassend geprüft werden. Häufig verbergen sich hier hinter unverständlichen, unübersichtlichen, auffallend umfangreichen oder intransparenten Unterlagen nachteilige Regelungen für den Anwender.

Service-Beschreibungen

Die verfügbaren Service-Beschreibungen des Cloud-Diensteanbieters sollten sorgfältig geprüft und hinterfragt werden. Es ist zu klären, wie die darin enthaltenden Angaben zu verstehen sind. Bei Unklarheiten oder Unsicherheiten sollte der entsprechende Cloud-Diensteanbieter direkt kontaktiert werden. Häufig ist zu beobachten, dass Anwender Leistungen voraussetzen, die vom Cloud-Diensteanbieter nicht oder lediglich als kostenpflichtige Zusatzleistung erbracht werden.

Beispiel:

- Der Anwender beauftragt einen Online-Speicher, den er für Daten einsetzen möchte, die häufigen Änderungen unterliegen. In der zugehörigen Service-Beschreibung des Cloud-Diensteanbieters wird das Backup der Daten als Inklusiv-Leistung beschrieben. Da der Anwender in seiner eigenen Institution täglich ein Backup der Daten vornimmt, setzt er diesen Backup-Zyklus auch beim beauftragten Diensteanbieter als Standard voraus. Der Cloud-Diensteanbieter bietet tatsächlich aber nur ein wöchentliches Backup an. Für einen kürzeren Backup-Zyklus fallen zusätzliche Kosten an.

Erwartete und tatsächliche Leistung

Ein Cloud-Diensteanbieter muss Gewinne erwirtschaften und deswegen seine Services möglichst kostengünstig erbringen. Unter Umständen widerspricht das jedoch den Erwartungen des Auftraggebers (hohe Dienstleistungsqualität, Flexibilität, Kundenfreundlichkeit, Sicherheitsniveau etc.).

Insbesondere bei Cloud-Nutzung ist jedoch häufig zu beobachten, dass IT-Verantwortliche die Werbeaussagen des Dienstleisters nicht hinterfragen. Missverständnisse hinsichtlich erwarteter und tatsächlich erbrachter Leistungen, die häufig nur mit zusätzlichen Kosten zu beheben sind, stellen sich daher oft erst im laufenden Betrieb heraus.

Deshalb sollten die Verantwortlichen innerhalb einer Institution bereits vorab eine Vergleichsrechnung durchführen, die Aufschluss darüber gibt, zu welchen Kosten ein Dienstleister die vereinbarte Leistung erbringen muss, damit sowohl Auftraggeber als auch Auftragnehmer von einem Vertragsverhältnis profitieren. Das Ergebnis der Berechnung ist dann eventuell, dass eine seriöse Leistung zu den angebotenen günstigen Konditionen nicht als realistisch angesehen werden kann.

Standardisierte SLA-Beschreibungen

Standardisierte SLA-Beschreibungen des Cloud-Diensteanbieters, die nicht individuell vereinbart werden, sollten bereits bei der Auswahl eines Cloud-Diensteanbieters sorgfältig hinsichtlich ihres Inhaltes und ihrer Aussagekraft untersucht werden. Häufig sind unklare Beschreibungen innerhalb von SLAs vorzufinden. Dies kann im laufenden Betrieb zu Unstimmigkeiten und Störungen führen. Sofern keine SLA-Beschreibungen vorliegen, sollten Institutionen die verfügbaren AGBs auf ähnliche Weise prüfen und eventuell mit konkreten Fragen an den Cloud-Diensteanbieter herantreten.

Beispiel:

- Ein Cloud-Diensteanbieter garantiert innerhalb des SLAs eine Serviceverfügbarkeit von 99,5 %, spezifiziert diese Zahl aber nicht genauer. Für den Anwender ist nicht transparent, was sie bedeutet. Der Service dürfte nach diesem SLA zwei Tage am Stück ausfallen, was einer für den Anwender maximal tolerierbaren Ausfallzeit von vier Stunden entgegenstehen würde.

Außendarstellung zur Leistungsfähigkeit des Cloud-Diensteanbieters

Die Außendarstellung zur Leistungsfähigkeit eines Cloud-Diensteanbieters ist kritisch zu betrachten und im Zweifelsfall durch individuelle Kontrollen zu überprüfen. Cloud-Nutzung wird nach wie vor als Trend-Thema angesehen. Verantwortliche in Institutionen sehen sich daher aus unterschiedlichen Gründen unter Umständen dazu verleitet, die Werbeversprechen von Cloud-Diensteanbietern nicht in ausreichendem Maße kritisch zu hinterfragen. Anwender gewinnen so eventuell einen falschen Eindruck davon, wer sich tatsächlich hinter dem Cloud-Diensteanbieter verbirgt und hinterfragen dessen getroffene Aussagen zur eigenen Leistungsfähigkeit nicht ausreichend.

Legt eine Institution bei der Auswahl ihres Cloud-Diensteanbieters besonderen Wert darauf, dass Zertifizierungen vorhanden sind, sollten auch diese näher hinterfragt werden. Häufig sind Zertifizierungen (zum Beispiel nach ISO/IEC 27001, ISO 9001 etc.) zwar grundsätzlich vorhanden, werden aber nicht regelmäßig aktualisiert und sind daher nicht mehr gültig oder der Scope deckt den betroffenen Service nicht ab. Auch sind der Inhalt und Umfang zu hinterfragen und gegebenenfalls weitere Informationen vom Cloud-Diensteanbieter zu fordern. Als zuverlässig sind Zertifizierungen nach IT-Grundschutz auf Basis von ISO 27001 anzusehen.

Kundenfreundlichkeit

Verwendet der Cloud-Diensteanbieter in seiner Leistungsbeschreibung unklare Definitionen und ist nicht willens oder in der Lage, diese verständlich zu erläutern, sollte die Institution prüfen, ob er ein geeigneter Vertragspartner für den geplanten Cloud-Dienst ist.

OPS.2.2.M9 Vertragsgestaltung mit dem Cloud-Diensteanbieter

Hat die Institution einen geeigneten Cloud-Diensteanbieter ausgewählt, sollten alle relevanten Aspekte der geplanten Cloud-Nutzung vertraglich in Service Level Agreements festgehalten und geregelt werden. Dabei sollten Art, Umfang und Detaillierungsgrad der vertraglichen Regelungen dem Schutzbedarf der Informationen angepasst werden, die im Zusammenhang mit der Cloud-Nutzung stehen.

Bei der Vertragsgestaltung mit dem Cloud-Diensteanbieter sind viele unterschiedliche Themen zu betrachten. Es ist darauf zu achten, dass alle zuvor definierten Anforderungen auch im Vertrag mit dem Cloud-Diensteanbieter berücksichtigt werden. Grundsätzlich sollten sich die vertraglichen Regelungen zumindest an den nachfolgend beschriebenen Punkten orientieren.

Ort der Leistungserbringung durch den Cloud-Diensteanbieter

Es ist festzuhalten, an welchen Standorten ein Cloud-Diensteanbieter die beauftragten Cloud-Dienste erbringt, zum Beispiel national oder innerhalb der Europäischen Union. Wenn notwendig, können auch explizit bestimmte Rechenzentren festgelegt werden.

An der Erbringung des Dienstes beteiligte Subunternehmer oder andere Dritte

Sofern Subunternehmer an der Dienste-Erbringung beteiligt sind bzw. der Cloud-Dienst auf anderen Cloud-Diensten basiert, ist dies unter Angabe der beteiligten Dritten vertraglich festzuhalten. Änderungen müssen dem Cloud-Anwender mitgeteilt werden. Bei kritischen Diensten muss zudem ein außerordentliches Kündigungsrecht eingeräumt werden.

Regelungen hinsichtlich der Infrastruktur des Cloud-Diensteanbieters

Im Vertrag sollte festgehalten werden, wie der Cloud-Diensteanbieter die vorhandene Infrastruktur absichern muss und welche Maßnahmen zur Ausfallsicherheit er umzusetzen hat. Auch Vorgaben zur Umsetzung einer mandantenfähigen Infrastruktur durch den Cloud-Diensteanbieter sollten vertraglich geregelt werden. Gegebenenfalls kann dies mithilfe von Zertifizierungen nachgewiesen werden.

Regelungen hinsichtlich des Personals beim Cloud-Diensteanbieter

Sofern die nutzende Institution besondere Anforderungen an Fähigkeiten, Qualifikationen und Zertifizierungen des Personals beim Cloud-Diensteanbieter stellt, sind diese vertraglich festzulegen. Dabei sind unter anderem folgende Aspekte denkbar:

- Regelungen zum Vorgehen des Cloud-Diensteanbieters bei der Einstellung von Administratoren oder anderen Mitarbeitern mit Zugriffsrechten auf Kundendaten. Bei Vertragspartnern mit Standorten in mehreren Ländern sollte sichergestellt sein, dass unabhängig vom Einsatzort des Mitarbeiters die gleichen Kriterien (zum Beispiel hinsichtlich Aus- und Weiterbildung, benötigten Zertifikaten oder Sprache) angesetzt werden.

Weiterhin sind folgende Themen hinsichtlich des Personals zu regeln:

- Vorgaben zu notwendigen Schulungen zur Informationssicherheit durch den Cloud-Diensteanbieter.
- Sofern dies als erforderlich angesehen wird, kann ein Nachweis der Sicherheitsüberprüfung von Mitarbeitern eingefordert werden.
- Vorgaben zur regelmäßigen Beurteilung des Personals, um das erforderliche Qualitätsniveau dauerhaft gewährleisten zu können.

Regelungen zu Kommunikationswegen und Ansprechpartnern

Es sind klare Verantwortlichkeiten, Eskalationsstufen und Kommunikationswege zwischen der beauftragenden Institution und dem Cloud-Diensteanbieter zu definieren. Die Kommunikationssprache ist festzulegen. Es ist insbesondere darauf zu achten, dass Regelungen zu Ansprechpartnern im Notfall, zum Sicherheitsvorfall-Management und zur Fehlerbehebung getroffen werden. Je nach Anforderungen des Auftraggebers sind hier explizit Telefonnummern, Kontaktpersonen sowie Erreichbarkeitszeiten anzugeben.

Regelungen zu Prozessen, Arbeitsabläufen und Zuständigkeiten

Folgende Themen sollten vertraglich vereinbart werden:

- Vorgaben zur Durchführung regelmäßiger Security-Monitoring-Aktivitäten,
- Vorgaben zum Incident Handling,
- Vorgaben zur Durchführung regelmäßiger Abstimmungsrunden,
- Vorgaben zum Änderungsmanagement beim Cloud-Diensteanbieter,
- Vorgaben zu den Fernzugangsrichtlinien des Cloud-Diensteanbieters,
- Umzusetzende Maßnahmen zum Schutz gegen Schadprogramme,
- Detaillierte Dokumentation des Backup- und Recovery-Prozesses,
- Einräumung des Rechts zur eigenen Datensicherung durch die nutzende Institution (soweit dies beim angebotenen Dienst möglich ist),
- Bereitstellung von verschlüsselten Transportwegen sowie
- Mitwirkungspflichten des Cloud-Anwenders.

Regelungen zur Beendigung des Vertragsverhältnisses

Es sind unter anderem Regelungen zu treffen, wie der Cloud-Diensteanbieter die Daten zurückgeben muss. Weiterführende Informationen zu umzusetzenden Maßnahmen, für den Fall, dass das Vertragsverhältnis beendet wird, sind OPS.2.2.M14 *Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses* zu entnehmen.

Sicherstellung der Datenlöschung beim Cloud-Diensteanbieter

Es sind Vereinbarungen darüber zu treffen, was unter der Löschung von Daten zu verstehen ist und was die vollständige Löschung der Daten beinhaltet. Hierbei kann beispielsweise unterschieden werden zwischen Tags entfernen und Daten (mehrfach) zu überschreiben.

Weiterhin sind Vereinbarungen darüber zu treffen, welches Sicherheitsniveau bei der Datenlöschung durch den Cloud-Diensteanbieter zu erzielen ist und ob unterschieden werden soll zwischen einer Datenlöschung im regulären Betrieb und einer bei Vertragsbeendigung. Hierfür bietet es sich an, den notwendigen Aufwand zur Wiederherstellung der Daten als Maßstab heranzuziehen. In den meisten Fällen sollte ein Sicherheitsniveau angestrebt werden, bei dem Daten auch mithilfe professioneller Recovery-Tools nicht mehr wiederhergestellt werden können. Sofern höhere Anforderungen an das Sicherheitsniveau der Datenlöschung, beispielsweise die Zerstörung der Datenträger nach DIN-Norm 66399, existieren, ist bereits vorher zu klären, ob diese durch den Cloud-Diensteanbieter tatsächlich erfüllt werden können (siehe hierzu auch OPS.2.2.M8 *Sorgfältige Auswahl eines Cloud-Diensteanbieters*).

Außerdem ist zu klären, wie die sichere Löschung von Daten durch den Cloud-Diensteanbieter gegenüber dem Kunden nachgewiesen wird.

Das Thema sicheres Löschen in modernen Speicherlösungen ist im Baustein SYS.1.8 *Speicherlösungen* beschrieben. Hier können sowohl Anwender als auch Cloud-Diensteanbieter Hilfestellung hinsichtlich des zu erzielenden Sicherheitsniveaus finden.

Regelungen zu Zutritts- und Zugriffsberechtigungen

Sofern sich eine solche Anforderung aus den vorangegangenen Betrachtungen der Institution ergibt, ist hier beispielsweise eine Regelung denkbar, die Zugriffsberechtigungen ausschließlich auf speziell überprüftes Personal beschränkt. Weiterhin sind Vorgaben zu umzusetzenden Sicherheitsmaßnahmen in den Rechenzentren des Cloud-Diensteanbieters festzuhalten.

Regelungen zur Notfallvorsorge

Es sollte vertraglich geregelt werden, dass der Cloud-Diensteanbieter Notfallpläne vorhält und diese von der Institution eingesehen werden können.

Abhängig von den Verfügbarkeitsanforderungen der Anwender sind Dringlichkeitsstufen festzulegen, garantierte Reaktionszeiten im Notfall zu vereinbaren sowie Notfallübungen beim Cloud-Diensteanbieter zu fordern.

Regelungen zu rechtlichen Rahmenbedingungen

Folgende Themen sind zu betrachten:

- Verpflichtung des Cloud-Diensteanbieters geltende Normen und Gesetze in Abhängigkeit des Standortes und der relevanten Branche einzuhalten.
- Regelungen zur Einbindung Dritter. Der Cloud-Diensteanbieter sollte verpflichtet werden, transparent zu agieren. Services, welche die Service Delivery Supply Chain betreffen, die Sicherheit (zum Beispiel die Verfügbarkeit) gefährden und durch Subunternehmer erbracht werden, sind offenzulegen. Darüber hinaus ist festzuhalten, dass SLAs, die Subunternehmer dem Cloud-Diensteanbieter bieten, nicht geringer sein sollten als jene, die der Cloud-Diensteanbieter seinen Kunden bietet. Der Cloud-Diensteanbieter sollte über Methoden verfügen, die ihn befähigen, den tatsächlichen Service-Level seiner Subunternehmer zu überprüfen. Zudem ist vertraglich zu regeln, dass Sicherheitsrichtlinien und Kontrollen auch von Dritten angewendet werden.Beispiel:Eine Institution schließt mit einem Cloud-Diensteanbieter einen Vertrag zur Nutzung eines definierten Cloud-Dienstes. Der gewählte Cloud-Diensteanbieter nutzt zur Leistungserbringung seinerseits Dienste eines Subauftragnehmers und gibt die Daten der Institution zur Verarbeitung an diesen weiter. Alle Kommunikationswege sowie die Art und der Umfang der weitergegebenen Daten sind in diesem Fall durch den Cloud-Diensteanbieter transparent darzulegen.

- Vorgaben zur Beendigung der Cloud-Nutzung, zum Beispiel Kündigungsregelungen
- Vertraulichkeitsvereinbarungen
- Vereinbarung von Vertragsstrafen
- Festlegung von Haftungsfragen
- Gerichtsstand und anwendbares Recht auch hinsichtlich geltender Datenschutzbestimmungen

Festlegungen zum Änderungsmanagement und zu Testverfahren

In Bezug auf das Änderungsmanagement und die Umsetzung von Testverfahren ist festzulegen, inwiefern flexible Anpassungsmöglichkeiten gegeben sind. Das ist insbesondere bei gesetzlichen Änderungen oder gestiegenen Anforderungen relevant.

Regelungen zur Durchführung von Kontrollen

Es sollte schriftlich bestätigt werden, dass Audits durch Dritte akzeptiert sowie Penetrationstests erlaubt sind. Dabei muss auch vereinbart werden, wer die Kosten für ein Audit trägt. Darüber hinaus ist festzulegen, wie mit den Audit-Logs des Cloud-Diensteanbieters umzugehen ist. Folgende Themen sollten hier betrachtet werden:

- Vorgaben zur Aufbewahrungsfrist für Log-Daten,
- Wirksame Kontrollen zum Schutz von Logs vor nicht autorisiertem Zugriff,
- Methoden zur Überprüfung und Sicherung der Integrität von Audit-Logs,
- Durchführung von Audit-Log-Reviews sowie
- Vorgaben zur Zeitquelle, die genutzt wird, um Systeme zu synchronisieren und einen exakten Zeitstempel für Audit-Logs anzubieten.

Weiterhin sollte vertraglich geregelt werden, wie kontrolliert wird, ob die SLAs eingehalten werden. Auch ist sicherzustellen, dass der Cloud-Diensteanbieter regelmäßig über anstehende Änderungen informiert, zum Beispiel bezüglich Funktionsumfang, Subunternehmer und sämtliche für das SLA relevanten Ereignisse.

Berücksichtigung besonderer Anforderungen

Manchmal stellen Institutionen besondere Anforderungen an einen Cloud-Dienst. Diese sollten ebenfalls im Vertrag festgehalten werden. Denkbar sind beispielsweise folgende Anforderungen:

- Nutzung von ausschließlich vorab definierten Rechenzentren
- Regelungen zum Import bzw. Export von Daten sowie zu benötigten Schnittstellen zu anderen Services und Systemen
- Festlegung der konkreten Konfigurationsparameter bezüglich definierter Interoperabilitätsanforderungen
- Einräumen des Rechts eigene Datensicherungen durchzuführen und notwendige Schnittstellen und Parameter zu erfassen.

OPS.2.2.M10 Sichere Migration zu einem Cloud-Dienst

Hat die Institution einen Cloud-Dienst ausgewählt, müssen bei der Migration verschiedene Sicherheitsaspekte betrachtet werden. Die Vorgaben zur sicheren Migration sollten auch angewendet werden, wenn ein Cloud-Dienst wieder zurück in die eigene Institution geholt oder er an einen anderen Anbieter übertragen wird.

Grundlegende Aspekte der Planung einer sicheren Migration zu einem Cloud-Dienst werden ausführlich in OPS.2.2.M5 *Planung der sicheren Migration zu einem Cloud-Dienst* beschrieben. Da die Zielinfrastruktur für einen Cloud-Dienst meistens durch den Cloud-Diensteanbieter bereitgestellt wird, ist diese nicht Gegenstand der Betrachtungen zur Migrationsumsetzung.

Durchführung der Migration

Die Migration erfolgt auf Basis des Migrationskonzeptes (siehe OPS.2.2.M5 *Planung der sicheren Migration zu einem Cloud-Dienst),* das die technischen sowie organisatorischen Voraussetzungen beschreibt. Während der Migration sind die Vorgaben des Migrationskonzeptes mit den tatsächlichen Gegebenheiten der Institution abzugleichen. Wenn es Abweichungen gibt, müssen diese erfasst und dokumentiert werden. In diesem Fall sind Maßnahmen zu ergreifen, um den im Migrationskonzept definierten Zustand herzustellen.

Auch das Sicherheitskonzept (siehe OPS.2.2.M7 *Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung*) ist während der Migration auf notwendige Anpassungen zu prüfen und gegebenenfalls zu aktualisieren. Um während der Einführungsphase das definierte Sicherheitsniveau kontinuierlich zu gewährleisten, sollten folgende sicherheitsrelevante Aspekte besonders beachtet werden:

- Um die Übertragung von Daten der Institution zu einem Cloud-Diensteanbieter vornehmen zu können, sind eventuell privilegierte Zugriffsrechte notwendig. Um das angestrebte Sicherheitsniveau gewährleisten zu können, ist sicherzustellen, dass die Zugriffsrechte ausschließlich gemäß den Planungsvorgaben vergeben werden. Auch müssen sie wieder entzogen werden, nachdem die Migration abgeschlossen ist.
- Wird die Migration durch einen externen Dritten geplant und durchgeführt und werden bei der Migrationsplanung besondere Regelungen aufgestellt, so ist deren Einhaltung zu prüfen.
- Im Falle einer fehlgeschlagenen oder abgebrochenen Migration ist sicherzustellen, dass die bereits übermittelten Daten vom Cloud-Diensteanbieter sicher gelöscht werden.

Bevor die ersten Daten einer Institution an den Cloud-Diensteanbieter übermittelt werden, sind zusätzlich alle Maßnahmen zur Notfallvorsorge zu prüfen. Sie müssen vollständig und aktuell sein. Gegebenenfalls müssen daraufhin Fallback-Szenarien angepasst werden, um im Notfall die Daten wieder aus der Cloud zurückholen zu können. Regelungen, wie die Institution mit einer abgebrochenen Datenübertragung umzugehen hat, sind auf deren Anwendbarkeit und Einhaltung hin zu überprüfen. Auch wenn bereits ein Teil der Daten migriert wurde und alle notwendigen Voraussetzungen zur Nutzung des Cloud-Dienstes geschaffen sind, sollten die Daten von der Institution kontinuierlich gesichert werden. Während der Migration sollte regelmäßig kontrolliert werden, dass die Daten ordnungsgemäß gesichert wurden.

Durchführung der Migration im Rahmen eines Testbetriebs

Damit der Übergang zu einem Cloud-Dienst möglichst reibungslos funktioniert und der laufende Betrieb nicht beeinträchtigt wird, sollte die Migration zunächst in einem Testbetrieb erfolgen. So lässt sich prüfen, ob alle Planungen und Vorgaben umsetzbar sind. Eventuell kann bereits zu diesem Zeitpunkt zusätzlicher Nachbesserungs- oder Entwicklungsbedarf identifiziert werden.

Während des Testbetriebs sollten, sofern möglich und sinnvoll, Leistungsmessungen vorgenommen werden, um diese mit den geforderten Leistungswerten zu vergleichen. So kann festgestellt werden, ob sich der geplante Migrationsweg grundsätzlich als umsetzbar erweist. Zudem ist erkennbar, ob die geplante Übertragungskapazität ausreicht und ob sich der zeitgleiche Umzug der festgelegten Anzahl an Datensätzen wie geplant realisieren lässt.

Durchführung der Migration innerhalb einer Pilotphase

Abhängig vom Umfang der angestrebten Cloud-Nutzung wird nach erfolgreich abgeschlossenem Prozesse und IT-Systeme und Anwendungen Testbetrieb der Übergang in eine Pilotphase empfohlen.

Ziel der Pilotphase ist es, zu testen, ob der Cloud-Dienst im produktiven Betrieb den zuvor definierten Anforderungen der Institution gerecht wird. Hierbei ist noch einmal zu überprüfen, ob alle Zusagen und Vereinbarungen mit dem Cloud-Diensteanbieter auch eingehalten werden.

Die Pilotphase dient in der Regel auch dazu, dass sich Service-Administratoren auf der Anwenderseite zunehmend mit dem neuen Dienst vertraut machen können. Die Service-Administratoren sollten ihre Erfahrungen entsprechend dokumentieren, um daraus eventuell zusätzliche Schulungsinhalte für zukünftiges Personal ableiten zu können.

Übergang in den Produktionsbetrieb

Sind der Testbetrieb und die Pilotphase positiv verlaufen, erfolgt anschließend die Migration und damit die Überführung des Cloud-Dienstes in den produktiven Betrieb. Dabei sind die zwischen Institution, Cloud-Diensteanbieter und gegebenenfalls externem Migrations-Dienstleister getroffenen Regelungen gemäß den Übergabeprozessen zu berücksichtigen.

OPS.2.2.M11 Erstellung eines Notfallkonzeptes für einen Cloud-Dienst

Ein Notfallkonzept für die internen Prozesse bei Cloud-Nutzung ist eine wichtige Maßnahme zur Notfallvorsorge. Im Rahmen des Notfallkonzeptes sollten sowohl organisatorische als auch technische Aspekte thematisiert werden.

Organisatorische Aspekte der Notfallvorsorge bei Cloud-Nutzung

Das Notfallkonzept sollte alle notwendigen Angaben zu Zuständigkeiten und Ansprechpartnern enthalten, um im Notfall schnell reagieren zu können. Alle vorgesehenen Abläufe müssen klar geregelt und vollständig dokumentiert werden.

Es sind Detailregelungen für die Datensicherung zu erstellen, da diese im Notfall besonders wichtig ist. Hier sind beispielsweise Vorgaben hinsichtlich getrennter Backup-Medien für jeden Cloud-Dienst-Anwender, Anforderungen an die Verfügbarkeit, Vertretungsregelungen, Eskalationsstrategien sowie Maßnahmen zum Virenschutz denkbar.

Ebenfalls müssen detaillierte Arbeitsanweisungen erstellt werden. Diese sollten konkrete Anordnungen für bestimmte Fehlersituationen enthalten.

Darüber hinaus ist durch die Institution ein Konzept für regelmäßig durchzuführende Notfallübungen zu erarbeiten. Sollte es der genutzte Cloud-Dienst beziehungsweise der damit abgebildete Geschäftsprozess erforderlich machen, ist zu entscheiden und festzuhalten, inwieweit gemeinsame Notfallübungen mit dem Cloud-Diensteanbieter vorgesehen sind.

Technische Aspekte der Notfallvorsorge bei Cloud-Nutzung

Im Rahmen der Notfallvorsorge sind neben den organisatorischen Aspekten auch technische Anforderungen zu dokumentieren. Besonders wichtig ist es, dass die Management-Tools verfügbar sind, die benötigt werden, um Cloud-Dienste nutzen zu können. Daher sind diese in der Regel redundant auszulegen beziehungsweise auf redundanter Infrastruktur aufzubauen. Auch die benötigten Schnittstellensysteme sollten redundant vorliegen. Darüber hinaus sollte das Notfallkonzept Angaben darüber beinhalten, wie eine ausfallsichere Anbindung an den Cloud-Diensteanbieter gewährleistet werden kann.

Wenn ein Notfallkonzept für die Cloud-Nutzung erstellt wird, gilt es zu beachten, dass der Schutzbedarf für die Anbindung und die Schnittstellensysteme verglichen mit den bisherigen Anforderungen der Institution höher sein kann. Ursache hierfür ist die Nutzung von Cloud-Diensten für kritische Geschäftsprozesse.

OPS.2.2.M12 Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb

Nach der erfolgreichen Migration zu einem Cloud-Dienst muss gewährleistet werden, dass die Informationssicherheit im laufenden Betrieb aufrechterhalten wird. Hierzu sind eine Reihe von Maßnahmen zu ergreifen, die im Folgenden näher beschrieben sind.

Alle nötigen Dokumentationen und Richtlinien müssen regelmäßig aktualisiert werden, z. B. Betriebshandbücher, Nutzungsanweisungen oder Anleitungen.

Weiterhin ist sicherzustellen, dass regelmäßige Kontrollen durchgeführt werden, die sich über möglichst viele Bereiche der Cloud-Nutzung erstrecken. Es sind zumindest folgende Aspekte zu betrachten und regelmäßig zu kontrollieren:

- Sicherstellung der ordnungsgemäßen Administration von Cloud-Diensten In den Bausteinen ORP.3 *Sensibilisierung und Schulung* und OPS.1.1.2 *Ordnungsgemäße IT-Administration* werden grundlegende Vorgaben zu den Anforderungen an Administratoren beschrieben. Es ist sicherzustellen, dass alle Administratoren von Cloud-Diensten diese Anforderungen kennen und dazu befähigt werden, sie zu erfüllen. Regelmäßige Reviews der vergebenen Berechtigungen können ebenfalls die ordnungsgemäße Administration von Cloud-Diensten sichern. Sofern dies im Rahmen der Planungsmaßnahmen als notwendig angesehen und dokumentiert wurde, ist an dieser Stelle auch darauf zu achten, dass das 4-Augen-Prinzip eingehalten wird.

- **Regelmäßige Kontrolle der Dienst-Erbringung** In diesem Bereich sind die für die Dienst-Erbringung unabdingbaren Parameter zu überprüfen, zum Beispiel Verfügbarkeit, maximale Anzahl gleichzeitiger Benutzer, Schnelligkeit der Einrichtung neuer Benutzer oder neuer Ressourcen. Hinzu kommen weitere Parameter, die Leistungen der eigenen Institution oder von Dritten beschreiben, wie beispielsweise die Performance der Netzanbindung und -verbindungen.

- **Regelmäßige Service-Reviews zwischen Cloud-Diensteanbieter und Anwender**Es sollten regelmäßig Service-Reviews zwischen dem beauftragten Cloud-Diensteanbieter und der Institution stattfinden. Dabei sollten die vereinbarten und die tatsächlich erreichten Service-Level gegenübergestellt werden. Die Behandlung von Ausnahmesituationen, wie beispielsweise eines groß angelegten Angriffs oder eines globalen Netzausfalls, sollte ebenfalls Inhalt der Reviews sein. Regelmäßige Service-Reviews unter Beteiligung von Auftraggeber und Auftragnehmer sind in der Praxis allerdings nicht für jeden Cloud-Dienst umsetzbar. Das Service-Review kann daher auch zunächst vom Auftraggeber allein vorgenommen werden. Bei ermittelten Problemen oder bei hohem Schutzbedarf sollte sich der Dienstleister aber in jedem Fall mit der auftraggebenden Institution abstimmen.

- Sicherstellung der Interoperabilität von Cloud-DienstenBei Nutzung mehrerer Cloud-Dienste sollten Interoperabilitätstests durchgeführt werden.

- Erbringung von Sicherheitsnachweisen durch den Cloud-Diensteanbieter Die Institution sollte regelmäßig die vorhandene Dokumentation aufseiten des Cloud-Diensteanbieters zur Einsicht einfordern. Ebenso sollte der Cloud-Diensteanbieter in der Lage sein, Nachweise über die Zertifizierung von internen Kontrollsystemen für seine Prozesse und Services zu erbringen, sofern dies vertraglich vereinbart ist.
- Ordnungsgemäße Durchführung von Datensicherungen
- Sicherstellung der Einhaltung vorgesehener und vereinbarter Prozesse
- Kontrolle der technischen Maßnahmen zur Verhinderung der Nutzung nicht erlaubter Services, beispielsweise mithilfe von Proxys
- Durchführung von Audits, Sicherheitsprüfungen, Penetrationstests oder Schwachstellenanalysen

Neben den bereits beschriebenen Maßnahmen können regelmäßige Abstimmungsrunden zwischen Cloud-Diensteanbieter und nutzender Institution die Informationssicherheit erhöhen. Als Themen dieser Runden bieten sich z. B. aktuelle Informationen bezüglich des Änderungsmanagements oder Personaländerungen an. Auch eine Diskussion über die Kundenzufriedenheit und mögliche Verbesserungspotenziale könnten Inhalte sein.

Weiterhin leisten Übungen und Tests einen wichtigen Beitrag zur Informationssicherheit. Dabei ist, mit Schwerpunkt auf der Kommunikation zwischen Institution und Cloud-Diensteanbieter, vor allem die Reaktion auf Systemausfälle (Teilausfall und Totalausfall) zu planen und zu überprüfen. Weiterhin müssen Planungen hinsichtlich des Wiedereinspielens von Datensicherungen vorgenommen und dokumentiert werden. Generell sind Vorgaben zum Sicherheitsvorfallsmanagement bei der Cloud-Nutzung festzuhalten.

OPS.2.2.M13 Nachweis einer ausreichenden Informationssicherheit bei der Cloud-Nutzung

Ein Bestandteil jedes erfolgreichen Informationssicherheitsmanagements ist die regelmäßige Überprüfung der etablierten Sicherheitsmaßnahmen und des Informationssicherheits-Prozesses. Cloud-Diensteanbieter müssen regelmäßig den IT-Sicherheitszustand ihrer Geschäftsprozesse, Dienste und ihrer Plattformen überprüfen und kontinuierlich verbessern und weiterentwickeln.

Erfahrungen aus der Praxis zeigen, dass Abweichungen zu vertraglichen Vereinbarungen häufig nur durch Audits aufgedeckt werden. Deswegen sollte die Institution regelmäßig überprüfen, ob der Cloud-Diensteanbieter die vereinbarten Sicherheitsanforderungen korrekt umsetzt. Dazu genügt es, wenn der Cloud-Diensteanbieter nachweisen kann, dass ein Audit der vereinbarten Leistungen basierend auf einem etablierten Regelwerk (z. B. ISO/IEC 27001, IT-Grundschutz, Anforderungskatalog Cloud Computing (C5), Cloud Controls Matrix der Cloud Security Alliance) durch einen unabhängigen Dritten stattgefunden hat. Entsprechende Nachweise sollten den Cloud-Kunden zur Verfügung gestellt werden. Die Institution sollte prüfen, ob der beschriebene Geltungsbereich und Schutzbedarf die genutzten Cloud-Dienste erfasst.

Setzt ein Cloud-Diensteanbieter Subunternehmer ein, um die Services zu erbringen, so entlässt ihn diesnicht von der Verpflichtung, die Sicherheit dieser Dienste zu überprüfen, da der Cloud-Diensteanbieter gegenüber seinen Kunden für die Gesamtsicherheit seines Angebots verantwortlich ist und dies nicht auf Subunternehmer übertragen kann. In einem solchen Fall muss der Cloud-Diensteanbieter die erforderlichen Nachweise aller notwendigen Sicherheitsprüfungen von seinen Subunternehmern einfordern. Generell sollten durchgeführte Audits so dokumentiert werden, dass es möglich ist, diese an seine Kunden weitergeben zu können, sowohl die Nachweise beim Cloud-Diensteanbieter selber als auch bei dessen Subunternehmen.

Bei einem Service, der in Form einer Private Cloud On-Premise erbracht wird, erfolgt die Überprüfung als internes Audit.

Um die Wirksamkeit vorhandener technischer Sicherheitsmaßnahmen zu überprüfen, sind Penetrationstests ein erprobtes und geeignetes Vorgehen. Sie dienen dazu, die Erfolgsaussichten eines vorsätzlichen Angriffs auf einen Informationsverbund oder ein einzelnes IT-System vorab einzuschätzen und daraus notwendige ergänzende Sicherheitsmaßnahmen abzuleiten, bzw. die Wirksamkeit von bereits umgesetzten Sicherheitsmaßnahmen zu überprüfen. Cloud-Diensteanbieter sollten für die von ihnen betriebenen Netze und IT-Systeme, Anwendungen regelmäßig Penetrationstests durchführen.

Generell sollten alle Formen von Sicherheitsprüfungen von Personen mit geeigneten Qualifikationen durchgeführt werden. Diese dürfen jedoch nicht an der Erstellung der geprüften Strategien und Konzepte beteiligt gewesen sein, um Betriebsblindheit und Konflikte zu vermeiden. Die Prüfer bzw. Auditoren müssen möglichst unabhängig und neutral sein.

OPS.2.2.M14 Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses [Fachverantwortliche, Institutionsleitung]

Die hier genannten Empfehlungen lassen sich in der Regel nur umsetzen, wenn bereits im Vertrag mit dem Cloud-Diensteanbieter alle relevanten Themen zum Vertragsende geregelt wurden.

Wird das Dienstleistungsverhältnis beendet, müssen die betroffenen Dienstleistungen, z. B. der IT-Betrieb, geordnet zurück in die eigene Verantwortung oder auf einen anderen Dienstleister übergehen. Es müssen für folgende Szenarien Vorkehrungen getroffen werden, damit durch das Vertragsende des Dienstleistungsvertrags die Geschäftstätigkeit der Institution nicht beeinträchtigt wird.

- Der Übergang auf einen anderen Dienstleister ist ein neues Cloud-Nutzungs-Vorhaben. Deswegen sind die Anforderungen dieses Bausteins entsprechend anzuwenden.
- Auch beim Insourcing sind die relevanten Anforderungen des Bausteins anzuwenden, sofern es sich um die Nutzung eines Cloud-Dienstes handelt. Für Strategie, Sicherheitskonzept für Insourcing, Migration und Notfallvorsorge gelten die gleichen Anforderungen wie bei einem klassischen Cloud-Nutzungs-Verfahren.

Folgende Gesichtspunkte sind zu beachten:

- Eigentumsrechte an Hard- und Software (Schnittstellenprogramme, Tools, Batchabläufe, Makros, Lizenzen, Backups) müssen geregelt werden.
- Die Weiterverwendung der vom Dienstleister eingesetzten Tools, Prozeduren, Skripte, Batchprogramme ist für den Fall der Beendigung des Dienstleistungsverhältnisses zu regeln.
- IT-Systeme, Anwendungen und Arbeitsabläufe müssen ausreichend dokumentiert sein.
- Alle notwendigen Daten müssen vom Dienstleister an den Auftraggeber übertragen beziehungsweise übergeben werden.
- Alle Datenbestände beim Dienstleister müssen sicher gelöscht werden.
- Interne oder externe Mitarbeiter, die Aufgaben des Dienstleisters übernehmen, müssen eingewiesen und geschult werden.
- Es ist empfehlenswert, vertraglich eine Übergangsfrist zu vereinbaren, in der der ehemalige Dienstleister noch für Rückfragen und Hilfestellungen zur Verfügung steht.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

OPS.2.2.M15 Portabilität von Cloud-Diensten (A)

Grundsätzlich ist der Wechsel von einem Cloud-Diensteanbieter zu einem anderen einfacher möglich als beispielsweise bei klassischen Outsourcing-Vorhaben. In der Praxis zeigt sich jedoch, dass auch bei Cloud-Diensten häufig Probleme auftreten, wenn diese zu einem anderen Cloud-Diensteanbieter übertragen oder zurück in die eigene Institution geholt werden sollen. Institutionen sollten daher zusätzliche Maßnahmen umsetzen, um die Portabilität ihrer Cloud-Dienste zu gewährleisten.

Soll ein Cloud-Diensteanbieter durch einen anderen ersetzt werden, kann meistens der Cloud-Dienst direkt an den neuen Dienstleister übertragen werden. Ist das nicht möglich oder gewünscht, wird der Cloud-Dienst zunächst an die Institution übergeben und danach zum neuen Cloud-Diensteanbieter migriert.

In beiden Fällen sind durch die Institution alle wichtigen Anforderungen (zum Beispiel hinsichtlich einzusetzender Datenformate) zu definieren, die einen einfachen Wechsel des Dienstleisters oder eine Rückholung in die eigene Infrastruktur ermöglichen.

Insbesondere bei der Nutzung von Software as a Service sollten die eingesetzten Datenformate beachtet werden. Denn benutzt der Cloud-Anbieter ein eigenes, nicht standardisiertes Format, kommt es häufig zu Import-Problemen der Daten in einen neuen Dienst. Um das zu verhindern, sollten Portabilitätstests durchgeführt werden.

Sofern die Institution auf den flexiblen Wechsel des Cloud-Diensteanbieters angewiesen ist, empfiehlt es sich, vertraglich zu regeln, dass die erforderliche Portabilität kontinuierlich gewährleistet ist (siehe OPS.2.2.M9 *Vertragsgestaltung mit dem Cloud-Diensteanbieter*).

Werden Daten in der Cloud verschlüsselt, so darf es nicht vergessen werden, auch diese mitzubetrachten, wenn Portabilitätstests durchgeführt werden.

OPS.2.2.M16 Durchführung eigener Datensicherungen [Fachverantwortliche, IT-Betrieb] (IA)

Stellt eine Institution fest, dass besondere Gegebenheiten eigene Datensicherungen erforderlich machen, sind einige wichtige Aspekte zu beachten. Der Grund für eigene Datensicherungen ist zu dokumentieren.

Grundsätzlich kann die Institution zusätzliche Datensicherungen selbst durchführen oder sie beauftragt dafür einen externen Dienstleister (Backup as a Service).

Wird ein externer Dienstleisters beauftragt, sollten die Anforderungen an den Backup-Service detailliert ausgearbeitet und sorgfältig dokumentiert werden. Sie sollten berücksichtigen, aus welchem Grund sich die Institution zu einer eigenen Datensicherung entschlossen hat. Der Backup-Service ist dann entweder ein weiterer Cloud-Dienst oder ein Outsourcing-Vorhaben, für das die Sicherheitsanforderungen aus den entsprechenden Bausteinen erfüllt werden müssen.

Grundsätzlich empfiehlt es sich, das Recht zur eigenen Datensicherung mit dem gewählten Cloud-Diensteanbieter vertraglich zu vereinbaren (siehe OPS.2.2.M9 *Vertragsgestaltung mit dem Cloud-Diensteanbieter*).

OPS.2.2.M17 Einsatz von Verschlüsselung bei Cloud-Nutzung (IA)

Grundsätzlich ist bei der Cloud-Nutzung zwischen der Verschlüsselung von Daten auf dem Transportweg (engl.: data in motion) und der Verschlüsselung von Daten an deren Ablageort (engl.: data at rest) zu unterscheiden.

Alle zwischen einem Cloud-Dienst und der Institution übertragenen Daten sollten auf dem Transportweg verschlüsselt werden. Weitere Empfehlungen hierzu finden sich in der Maßnahme zur Vertragsgestaltung mit dem Cloud-Diensteanbieter (siehe OPS.2.2.M9 *Vertragsgestaltung mit dem Cloud-Diensteanbieter*). Deshalb wird hier nicht näher auf die Verschlüsselung von Daten auf dem Transportweg eingegangen.

Werden Daten an ihrem Speicher- bzw. Verarbeitungsort verschlüsselt, sind zwei Varianten zu unterscheiden. Zum einen können Daten direkt durch die nutzende Institution verschlüsselt werden, bevor sie an den Cloud-Diensteanbieter übertragen werden. Bei der zweiten Variante werden die übertragenen Daten erst auf den IT-Systemen des Cloud-Diensteanbieters verschlüsselt.

Werden Daten durch den Cloud-Diensteanbieter verschlüsselt, sind hierzu entsprechende vertragliche Regelungen zu treffen, die unter anderem sichere Verschlüsselungsmechanismen und geeignete Schlüssellängen vorgeben. Darüber hinaus sollte vereinbart werden, dass der Cloud-Anwender bei Bedarf die Neuvergabe von Schlüsseln anstoßen und die Lebenszyklen der Schlüssel beeinflussen kann. Es ist zu beachten, dass bei der Verschlüsselung durch den Cloud-Diensteanbieter er auch für das Schlüsselmanagement verantwortlich ist. Mitarbeiter des Cloud-Diensteanbieters, die Kenntnis von den entsprechenden Schlüsseln haben, können so auf die Daten der Institution zugreifen.

Alternativ zur Verschlüsselung der Daten durch den Cloud-Diensteanbieter kann, abhängig vom Cloud-Dienst, die Institution eigene Verschlüsselungsmechanismen einsetzen. Das sichere Schlüsselmanagement liegt dann in ihrer Hand. Hierfür sind sogenannte Hardware-Security-Module (HSM) hilfreich, die Schlüssel sicher erzeugen und speichern können. Durch ein HSM ist es unerheblich, wo verschlüsselt wird, in der Cloud oder auf den IT-Systemen der Institution, der Cloud-Diensteanbieter kann nicht auf die Schlüssel zugreifen.

Allerdings ist eine Verschlüsselung durch die Institution nicht in jedem Fall realisierbar. So ist beispielsweise bei der Nutzung von Software as a Service eine eigene Verschlüsselung in Verbindung mit der Nutzung von Anwendungen über eine API (zum Beispiel CRM-Datenbankverschlüsselung) in vielen Fällen nicht möglich. Sollte aber eine Verschlüsselung gefordert werden und der Cloud-Diensteanbieter kann diese nicht bereitstellen, ist es je nach Cloud-Dienst auch möglich, auf Drittanbieter zurückzugreifen, die eine solche Verschlüsselung anbieten. Sofern eine Institution eigene Verschlüsselungsmechanismen plant oder einen Drittanbieter nutzt, sollte sie sich eng mit dem Cloud-Diensteanbieter abstimmen, um mögliche Probleme im laufenden Betrieb möglichst frühzeitig ausschließen zu können.

Bei der Umsetzung dieser Maßnahme ist zusätzlich der Baustein CON.1 *Kryptokonzept* zu berücksichtigen.

OPS.2.2.M18 Einsatz von Verbunddiensten (CIA)

Federation Services (Verbunddienste) zeichnen sich dadurch aus, dass zwischen Authentisierung und Autorisierung getrennt wird.. Für Federation Services spielen der sogenannte Identity-Provider und der Service-Provider eine wesentliche Rolle. Der Identity-Provider übernimmt die Authentisierung des Benutzers, beim Service-Provider erfolgt die Autorisierung. Zwischen Identity-Provider und Service-Provider muss eine explizite Vertrauensstellung eingerichtet werden.

Federation Services ermöglichen die Absicherung der Cloud-Nutzung durch gesicherte Übertragung von Claims-Token (verifizierte, zentral ausgestellte Aussagen zur Identität eines Benutzers), häufig auch Authentisierungstoken genannt. Dabei können die Benutzerinformationen (zum Beispiel Benutzername) oder andere Informationen zur Identifizierung eines Mitarbeiters auch über Institutionsgrenzen hinweg sicher übertragen werden.

Nur durch die beschriebene Vertrauensstellung kann gewährleistet werden, dass der Service-Provider die vom Identity-Provider ausgestellten Claims-Token akzeptiert. Sollen Federation Services eingesetzt werden, übernimmt die Institution als Cloud-Anwender dabei die Rolle des Identity-Providers.

Mitarbeiter, die einen Cloud-Dienst benutzen wollen, melden sich dazu zunächst am zentralen Verzeichnisdienst an und erhalten danach ein Ticket (zum Beispiel Kerberos-Ticket), mit dessen Hilfe sie sich für festgelegte Dienste authentisieren können. Die Anforderung zur Nutzung eines bestimmten Cloud-Dienstes wird in der Folge vom Federation Server der nutzenden Institution in ein sogenanntes SAML-Ticket umgewandelt.

SAML steht dabei für Security Assertion Markup Language und stellt einen Standard für die Gestaltung von Tokens dar. Das auf diesem Weg erzeugte Token wird an den Federation-Server des Cloud-Diensteanbieters übertragen. Dieser entpackt das SAML-Ticket, verifiziert die Unterschrift vom Federation-Server des Cloud-Anwenders und leitet die Inhalte an die Anwendung weiter.

Da die Institution wie beschrieben als Identity-Provider agiert, geht die Verantwortung für die ordnungsgemäße Authentisierung der Benutzer auf diese über. Die Verantwortlichen innerhalb der nutzenden Institution müssen sicherstellen, dass lediglich berechtigten Benutzern ein SAML-Ticket ausgestellt wird. Auch die weitergehenden Berechtigungen, die nach erfolgreicher Authentisierung an die Anwendung übergeben werden, sollten sorgfältig definiert und regelmäßig überprüft werden. Benutzern sollten nur Berechtigungen zugewiesen werden, die diese auch tatsächlich zur Erfüllung ihrer Aufgaben benötigen.

Die Übernahme der Verantwortung für die Authentisierung ihrer Benutzer bei der Nutzung von Cloud-Diensten bringt gleichzeitig eine Reihe von Vorteilen für die Institution mit sich. So ist beispielsweise die Umsetzung einer institutionsweiten Passwortrichtlinie unabhängig von möglicherweise abweichenden Vorgaben des Cloud-Diensteanbieters möglich. Außerdem liegt die Hoheit über die Berechtigungsvergabe allein bei der nutzenden Institution. Bei sorgfältiger Konfiguration des zentralen Verzeichnisdienstes können unberechtigte Zugriffe, beispielsweise durch ehemalige Mitarbeiter, wirksam ausgeschlossen werden, ohne dabei auf den Cloud-Diensteanbieter angewiesen zu sein.

Aufgrund dieser Vorteile und der Möglichkeit, Services durch den Cloud-Diensteanbieter einfach bereitzustellen, werden Federation Services daher bereits in großem Umfang von Cloud-Diensten unterstützt.

Sollen bei einem Cloud-Nutzungs-Vorhaben Federation Services eingesetzt werden, ist dies im Rahmen der Vertragsverhandlungen mit dem Cloud-Diensteanbieter zu berücksichtigen (siehe OPS.2.2.M9 *Vertragsgestaltung mit dem Cloud-Diensteanbieter*). In der Regel stellt der Cloud-Diensteanbieter der nutzenden Institution zusätzlich Informationen bezüglich notwendiger Konfigurationsparameter für deren Federation-Server zur Verfügung. Bei der Festlegung der Konfigurationsparameter und der im SAML-Ticket zu übertragenden Informationen sollte die Institution darauf achten, dass möglichst nur die erforderlichen Informationen an den Cloud-Diensteanbieter übertragen werden. Eine umfassende Replikation weitreichender und nicht erforderlicher Informationen aus dem Verzeichnisdienst, wie zum Beispiel Telefonnummern, sollte vermieden werden.

OPS.2.2.M19 Sicherheitsüberprüfung von Mitarbeitern [Leiter Personal] (CIA)

Der Cloud-Kunde sollte sich die Qualifikation, aber auch die Vertrauenswürdigkeit der Mitarbeiter des Cloud-Diensteanbieters geeignet nachweisen lassen.

Die Möglichkeiten, die Vertrauenswürdigkeit von Personal überprüfen zu lassen, sind in Deutschland, aber auch in vielen anderen Ländern, rechtlich sehr eingeschränkt. Zudem sind die Ergebnisse meist wenig aussagekräftig, z. B. bei polizeilichen Führungszeugnissen. Grundsätzlich sollte aber vor der Übernahme neuer oder externer Mitarbeiter beim Cloud-Diensteanbieter überprüft werden, ob

- diese hinreichende Referenzen haben, z. B. aus anderen, ähnlichen Arbeitsbereichen, sowie
- der vorgelegte Lebenslauf des Bewerbers aussagekräftig und vollständig ist.

Darüber hinaus kann es sinnvoll sein, sich akademische und berufliche Qualifikationen bestätigen zu lassen, beispielsweise durch Nachfragen bei der Universität oder früheren Arbeitgebern oder Kunden. Auch die Identität des Bewerbers sollte verifiziert werden, z. B. durch Vorlage von Ausweispapieren.

Wenn ein Cloud-Diensteanbieter externes Personal einsetzt, das auf interne Informationen zugreifen kann, sollten vergleichbare Überprüfungen wie für eigene Mitarbeiter durchgeführt werden. Bei der Vertragsgestaltung mit Cloud-Diensteanbietern sollte vertraglich festgehalten werden, welche Seite solche Überprüfungen durchzuführen hat und in welcher Tiefe diese erfolgen.

3 Weiterführende Informationen

3.1 Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind.

Im Sinne der IT-Grundschutz-Vorgehensweise umfasst Cloud-Nutzung alle Themengebiete, die zur Nutzung einer Cloud-Umgebung erforderlich sind. Damit schließt Cloud-Nutzung insbesondere folgende Aspekte ein:

- Anwendung des Cloud-Dientes durch Mitarbeiter der nutzenden Institution
- Administration des Cloud-Dientes durch Mitarbeiter der nutzenden Institution

Definitionen und Grundbegriffe zur Cloud-Nutzung

Ein Cloud-Dienst wird durch die nachfolgend aufgeführten Eigenschaften charakterisiert (gemäß Cloud Security Alliance - CSA). Die Beschreibung ist dabei nicht starr definiert, sondern kann immer noch interpretiert, ergänzt oder auch reduziert werden.

- On-demand Self-Service
- Die Provisionierung, also die Bereitstellung der IT-Ressourcen, wie beispielsweise Rechnerleistung oder Speicherkapazitäten, läuft automatisch ohne Interaktion mit dem Cloud-Diensteanbieter (engl. Cloud Service Provider, kurz CSP) ab.
- Broad Network Access
- Cloud-Dienste werden über ein Netz bereitgestellt und sind über Standard-Mechanismen beziehungsweise Standard-Protokolle zugänglich.
- Resource Pooling
- Die IT-Ressourcen des Cloud-Diensteanbieters sind in sogenannten Pools organisiert. Basierend auf einem mandantenfähigen Modell ist es dem Cloud-Diensteanbieter somit möglich, den Anforderungen einer Vielzahl von Benutzern bedarfsgerecht zu entsprechen.
- Dem Auftraggeber ist der genaue Ort der IT-Ressourcen des Cloud-Diensteanbieters in der Regel nicht bekannt. Beispiele für solche Ressourcen können Speichersysteme, Prozessorleistung, Arbeitsspeicher oder auch Anwendungssoftware sein.
- Rapid Elasticity
- Cloud-Dienste lassen sich automatisiert, schnell und flexibel anpassen, um auf sich rasch ändernden Bedarf aufseiten der nutzenden Institution reagieren zu können.
- Measured Services
- Cloud-Dienste verwenden häufig Werkzeuge, die die Ressourcennutzung in Abhängigkeit des genutzten Services (zum Beispiel Speicherlösungen, Prozessorleistung oder aktive Benutzerkonten) automatisch überwachen und optimieren können.
- Um Transparenz sowohl aufseiten der nutzenden Institution als auch aufseiten des Providers zu schaffen, kann die Ressourcennutzung gemessen und die Ergebnisse können gegenüber dem Anwender kommuniziert werden.
- Pay per Use
- Die Abrechnung erfolgt bei Cloud-Nutzung in der Regel auf Basis der Leistungen beziehungsweise Ressourcen, die auch tatsächlich vom Anwender in Anspruch genommen wurden.

Definition des BSI

Um für alle Arbeiten rund um Cloud-Computing eine einheitliche Grundlage zu haben, hat das BSI folgende Definition für den Begriff *Cloud Computing* festgelegt:

Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (zum Beispiel Rechenleistung, Speicherplatz), Plattformen und Software.

In diesem Dokument wird der Begriff *Cloud Computing* entsprechend benutzt, wobei die oben genannten Charakteristika stets im Hinterkopf zu behalten sind. So ist eine einfache Webanwendung in der Regel kein Cloud-Computing, obwohl dies von den Marketingabteilungen der Hersteller oft so bezeichnet wird.

Cloud-Nutzung mittels unterschiedlicher Cloud-Service-Modelle

Bei Cloud-Nutzung können grundsätzlich drei Kategorien von Service-Modellen unterschieden werden. Zum besseren Verständnis sind diese nachfolgend näher beschrieben.

- Infrastructure as a Service (IaaS)
- Bei IaaS werden IT-Ressourcen wie zum Beispiel Rechenleistung, Datenspeicher oder Netze als Dienst angeboten. Ein Cloud-Anwender kauft diese virtualisierten und in hohem Maße standardisierten Services und baut darauf eigene Services zum internen oder externen Gebrauch auf. So kann ein Cloud-Anwender zum Beispiel Rechenleistung, Arbeitsspeicher und Datenspeicher anmieten und darauf ein Betriebssystem mit Anwendungen seiner Wahl laufen lassen.
- Die Verwaltung der IT-Ressourcen obliegt der nutzenden Institution und wird in der Regel durch den Cloud-Service-Administrator auf Kundenseite (engl. Customer Cloud Service Administrator) vorgenommen.
- Platform as a Service (PaaS)
- Ein PaaS-Anbieter stellt eine komplette Infrastruktur bereit und bietet dem Anwender auf der Plattform standardisierte Schnittstellen an, die von Diensten des Kunden genutzt werden. So kann die Plattform zum Beispiel Mandantenfähigkeit, Skalierbarkeit, Zugriffskontrolle, Datenbankzugriffe etc. als Service zur Verfügung stellen. Die nutzende Institution hat keinen Zugriff auf die darunter liegenden Schichten (Betriebssystem, Hardware). Sie kann aber auf der Plattform eigene Anwendungen laufen lassen, für deren Entwicklung der Cloud-Diensteanbieter in der Regel eigene Werkzeuge anbietet.
- Software as a Service
- Sämtliche Angebote von Anwendungen, die den Kriterien des Cloud-Computings entsprechen, fallen in diese Kategorie. Dem Angebotsspektrum sind hierbei keine Grenzen gesetzt. Als Beispiele seien Kontaktdatenmanagement, Finanzbuchhaltung, Textverarbeitung oder Kollaborationsanwendungen genannt.
- Die Mitarbeiter der Institution nutzen Software-Anwendungen direkt über das Internet. Eine Installation auf dem eigenen PC beziehungsweise im Rechenzentrum der Institution ist häufig nicht erforderlich.
- Teilweise werden jedoch auch Architekturen eingesetzt, bei denen der Einsatz spezieller Clientsoftware erforderlich oder möglich ist (Nutzung über Browser und/oder Clientsoftware).

Cloud-Nutzung mittels unterschiedlicher Cloud-Bereitstellungsmodelle

Institutionen, die sich für Cloud-Dienste entscheiden, haben in der Regel die Wahl zwischen folgenden Bereitstellungsmodellen:

- Public CloudBereitstellung von Cloud-Diensten für beliebige Anwender über das Internet.
- Private CloudBereitstellung von Cloud-Diensten ausschließlich für die eigene Institution. Bei einer Private Cloud ist eine weitere Unterscheidung möglich:

- On-Premise: Die Cloud-Infrastruktur wird in einem Rechenzentrum der Institution betrieben.
- Off-Premise: Die Cloud-Infrastruktur wird in einem fremden Rechenzentrum betrieben.
- Hinweis zur Problematik bei der Zuordnung zu einem Bereitstellungsmodell:

In Konzernen mit mehreren Konzerngesellschaften wird aus Sicht der IT-Tochter eine Private Cloud für den Konzern betrieben. Eine nutzende Konzerngesellschaft teilt diese Sicht jedoch unter Umständen nicht, da sie sich diese Cloud in ihren Augen mit "Fremden" teilt. Daher betrachtet die Konzerngesellschaft die Cloud als "public".

- Hybrid Cloud

Eine Hybrid Cloud stellt in der Regel eine Mischform aus Public Cloud und Private Cloud dar. Teile des Services werden dabei durch On-Premise-Systeme abgebildet, während andere Teile des Services durch (Public)-Cloud-Systeme bei einem Cloud-Diensteanbieter abgebildet werden. Die Services, die durch den Cloud-Diensteanbieter abgebildet werden, können auch Private-Cloud-Off-Premise- oder Community-Cloud-Lösungen sein.

Die Hybrid Cloud bietet die Möglichkeit Dienste zwischen Public Cloud und Private Cloud aufzuteilen.

Beispiel:

Für die Inanspruchnahme eines Office-Services werden die E-Mail-Konten in der Private Cloud der Institution verwaltet, für die Nutzung von Webkonferenzen und Dateifreigaben wird jedoch auf die Public-Cloud-Infrastruktur des Dienste-Anbieters zurückgegriffen.

- Eine **Virtual Private Cloud** wird durch einen Cloud-Diensteanbieter in seinem Rechenzentrum für dedizierte Kunden betrieben. Aus Kundensicht sieht die Cloud wie eine Private Cloud aus, der Dienstleister stellt diese aber in der Regel auf einer mandantenfähigen, geteilten Infrastruktur bereit.
- Bei der **Managed Private Cloud** kann die Cloud-Infrastruktur hingegen auch im eigenen Rechenzentrum untergebracht sein. Betrieben und gemanagt wird diese allerdings von einem externen Dienstleister.

- Community CloudIn einer Community Cloud schließen sich Institutionen der selben Branche oder mit gleichen Interessen zusammen und nutzen gemeinsam eine Cloud-Umgebung, die vom Cloud-Diensteanbieter speziell für diese Community bereitgestellt wird.Community Clouds finden sich auch im Bereich der öffentlichen Verwaltung. Hier stellt ein Cloud-Diensteanbieter einer Benutzergruppe eine Anwendung dediziert als Cloud-Dienst zur Verfügung, z. B. Personalverwaltung oder E-Mail-Service.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Cloud-Nutzung" finden sich unter anderem in folgenden Veröffentlichungen:

[27001] ISO/IEC 27001:2013

Information technology - Security techniques - Information security management systems – Requirements, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/SC 27, Oktober 2013

[BSIC5] Anforderungskatalog Cloud Computing (C5)

(BSI), Kriterien zur Beurteilung der Informationssicherheit von Cloud-Diensten, Bundesamt für Informationstechnik (BSI), September 2017,https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Anforderungskatalog-Cloud_Computing-C5.pdf, zuletzt abgerufen am 30.08.2018

[CSA] Security Guidance for Critical Areas of Focus in Cloud Computing

Cloud Security Alliance (CSA), Version 4.0, 2017, https://cloudsecurityalliance.org/download/security-guidance-v4/, zuletzt abgerufen am 30.08.2018

[DIN663993] DIN SPEC 66399-3:2013-02 - Büro- und Datenträgertechnik - Vernichtung von Datenträgern

Teil 3: Prozess der Datenträgervernichtung, Februar 2013

[ENISA] Cloud Computing: Benefits, Risks and Recommendations for Information Security

European Union Agency for Network and Information Security (ENISA), November 2009, https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment/at_download/fullReport, zuletzt abgerufen am 30.08.2018

[ISF] The Standard of Good Practice for Information Security

Information Security Forum (ISF), June 2018

[NIST800144] Guidelines on Security and Privacy in Public Cloud Computing

NIST Special Publication 800-144, December 2011, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf, zuletzt abgerufen am 30.08.2018

[NIST80053] Security and Privacy Controls for Federal Information Systems and Organizations

NIST Special Publication 800-53, Revision 4, April 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf , zuletzt abgerufen am 30.08.2018

OPS.2: IT-Betrieb von Dritten

Umsetzungshinweise zum Baustein OPS.2.4 Fernwartung

1 Beschreibung

1.1 Einleitung

Die Fernwartung beschreibt einen räumlich getrennten Zugriff auf IT-Systeme und die darauf laufenden Anwendungen zu Konfigurations-, Wartungs-, Reparatur- oder Kontrollzwecken. Die Fernwartung kann passiv durch einen ausschließlich betrachtenden Zugang auf das IT-System bzw. die Anwendungen erfolgen oder aktiv durch direkte administrative Eingriffe in das Betriebssystem oder laufende Anwendungen. Im Fall der passiven Fernwartung muss ein Benutzer vor Ort die eigentlichen Aktionen veranlassen. Bei der aktiven Fernwartung dagegen wird in ein Betriebssystem eingegriffen und dieses direkt durch einen Administrator bedient. Dabei werden unter anderem die Signale einer Maus und Tastaturbefehle, sowie Bildschirminhalte und Konsolenausgaben übertragen.

Selbst wenn wirkungsvolle Mechanismen zur Absicherung des Zugangs zur Fernwartung implementiert werden, bestehen direkte Zugriffsmöglichkeiten von außerhalb auf das interne Netz und alle darin verarbeiteten Daten. Durch diese Schnittstellen können Externe die Institution gefährden und somit wirtschaftliche und betriebstechnische Schäden anrichten. Daher ist es notwendig, bei der Fernwartung den gesamten Lebenszyklus der Informationssicherheit abzusichern.

1.2 Lebenszyklus

Planung und Konzeption

Ist die Entscheidung für eine Fernwartung gefallen, muss der sichere Einsatz geplant und konzipiert werden. Die dabei zu berücksichtigenden Aspekte sind in *OPS.2.4.M1 Planung des Einsatzes der Fernwartung* und *OPS.2.4.M5 Erstellung einer Richtlinie für die Fernwartung* zusammengefasst. Die Sicherheit der Fernwartung kann bereits in der Planungs- und Konzeptionsphase entscheidend beeinflusst werden, indem sicherheitsrelevante Aspekte berücksichtigt werden.

Wichtig ist außerdem *OPS.2.4.M6 Dokumentation bei der Fernwartung* für die durchgehende Dokumentation von Prozessen der Fernwartung und *OPS.2.4.M22 Planung des sicheren Einsatzes in einem abgesicherten Netzsegment* für die Sicherheit in Internet- und Intranet-Szenarien.

Unabhängig von den nachfolgenden Maßnahmen sollten die Anforderungen des *Bausteins ORP.4 Identitäts- und Berechtigungsmanagement* beachtet, bewertet und umgesetzt werden.

Beschaffung

Im nächsten Schritt muss die Beschaffung geeigneter Werkzeuge für die Fernwartung und eventuell zusätzlich benötigter Hardware erfolgen. Aufbauend auf Einsatzszenarien sind die Anforderungen an zu beschaffende Produkte zu formulieren und basierend darauf die Auswahl der geeigneten Produkte zu treffen. Daher muss an dieser Stelle *OPS.2.4.M8 Auswahl geeigneter Fernwartungswerkzeuge* berücksichtigt werden.

Umsetzung

Nachdem die organisatorischen Vorarbeiten durchgeführt worden sind, kann die Umsetzung der Fernwartung erfolgen. Dabei sind vor allem die Maßnahmen *OPS.2.4.M9 Verwaltung der Fernwartungswerkzeuge*, *OPS.2.4.M10 Einsatz von kryptographischen Verfahren bei der Fernwartung* und *OPS.2.4.M11 Patch- und Änderungsmanagement bei der Fernwartung* zu beachten.

Es sollten für die Fernwartung ausschließlich sichere Authentisierungsmechanismen eingesetzt werden (siehe hierzu *OPS.2.4.M16 Authentisierungsmechanismen bei der Fernwartung*).

Alle Benutzer und Administratoren sollten ausreichend über die Prozesse der Fernwartung geschult werden (siehe hierzu *OPS.2.4.M15 Schulung zur Fernwartung*).

Da die reine Umsetzung der Fernwartung viele Schnittstellen zum internen sowie externen Netz aufweist, sind geeignete Maßnahmen zum Schutz der Netze, IT-Systeme und Anwendungen zu treffen (siehe hierzu *OPS.2.4.M7 Sichere Protokolle bei der Fernwartung*, *OPS.2.4.M3 Regelungen zu Kommunikationsverbindungen*, *OPS.2.4.M17 Passwortsicherheit bei der Fernwartung* und *OPS.2.4.M14 Absicherung der Fernwartung*).

Sollten Dritte in die Umsetzung der Fernwartung eingebunden werden, sollten die Empfehlungen der Maßnahme *OPS.2.4.M18 Fernwartung durch Dritte* beachtet werden.

Um eine Hochverfügbarkeit der Fernwartung gewährleisten zu können, sollten die Maßnahmen aus *OPS.2.4.M21 Redundante Verwendung von Kommunikationsnetzen* berücksichtigt werden.

Betrieb

Nach der Umsetzung der Anforderungen für die Fernwartung wird der Regelbetrieb aufgenommen. Damit Sicherheitsverstöße bemerkt werden, muss eine entsprechende Angriffsabwehr und Überwachung aller IT-Systeme und Anwendungen, die durch die Fernwartung verwaltet werden, erfolgen.

Da die Fernwartung immer Veränderungen unterworfen ist, die sich meist aus veränderten Anforderungen oder Einsatzszenarien ableiten, muss sichergestellt werden, dass das gewünschte Sicherheitsniveau aufrechterhalten wird (siehe hierzu *OPS.2.4.M19 Betrieb der Fernwartung und OPS.2.4.M11 Patch- und Änderungsmanagement bei der Fernwartung*).

Notfallvorsorge

Empfehlungen zur Notfallvorsorge für die Fernwartung finden sich in den Maßnahmen *OPS.2.4.M12 Datensicherung bei der Fernwartung* und *OPS.2.4.M20 Erstellen eines Notfallplans für den Ausfall der Fernwartung.*

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Fernwartung" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

OPS.2.4.M1 Planung des Einsatzes der Fernwartung [IT-Betrieb]

Der Einsatz der Fernwartung muss an die Institution angepasst und bedarfsgerecht hinsichtlich technischer und organisatorischer Aspekte geplant werden. Es sollten mindestens die folgenden Aspekte im Rahmen der Einsatzplanung betrachtet werden:

- Soll die Fernwartung In-Band (also innerhalb des normalen IT-Netzes) oder Out-Band (also über ein dediziertes Administrationsnetz) stattfinden? Bei erhöhtem Schutzbedarf empfiehlt es sich, die Fernwartung aus einem dedizierten Administrationsnetz durchzuführen.
- Welche Schnittstellen und Protokolle sollen verwendet werden?
- Was für ein Schutzbedarf liegt vor? Welche Schutzziele müssen erfüllt werden?
- Welche Auditierungsanforderungen müssen beachtet werden?
- Welche gesetzlichen und internen Regelungen sind zu berücksichtigen?
- Erfolgt die Fernwartung durch Dienstleister? Dann ist OPS.2.4.M18 Fernwartung durch Dritte umzusetzen.
- Dürfen Online-Dienste zur Fernwartung genutzt werden?
- Welche Aufgabenverteilung innerhalb der Institution muss beim Einsatz der Fernwartung erfolgen?
- Welche Anforderungen aus der Netzseparierung sind zu beachten?

Je genauer die Rahmenbedingungen bekannt und je präziser die Vorgaben formuliert sind, desto einfacher werden die nächsten Konzeptionierungs- und Umsetzungsschritte der Fernwartung.

OPS.2.4.M2 Sicherer Verbindungsaufbau bei der Fernwartung [Benutzer]

Die Initiierung eines Fernwartungs-Zugriffs muss immer aus der Institution heraus erfolgen. Dies kann durch Anruf des zu wartenden IT-Systems bei der Fernwartungsstelle oder über einen automatischen Rückruf (Callback) realisiert werden. Das externe Wartungspersonal muss sich zu Beginn der Wartung authentisieren. Wird die Verbindung zur Fernwartungsstelle auf irgendeine Weise unterbrochen, so muss der Zugriff auf das System durch einen "Zwangslogout" beendet werden.

Der Benutzer des fernadministrierten IT-Systems muss dem Fernzugriff explizit zustimmen, z. B. über eine entsprechende Bestätigung am System.

OPS.2.4.M3 Absicherung der Kommunikationsverbindungen bei der Fernwartung [IT-Betrieb]

Die Kommunikationsschnittstellen und möglichen Zugänge für einen Verbindungsaufbau von außen sind auf das notwendige Maß, entsprechend der verwendeten Betriebssysteme und weiteren damit in Verbindung stehenden Hardware- und Software-Komponenten, zu beschränken. Ebenso müssen alle Kommunikationsverbindungen nach vollzogenem Fernzugriff getrennt werden (Deaktivierung). Für eine Fernwartung müssen notwendige Ports ständig bereitgestellt werden. Zum Beispiel können die zur Verfügung stehenden Ports mit Hilfe eines Firewall-Portals und hinterlegten Firewall-Regel nach erfolgreicher Authentisierung eines berechtigten Administrators geöffnet werden.

Es müssen unter Berücksichtigung des Schutzbedarfes des jeweiligen IT-Systems, der Anwendung bzw. der damit verbundenen Netzseparierung sichere Authentisierungsmechanismen eingesetzt werden. Wird für die Kommunikation kein eigenständiges Administrationsnetz verwendet, sollte eine Alternative mit identischen Sicherheitsmerkmalen verwendet werden. Der erlaubte Personenkreis für einen Verbindungsaufbau sollte nach dem Minimalprinzip eingeschränkt werden.

Wichtig ist, dass bei den Kommunikationsverbindungen und dem Verbindungsaufbau bei der Fernwartung folgende Punkte beachtet werden:

- Sicherstellung der Vertraulichkeit der übertragenen Daten: Die Sicherstellung der Vertraulichkeit der übertragenden Daten muss durch eine ausreichende sichere Verschlüsselung erreicht werden.
- Sicherstellung der Integrität der übertragenen Daten: Die eingesetzten Übertragungsprotokolle müssen eine zufällige Veränderung übertragener Daten erkennen und beheben.
- Sicherstellung der Verfügbarkeit der Fernwartung: Falls zeitliche Verzögerungen bei der Fernwartung nur schwer zu tolerieren sind, sollten redundante Übertragungswege zur Verfügung gestellt werden.
- Sicherstellung der Nachvollziehbarkeit der Datenübertragung: Um eine Kommunikation nachvollziehbar zu machen, können Protokollierungsfunktionen eingesetzt werden, die nachträglich feststellen lassen, welche Daten wann und an wen übertragen wurden.
- Sicherstellung des Datenempfangs: Ist es für die Fernwartung von Bedeutung, ob Daten korrekt empfangen wurden, können Quittungsmechanismen eingesetzt werden, aus denen hervorgeht, ob der Empfänger die Daten korrekt empfangen hat.

OPS.2.4.M4 Regelungen zu Kommunikationsverbindungen [IT-Betrieb]

Unter Beachtung des Bausteins *NET.3.2 Firewall* muss die Fernwartung in das Firewall-Regelwerk der Institution eingebunden werden. Hierbei muss darauf geachtet werden, dass bestehende Firewall-Infrastrukturen und deren Regelungen nicht umgangen werden.

Entsprechend dem Minimalprinzip (Whitelist-Strategie) sollten die für die Fernwartung benötigten Protokolle ergänzt werden.

Bei der Überprüfung der Netz-Konnektivität mittels ICMP müssen die Regelungen für die lokalen und entfernten Prüfungen beachtet werden. Lokal empfiehlt es sich, einen Ping of localhost in der lokalen Firewall zur Überprüfung der korrekten Funktionstüchtigkeit der Netzwerkkarte zu erlauben. Zur Überprüfung der grundsätzlichen Netzkonnektivität sollte eine entfernte Prüfung mittels Ping auf die benötigte Gegenstelle erlaubt sein.

Im Sinne der Firewall-Sicherheit muss überprüft werden, ob Remote Procedure Calls (RPCs) durch die etablierte Sicherheitsarchitektur analysiert und gefiltert werden können. Sollte eine Filterung nicht möglich sein, müssen entsprechende Schutzmaßnahmen gegen missbräuchliche RPC-Aufrufe getroffen werden.

Gemeinsam mit den Basismaßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich Fernwartung.

OPS.2.4.M5 Einsatz von Online-Diensten [Benutzer, IT-Betrieb]

Oftmals ist eine etablierte Software für die Fernwartung kostenpflichtig und muss auf jedem Client installiert werden. In Ausnahmesituationen kann es jedoch hilfreich sein, kurzfristig IT-Systeme über eine Fernwartung zu administrieren. Pragmatisch erscheint die Lösung, dass die Clients eine Verbindung zu einem Online-Dienst aufbauen und der Administrator über einen Webserver über den Online-Dienst auf die Clients zugreift.

Werden Online-Dienste genutzt, entstehen aber sicherheitstechnische Risiken. Dies sollte daher grundsätzlich verboten sein. Die Fernwartung über Online-Dienste sollte durch technische Maßnahmen verhindert werden. Wenn ein grundsätzliches Verbot im Einzelfall nicht möglich ist, sollte der Einsatz auf ein Minimum und nur für klar definierte Einsatzgebiete mit strikten Regelungen beschränkt werden.

Bei Online-Diensten zur Fernwartung verbindet sich die IT-Systeme des Fernwartenden und des Administrators jeweils mit einem Dienstanbieter im Internet. Dabei ist vom Fernwartenden nicht erkennbar, was mit diesen Informationen beim Diensteanbieter passiert bzw. welche Eingriffsmöglichkeiten dort bestehen. Es könnten Inhalte mitgeschnitten oder auch manipuliert werden. Dies gilt z. B. auch für Tastatureingaben (z. B. Passwörter).

Oft starten die Clients der Fernwartenden den Dienst automatisch und verbinden sich mit dem Online-Dienst. Ist dies der Fall, kann jeder, der die Zugangsdaten kennt (oft nur eine ID und PIN) unbeobachtet und unbemerkt auf die Clients zugreifen.Es sollte verboten werden, dass Clients automatisch eine Verbindung zu Online-Diensten aufbauen können, dies sollte auch technisch verhindert werden.

Der Vorteil von Online-Diensten besteht darin, dass z. B. in einem Notfall eine Fernwartung schnell initiiert werden kann, weil bei den Beteiligten keine besondere Infrastruktur notwendig ist. In diesem Fall müssen allerdings vorab genau geregelt werden, in welchen Fällen und unter welchen Bedingungen Online-Dienste zum Fernzugriff erlaubt sind. Diese sind zu dokumentieren und mit dem ISB und dem Datenschutzbeauftragten der Institution vorab abzustimmen.

Die Regelungen sollten z. B. folgende Punkte umfassen:

- Es sollte festgelegt werden, in welchen Fällen eine Fernwartung über Online-Dienste erlaubt ist. Beispielsweise kann es notwendig sein, bei definierten Notfällen oder um unmittelbare Gefahr für den Dienstbetrieb abzuwenden, auf die Fernwartung über Online-Dienste zurückzugreifen.
- Es muss geregelt werden, wie und von wem die Nutzung von Online-Diensten autorisiert wird. Dabei sollten für den Einzelfall die existierenden Meldewege eingehalten werden.
- Ein automatischer Verbindungsaufbau sollte untersagt werden. Die Verbindung muss im Einzelfall vom fernzuwartenden IT-System freigegeben werden.
- Für jede Verbindung sind neue Zugangsdaten zu generieren (z. B. neue PIN).
- Die Zugangsdaten dürfen nicht in Klartext übermittelt werden (z. B. nur mündlich, verschlüsselt).
- In einer Verbindung über einen Online-Dienst dürfen keine Passwörter oder andere vertrauliche Informationen dargestellt oder lokal eingegeben werden. Mit einer "Whitelist" kann beschrieben werden, welche Informationen übertragen werden dürfen.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Fernwartung".

OPS.2.4.M6 Erstellung einer Richtlinie für die Fernwartung [IT-Betrieb]

Es ist zu entscheiden, ob die Aspekte der Fernwartung in bestehenden Richtlinien ergänzt werden oder eine eigenständige Richtlinie zu erstellen ist. Sollte eine eigenständige Richtlinie erstellt werden, so ist in den bestehenden Richtlinien der Institution auf die Richtlinie für Fernwartung zu referenzieren. Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution sollten die wesentlichen Kernaspekte für die Fernwartung konkretisiert werden. Die Richtlinie muss allen Verantwortlichen, die an der Konzeption, dem Aufbau und dem Betrieb sowie der Aussonderung beteiligt sind, bekannt sein und die Grundlage für deren Arbeit bilden können. Die Umsetzung der in der Richtlinie geforderten Inhalte sollte regelmäßig überprüft werden und die Ergebnisse sind anschließend sinnvoll zu dokumentieren. Die Vorgaben innerhalb der Richtlinie sollten stringent sein, um spätere Risikoeinschätzungen oder Risikoübernahmen durchführen zu können. Wird kryptographische Kommunikation für die Fernwartung benötigt, müssen die Anforderungen des Bausteins *CON.1 Kryptokonzept* berücksichtigt werden.

OPS.2.4.M7 Dokumentation bei der Fernwartung [IT-Betrieb]

Es muss eine aktuelle Dokumentation der Fernwartung vorliegen. Vorhandene Stellvertreter müssen, mit Hilfe der Fernwartungsdokumentation, zu jeder Zeit die Aufgaben und Prozesse, übernehmen können. Aus diesem Grund empfiehlt es sich, bei größeren Infrastrukturen ein einheitliches Namenskonzept für die IT-Systeme der Institution zu verwenden, um die Transparenz zu erhöhen und Arbeitsprozesse durch gezielte Zugriffe zu optimieren.

Da die Dokumente, z. B. Arbeitsanweisungen für die Initiierung eines Fernzugriffs, meist vertrauliche Informationen und Daten beinhalten, müssen sie an geeigneten Orten gesichert abgelegt werden und auch im Rahmen des Notfallmanagements zur Verfügung stehen. Ebenso müssen sie vor unbefugtem Zugriff geschützt sein. Sämtliche Fernzugriffsmöglichkeiten müssen erfasst und dokumentiert sein, sofern es sich nicht um übliche Vorgehensweisen nach Betriebssystemstandard handelt. Im Asset-Management der Institution sollten die Systeme und deren Schnittstellen für die Fernadministration hinterlegt sein. Für das Notfallmanagement und für den Wiederanlaufplansollten die internen und externen Ansprechpartner der Systeme hinterlegt werden.

Die allgemeine Dokumentation der administrativen Prozesse für die verschiedenen IT-Komponenten sollte in Form von Betriebshandbüchern erfolgen. Im Betriebshandbuch für das jeweilige System, welches aus der Ferne administriert werden soll, muss ein Hinweis enthalten sein, von welchem System aus, mit welchen Rechten und durch welche Organisationseinheit hierauf zugegriffen werden darf.

Innerhalb der Fernwartungsprozesse wird auf die folgenden dokumentierten Angaben zugegriffen:

- Die aktuelle Dokumentation aller vorhandenen IT-Systeme und deren Konfiguration sowie gegebenenfalls dem Namenskonzept der IT-Systeme,
- Die Dokumentation der auf den jeweiligen IT-Systemen eingerichteten Benutzer und deren Rechteprofilen,
- Die neu hinzugekommenen Hard- und Softwarekomponenten in der Systemdokumentation,
- Die Dokumentation aller sicherheitsrelevanten Abläufe wie der Datensicherung oder der Vernichtung von Datenträgern,
- Die Beschreibungen aller gefundenen und behobenen Fehler.

OPS.2.4.M8 Sichere Protokolle bei der Fernwartung [IT-Betrieb]

Es sollten ausschließlich aktuelle und als sicher eingestufte Kommunikationsprotokolle zur Fernwartung eingesetzt werden. Die Kommunikation sollte verschlüsselt erfolgen. Die Empfehlungen des BSI aus der technischen Richtlinie (TR-02102) "Kryptographische Verfahren: Empfehlungen und Schlüssellängen" sollten bei der Auswahl der Protokolle und Algorithmen beachtet werden. Damit die eingesetzten Protokolle geeignet verwaltet und die Sicherheitsanforderungen berücksichtigt werden, müssen Informationen zu Schwachstellen aus der Fachpresse bzw. aus einschlägigen Quellen beachtet und kontinuierlich aktualisiert werden.

Die Administration mittels Tunnel kann durch einen SSH-Tunnel, SSL-Tunnel oder IPSec-Tunnel abgesichert erfolgen. Es sollte ausgehend vom Schutzbedarf der Institution eine angemessene Tunnelmethode ausgewählt werden. Diese muss natürlich von den eingesetzten IT-Systemen auch unterstützt werden.

Für die Verwendung der folgenden Protokolle empfiehlt sich die Verwendung der jeweiligen Versionen:

- Einsatz von SSH in der Version 2
- Gebrauch von TLS 1.2
- Verwendung von SNMP ab Version 3
- Nutzung von IPsec mit IKEv2 und idealerweise Zertifikaten

Bei erhöhtem Schutzbedarf sollte für SNMP Version 3 jeweils ein eigenständiges Benutzerkonto für den lesenden, schreibenden und sendenden Zugriff eingerichtet werden.

Alle anfallenden Syslog- und Event-Meldungen im Rahmen der Fernwartung müssen entsprechend der Protokollierungs- und Überwachungsvorgaben der Institution aufbereitet werden.

OPS.2.4.M9 Auswahl geeigneter Fernwartungswerkzeuge [IT-Betrieb]

Die Auswahl geeigneter Fernwartungswerkzeuge orientiert sich an den betrieblichen, sicherheitstechnischen und datenschutzrechtlichen Anforderungen der Institution. Die Auswahl und Bewertung der in Frage kommenden Fernwartungswerkzeuge sollte mittels einer Anforderungsanalyse und anschließender Risikobewertung festgestellt werden. Alle Beschaffungsentscheidungen sollten mit den Verantwortlichen des Einkaufes, dem System- und Anwendungsverantwortlichen sowie dem Sicherheitsmanagement abgestimmt werden. Hierbei sollte auch die Personalvertretung beteiligt werden.

Die Fernwartungswerkzeuge sollten die Sicherheitsanforderungen der Institution unter Berücksichtigung des zu erfüllenden Schutzbedarfs erfüllen. Hieraus ergeben sich insbesondere Anforderungen an die kryptographischen Mechanismen. Ebenso sollten bei der Datenübermittlung die Verbindungsqualität und die Systemauslastung berücksichtigt werden. Für alle weiteren Funktionen sollten immer die Aspekte aus *OPS.2.4.M1 Planung des Einsatzes der Fernwartung* berücksichtigt werden.

Nach der Betrachtung der Funktionen der Fernwartungswerkzeuge sollten abschließend die Hilfestellungs- und Support-Leistungen geprüft werden. Es sollte möglich sein, Fragen und Problemstellungen den Hersteller bzw. Herausgeber zu richten. Dieser sollte über einen Support mit mehrstufiger Eskalation und Priorisierung verfügen.

OPS.2.4.M10 Verwaltung der Fernwartungswerkzeuge [Benutzer, IT-Betrieb]

Da Fernwartungswerkzeuge eine Vielfalt unterschiedlicher Funktionen ermöglichen, müssen organisatorische Verwaltungsprozesse zum Umgang mit den ausgewählten Werkzeugen etabliert werden. Es muss eine Bedienungsanleitung für den geeigneten Umgang mit den Fernwartungswerkzeugen für den IT-Betrieb vorliegen. Musterabläufe für die passive und die aktive Fernwartung müssen für die Nutzung innerhalb der Institution erstellt und kommuniziert werden. Um mögliche Sicherheitslücken, resultierend aus Fehlkonfigurationen und Bedienungsproblemen, zu minimieren, muss der IT-Betrieb im Umgang mit den Fernwartungswerkzeugen sensibilisiert und geschult werden. Es muss ein Anwendungsverantwortlicher benannt werden, der als Ansprechpartner für alle fachlichen Fragen zu den Fernwartungswerkzeugen dient.

Vorgaben für die Administration

- Die Berechtigungen der Administratoren sollten nach dem Minimumprinzip vergeben werden. Wenn Administratoren ihre Zuständigkeit und Aufgabenbereiche verändern, müssen die Berechtigungen zeitnah angepasst werden.
- Die vorhandenen Prozesse der Berechtigungsvergabe und des Berechtigungsentzugs der Institution sind für die Fernwartung entsprechend anzupassen.
- In den Arbeitsanweisungen für die Fernwartung sollte aufgeführt werden, welche exakten Einsatzzwecke vorgesehen sind und welche verfügbaren Mittel verwendet werden sollten und dürfen.

Die benötigten Berechtigungen und Identitäten für die Fernwartung von Systemen und Anwendungen sollten in das etablierte Identitäts- und Berechtigungsmanagement eingebunden werden.

Vorgaben für die Prozesse der Fernwartung

- Für den Betrieb von Fernwartungswerkzeugen sind Vorgaben und Abläufe festzulegen. Zum Beispiel sollte festgelegt werden, wer auf die Werkzeuge zugreifen darf und wo Änderungen damit durchgeführt werden dürfen. Dies sollte in Form eines Prozessschaubildes dokumentiert werden.
- Die Fernwartungswerkzeuge müssen in den Prozess der Fernwartung selbst und in das Patch- und Änderungsmanagement eingegliedert werden, sofern diese nicht bereits Teil des Betriebssystems sind.

OPS.2.4.M11 Einsatz von kryptografischen Verfahren bei der Fernwartung [IT-Betrieb]

Bei der Fernwartung müssen kryptographische Verfahren (Signaturen und Verschlüsselungsverfahren) genutzt werden, um einerseits die Kommunikation abzusichern und andererseits eine sichere Authentisierung zu gewährleisten. Es müssen hinreichend starke kryptographische Verfahren zur Verschlüsselung bzw. Signatur innerhalb der Fernwartung verwendet werden. Die Stärke der verwendeten kryptographischen Verfahren und Schlüssel muss im Rahmen der Fernwartung regelmäßig überprüft und falls erforderlich angepasst werden. Die genutzten kryptographischen Verfahren sind, basierend auf den internen Vorgaben und den Empfehlungen des BSI, auf dem aktuellen Stand der Technik zu halten. Die allgemeinen Anforderungen und Maßnahmen werden durch die Empfehlungen des Bausteins *CON.1 Kryptokonzept* abgedeckt und gelten auch für den Einsatz der Verfahren bei der Fernwartung.

OPS.2.4.M12 Patch- und Änderungsmanagement bei der Fernwartung [IT-Betrieb]

Alle Updates, Patches und sonstigen Änderungen an IT-Systemen und den darauf laufenden Anwendungen, die per Fernwartung getätigt werden, unterliegen den allgemeinen Vorgaben zum Patch- und Änderungsmanagement der Institution.

Darüber hinaus sollten die Anforderungen des Bausteins OPS.1.1.3 Patch- und Änderungsmanagement beachtet werden.

OPS.2.4.M13 Datensicherung bei der Fernwartung [IT-Betrieb]

Um Datenverluste innerhalb der Infrastruktur für die Fernwartung zu vermeiden, müssen für diese regelmäßige Datensicherungen (Backups) durchgeführt werden. Es müssen Vorgaben für die Datensicherung bei der Fernwartung anhand der Menge und Wichtigkeit der laufend neu gespeicherten Daten und des möglichen Schadens für die Institution bei Verlust dieser Daten getroffen werden. Die Anforderungen müssen dabei dem Patch- und Änderungsmanagement der Institution entsprechen.

Es muss ein Verantwortlicher für die Durchführung und Überwachung der Datensicherungen sowie für die Wiederherstellungsübungen benannt werden. Dieser muss Fehlermeldungen in Bezug auf die Datensicherungen behandeln und Speicherplatzressourcen verwalten.

Die Datensicherungsanforderungen der Fernwartung müssen mit den allgemeinen Vorgaben der Institution zur Datensicherung korrespondieren und sollten die folgenden Kriterien berücksichtigen:

- Zeitintervalle (z. B. täglich, wöchentlich, monatlich),
- Zeitpunkte (z. B. nachts, freitags abends),
- die Anzahl der aufzubewahrenden Generationen,
- der Umfang der zu sichernden Daten,
- die Speichermedien (abhängig von der Datenmenge),
- die vorherige Löschung der Datenträger vor Wiederverwendung (z. B. bei Bändern oder Kassetten),
- die Zuständigkeit für die Durchführung der Datensicherung,
- die Zuständigkeit für die Überwachung der Sicherung, insbesondere bei automatischer Durchführung (z. B. Fehlermeldungen, verbleibender Platz auf den Speichermedien),
- die Dokumentation der erstellten Sicherungen (Datum, Art der Durchführung der Sicherung sowie gewählte Parameter, Beschriftung der Datenträger)

OPS.2.4.M14 Dedizierte Systeme bei der Fernwartung [IT-Betrieb]

Innerhalb der Fernwartung sollten Komponenten eingesetzt werden, die ausschließlich diesem Anwendungszweck dienen. Alle weiteren Funktionen und Dienste sollten deaktiviert werden. Durch die Umsetzung des Minimalprinzips wird automatisch auch die mögliche Angriffsfläche reduziert, die von Angreifern für Kompromittierungen genutzt werden könnten. Die dedizierten IT-Systeme stellen ihre Leistung und Ressourcen (z. B. RAM, CPU-Kapazität, Festplattenplatz) somit nur dem notwendigen Einsatzzweck zur Verfügung. Die Komponenten der Fernwartung sollten sicher konfiguriert sowie mit den aktuellsten Betriebssystem- und Anwendungssoftwareversionen betrieben werden.

OPS.2.4.M15 Absicherung der Fernwartung [IT-Betrieb]

Der direkte administrative Zugriff auf die IT-Systeme und Anwendungen über öffentliche Netze sollte im Grundsatz verboten und verhindert werden. Die Fernwartung sollte nur aus dem internen Netz (z. B. Institutionsstandort)über einen Kopplungs-Server erfolgen. Ein Kopplungs-Server (auch Jump Server) ist ein dediziertes gehärtetes IT-System, das verwendet wird, um Geräte in separaten Sicherheitszonen zu verwalten. Bei einem Zugriff über das öffentliche Netz sollte sich dieses System in einer sogenannten demilitarisierten Zone (DMZ) der Firewall befinden. Damit die übertragenen Informationen nicht abgehört oder gar manipuliert werden können, darf die Administration nur über sichere Protokolle (beispielsweise über SSH und HTTPS) erfolgen.

Bei Zugang über das öffentliche Netz erhält der Fernwartende nur die Möglichkeit, einen SSH- oder VPN-Tunnel (siehe NET.3.3 VPN) zum dedizierten System aufzubauen. Erst nach erfolgreicher Authentisierung öffnet ein Administrator aus dem inneren Netz einen entsprechenden Tunnel zwischen Wartungsobjekt und Kopplungs-Server und etabliert damit erst eine durchgehende Verbindung zwischen Fernwartendem und Wartungsobjekt (Rendezvous Prinzip). Die hierbei verwendeten Protokolle und Algorithmen sollten den Empfehlungen des BSI und den internen kryptographischen Vorgaben der Institution entsprechen.

Weitere Anforderungen beim Einsatz von VPN sind im Baustein *NET.3.3 VPN* beschrieben.

OPS.2.4.M16 Schulungen zur Fernwartung [IT-Betrieb]

Den Administratoren sollten ausreichende Kenntnisse im Umgang mit den Fernwartungskomponenten vermittelt werden. Diese Schulungsmaßnahmen sollten in die bereits etablierten Verfahren der Institution integriert werden.

Innerhalb der Sensibilisierungs- und Schulungsmaßnahmen sollten Grundlagen, Konzepte und Besonderheiten der Fernwartung sowie Kenntnisse über relevante Kommandos für die Einrichtung, Änderung und Löschung von Einstellungen innerhalb der Werkzeuge geschult werden. Die Schulungen sollten regelmäßig, z. B. einmal jährlich, oder bei Bedarf stattfinden. Alle Sensibilisierungs- und Schulungsmaßnahmen sollten dokumentiert werden.

Wichtige Aspekte bei der Planung der Sensibilisierung und Schulung von Administratoren der Fernwartung sind:

- Analyse der Zielgruppen für Sensibilisierungs- und Schulungsprogramme
- die Planung von Schulungsinhalten (z. B. Anforderungen an die Fernwartung auf Basis dieses Umsetzungshinweises, Gesetze, interne Regularien)
- Messung und Auswertung des Lernerfolgs
- Bekanntgabe von Ansprechpartnern zu Sicherheitsfragen

Die Themenfelder der Schulung müssen entsprechend dem Einsatzzweck des Werkzeuges angepasst werden. Die folgenden oder einer Kombination mehrerer Themenfelder können Inhalt der Schulung sein:

- Einsatz im Rahmen vom Problem- und Incident-Management
- Einsatz im Rahmen des Notfallmanagements
- Einsatz bei Sicherheitsvorfallbehandlungen
- Sensibilisierung der Mitarbeiter:
    - im Umgang mit Passwörtern
    - im Umgang mit dem Fernwartungswerkzeug
    - in der Umsetzung der Anforderungen bzgl. der Nutzung kryptographischer Verfahren
    - die Nutzung sicherer Protokolle
    - das Rechte- und Rollenkonzept
    - in der Vorgehensweise und dem Betrieb der Fernwartungsinfrastruktur und deren Werkzeuge
    - hinsichtlich den abhängigen prozessualen Schnittstellen sowie Anwendungsschnittstellen
    - der Durchführung von Datensicherungen

Die Mitarbeiter müssen darauf hingewiesen werden, was sie bei der Fernwartung zu beachten haben. Wenn IT-Systeme von Mitarbeitern fernadministriert werden, müssen sie der Fernwartung explizit zustimmen, z. B. über eine entsprechende Bestätigung am System. Außerdem müssen sie alle Tätigkeiten während der Fernwartung beobachten.

OPS.2.4.M17 Authentisierungsmechanismen bei der Fernwartung [IT-Betrieb]

Zur Fernwartung werden dem Schutzbedarf angemessene Mechanismen zur Identifikation und Authentisierung benötigt. Es sollte Zwei-Faktor-Authentisierung verwendet werden.

Die Auswahl der Authentisierungsmethode und die Gründe, die zu der Auswahl geführt haben, sollten dokumentiert werden. Bestehende Authentisierungsmechanismen der Institution dürfen durch die Fernwartung nicht umgangen werden. Zur Erleichterung der Anmeldung bei der Fernwartung empfiehlt es sich, diese in ein Identitäts- und Berechtigungsmanagement und deren Infrastruktur zu integrieren.

OPS.2.4.M18 Passwortsicherheit bei der Fernwartung [IT-Betrieb]

Falls bei der Fernwartung passwortbasierte Authentisierungen verwendet werden, sollten Passwortregeln definiert, dokumentiert und den Administratoren bekannt gemacht werden, um ein Mindestniveau der Passwortqualität sicherzustellen. Für die Fernwartung sollten diese Passwortregeln technisch forciert werden. Da für die Fernwartung Zwei-Faktor-Verfahren zur Authentisierung eingesetzt werden sollten, bietet das passwortbasierte Authentisierungsverfahren alleine nur einen Basisschutz.

Für die Passwortsicherheit innerhalb der Fernwartungsprozesse sollte eine Softwarelösung eingesetzt werden, die den Umgang mit vielen unterschiedlichen Passwörtern sowie das Erstellen sicherer Passwörter erleichtert. Da es viele differenzierte Passwort-Manager-Anwendungen gibt, sollte die Auswahl der Anwendung an Hand folgender Kriterien stattfinden:

- Aktueller Stand der Technik
- Komplexität der generierten Passwörter
- Unterscheidung nach Bedarf zwischen On- und Offline-Passwort-Manager
- Passwort-Manager mit Zwei-Faktor-Authentisierung
- Security Optionen (z. B. automatischer Log-Off)

OPS.2.4.M19 Fernwartung durch Dritte [IT-Betrieb]

Es kann verschiedene Gründe geben, warum die Fernwartung durch Dritte durchgeführt werden soll. Beispielsweise kann die Fernwartung zu den vereinbarten Serviceleistungen von Geräte-Herstellern gehören. Es können auch intern die erforderlichen Ressourcen oder das Fachwissen fehlen.

Fernwartung durch Dritte ist besonders kritisch. Sollte sie im Einzelfall notwendig sein sind folgende Punkte zu beachten:

- Im Grundsatz sollte eine Fernwartung durch Dritte nur passiv, also betrachtend sein.
- Alle durchgeführten Änderungen (z. B. der Konfigurationseinstellungen, innerhalb des Quellcodes) sollten dokumentiert werden. Diese Dokumentation muss der ferngewarteten Institution übergeben werden.
- Wenn dies technisch möglich ist, sollten alle Tätigkeiten während der Administration von Dritten durch eigene IT-Experten beobachtet werden. Beispielsweise können bei der Fernadministration eines Clients über eine graphische Benutzeroberfläche oft alle Ein- und Ausgaben am zu wartenden IT-System angezeigt und aufgezeichnet werden. Auch wenn Fernwartung durch Dritte genutzt wird, weil intern das Know-How oder die Kapazität nicht verfügbar ist, kann das externe Wartungspersonal nicht unbeaufsichtigt gelassen werden. Bei Unklarheiten über die Vorgänge sollte die Verbindung sofort unterbrochen bzw. auf betrachtenden Modus umgeschaltet werden. Danach können die Fragen geklärt werden.
- Es muss jederzeit die Möglichkeit geben, die Fernwartung lokal abzubrechen.
- Werden während der Wartung Daten oder Programme auf dem lokalen IT-System angelegt, so muss dies deutlich erkennbar und nachvollziehbar sein, also z. B. darf dies nur in besonders markierten Verzeichnissen oder unter bestimmten Benutzer-Kennungen erfolgen.
- Alle Fernwartungsvorgänge müssen aufgezeichnet werden. Dabei ist zumindest Anfang und Ende der Fernwartung sowie die Beteiligten festzuhalten. Wenn auf dem gewarteten IT-System niemand die Fernzugriffe beobachten kann, müssen alle Tätigkeiten bei der Durchführung der Fernwartung auf dem zu wartenden IT-System protokolliert werden.
- Für das externe Wartungspersonal müssen vertragliche Regelungen getroffen worden sein, vor allem über die Geheimhaltung von Daten (Vertraulichkeitsvereinbarungen). Insbesondere ist festzulegen, dass Daten, die im Rahmen der Wartung extern gespeichert wurden, nach Abschluss der Arbeiten sorgfältig gelöscht werden. Ebenso sind die Pflichten und Kompetenzen des externen Wartungspersonals sorgfältig festzulegen.

Bei höherem Schutzbedarf sollten außerdem die folgenden Maßnahmen ergriffen werden:

Vor Auswahl eines Fernwartungspartners sollten Informationen über dessen Zuverlässigkeit und weiterführende Informationen eingeholt werden. Im Rahmen der betrieblichen, sicherheitstechnischen, datenschutzrechtlichen Vereinbarungen sowie der Zusammenarbeit in Notfällen sollten beispielsweise die Anforderungen an die zu erfüllenden Service Level Agreements (SLAs, Dienstgütevereinbarungen) übergeben werden. Darüber hinaus sollten Abstimmungen hinsichtlich der zu erfüllenden Netzsegmentierungs- und Separierungsvorgaben sowie die erwarteten Schutzmechanismen für die Clients und den zugrundeliegenden Betriebssystemen getroffen werden. Die Institution sollte mit dem Dienstleister vertraglich entsprechende Kontrollmechanismen der vereinbarten Services festlegen.

In Bezug auf das Identitäts- und Berechtigungsmanagement gilt bei der Auswahl des Fernwartungsdienstleisters, das dieser nie mehr Rechte erhalten darf, als er für die Erfüllung seiner Aufgaben unbedingt benötigt und das sich jeder Mitarbeiter des Dienstleisters über eine eindeutige personalisierte Benutzerkennung authentisieren muss.

Da die Institution als Dienstleistungsnehmer keinen direkten Einfluss auf die Arbeitsweise des Dienstleisters und dessen Personal besitzt, können sich durch mögliche Nachlässigkeiten oder Unzuverlässigkeiten unkontrollierbare Risiken ergeben. Um diese Risiken zu minimieren, sollten vertragliche Vereinbarungen zu mindestens den folgenden Themenfeldern benannt werden:

- gemeinsames Risikomanagement durch die enge Verzahnung der Fernwartungssysteme des Dienstleisters mit den Systemen der Institution
- Sicherheitsvorfallerkennung und -behandlung
- gemeinsames Notfallmanagement inklusive der Benennung der Business Impact Analyse Werte (BIA-Werte)
- eine Vertraulichkeitsvereinbarung,
- Festlegung der Kompetenzen und Pflichten
- Festlegungen bezüglich Backup und Archivierungsanforderungen
- eine genaue Beschreibung, wie die IT-Systeme des Dienstleisters geschützt werden,
- Festlegungen rund um die Möglichkeit der Auditierung
- Festlegungen zum Zwecke der Einbindung in die Überwachungs- und Protokollierungsinfrastruktur der Institutionsstandorte
- Übergabe bzw. bestätigte Vernichtung (Vernichtungserklärung) der Backup- und Archivierungsdaten im Rahmen der Fernwartung nach Vertragsbeendigung

Weitere Informationen für den Betrieb der Fernwartung durch Dritte sind in den Bausteinen OPS.2.1 Outsourcing-Nutzung und OPS.3.1 Outsourcing-Anbieter beschrieben.

OPS.2.4.M20 Betrieb der Fernwartung [IT-Betrieb]

Damit der Betrieb der IT-Systeme und Anwendungen durch die Fernwartung gewährleistet werden kann, sollten die Initiative zum Aufbau einer Support- oder Fernwartungssession immer von den Benutzern der betreuten IT-Komponenten ausgehen. Da diese direkt mit den IT-Systemen und Anwendungen arbeiten, sollte ein Meldeprozess für Support- und Fernwartungsanliegen etabliert werden (z. B. Ticketsystem). Alle Zugriffe durch die Fernwartung sollten erst nach erfolgreicher Authentisierung gestattet werden.

Die zur Etablierung der Fernwartungszugänge erforderlichen Freischaltungen an der Sicherheitsinfrastruktur sollte in die etablierten Prozesse für Firewall-Regeln integriert werden. Die Integration der Fernwartung in die Sicherheitsinfrastruktur sollte alle Angaben des Bausteins *NET.3.2 Firewall* berücksichtigen.

Ein Fernwartungsdienstleister sollte keinen Zugriff auf IT-Systeme und Anwendungen außerhalb des für die jeweilige Fernwartung notwendigen erhalten. Um sicherzustellen, dass nur berechtigte Zugriffe durch Administratoren möglich sind, sollte die Kommunikation zwischen Fernwartungserver und -client mittels einer Stateful-Firewall, besser einer Firewall-NG, verifiziert werden.

Darüber hinaus sollte überlegt werden, am zu wartenden IT-System noch weitere Funktionalitäten zu implementieren:

- Wenn eine Fernwartung durch Dritte nicht überwacht wird: Sperren der Fernwartung im Normalbetrieb und explizite Freigabe für eine genau definierte Zeitspanne,
- Einschränkung der Rechte der Administratoren: Die Administratoren sollten nicht die vollen Administrator-Rechte besitzen. Es sollte eine abgestufte Rechteverwaltung realisiert werden. Die Administratoren sollte nur auf die Daten und Verzeichnisse Zugriff haben, die aktuell von der Fernwartung betroffen sind.
- Sollte die Session ohne die Einwirkung der Administratoren unterbrochen werden, sollte der Wiederaufnahme der Verbindung eine erneute Authentisierung vorangehen.

Darüber hinaus sollten die nachfolgenden Hinweise beachtet werden.

Alle Fernwartungsvorgänge müssen aufgezeichnet werden. Dabei ist zumindest Anfang und Ende der Fernwartung sowie die Beteiligten festzuhalten. Wenn auf dem gewarteten IT-System niemand die Fernzugriffe beobachten kann, müssen alle Tätigkeiten bei der Durchführung der Fernwartung auf dem zu wartenden IT-System protokolliert werden. Die anfallenden Protokolldaten sollten regelmäßig ausgewertet werden.

Wenn ein Security Information and Event Management (SIEM) vorhanden ist, sollten die Protokolldaten zur Überprüfung auf Sicherheitsvorfälle an dieses übermittelt werden.

Nach einer definierten Anzahl von Fehlversuchen sollte eine temporäre Sperre des Zuganges zur Fernwartung aktiviert werden. Anders als in der konventionellen IT sind mit Blick auf die besonderen Anforderungen der Fernwartung hinsichtlich Verfügbarkeit solche Sperren aber beispielsweise nicht erst nach zwanzig, sondern bereits nach drei Fehlversuchen vorzunehmen.

Ein erfolgreicher DoS- oder DDoS-Angriff kommt einer Einladung zu weiteren Angriffen auf die IT-Systeme der Institution und beteiligten Dienstleistern gleich. Aus diesem Grund sollten Mechanismen zur Erkennung und Abwehr von hochvolumigen Angriffen, TCP-State-Exhaustion Angriffen und Angriffen auf Applikationsebene implementiert sein. Mögliche Maßnahmen gegen diese Art der Angriffe sind nicht Bestandteil dieser Umsetzungshinweise, werden jedoch in den Umsetzungshinweisen der Bausteine *NET.3.1 Router/Switche* und *NET.3.2Firewall* beschrieben.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

OPS.2.4.M21 Erstellen eines Notfallplans für den Ausfall der Fernwartung (A)

Im Rahmen der Notfallvorsorge sollte ein Konzept entwickelt werden, wie die Folgen eines Ausfalls von Fernwartungskomponenten minimiert werden können und welche Aktivitäten im Falle eines Ausfalls durchzuführen sind. Durch den Notfallplan sollte sichergestellt sein, dass Störungen, Schäden und Folgeschäden minimiert werden sowie eine zeitnahe Wiederherstellung des Normalbetriebs erfolgt. Bei Hochverfügbarkeit sollte die Infrastruktur der Fernwartung mittels einer Business Impact Analyse auf Kritikalität geprüft werden.

Weitere Aspekte der Notfallplanung werden im Baustein im Baustein *DER.4 Notfallmanagement* behandelt.

OPS.2.4.M22 Redundante Verwendung von mobilen Kommunikationsnetzen (A)

Für den Schutz der Kommunikationsnetze der Fernwartung bei Hochverfügbarkeitsanforderungen sollten redundante Verbindungs- bzw. Kommunikationsnetze eingerichtet werden. Es sollten geregelt werden, ob hierfür externe Telekommunikationsnetze genutzt werden sollen, z. B. über Mobilfunk.

Die internen IT-Systeme der Institution sollten neben den etablierten produktiven Wegen zusätzlich über ein nicht produktiv genutztes Fallback-Zugangsnetz erreichbar sein. Der Fallback-Zugang könnte zum Beispiel über eine DSL- oder LTE-Verbindung realisiert sein beziehungsweise durch eine Festnetzverbindung.

OPS.2.4.M23 Planung des sicheren Einsatzes in einem abgesicherten Netzsegment [IT-Betrieb] (C)

Für die Fernwartung sollte ein abgesichertes Netzsegment eingesetzt werden, dieses sollte in der Art wie eine *Demilitarized Zone* (*DMZ) realisiert und betrieben werden.*

Im Bereich der Fernwartung sollten sich alle Fernwartungskomponenten möglichst im abgesicherten Netzsegment befinden und nicht direkt im internen Netz lokalisiert sein. Dadurch kann die Ausbreitung aus einem nicht vertraulichen Netz in das Netz mit dem Fernwartungssystem geschützt werden, wenn dazwischen entsprechende Analysewerkzeuge und Tools integriert sind.

Die Fernwartungszugänge sollten nicht dazu führen, dass vorhandene Sicherheitsinfrastrukturen umgangen werden und so ein Zusammenschluss von vertrauenswürdigen und nicht vertrauenswürdigen Netzen erfolgt.

3 Weiterführende Informationen

3.1 Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Fernwartung" finden sich unter anderem in folgenden Veröffentlichungen:

[CSE108] Fernwartung im industriellen Umfeld

BSI-Veröffentlichungen zur Cyber-Sicherheit (CSE 108), Version 1.0, Januar 2015, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_108.pdf, zuletzt abgerufen am 05.10.2018

[CSE54] Grundregeln zur Absicherung von Fernwartungszugängen

BSI-Veröffentlichungen zur Cyber-Sicherheit (BSI-CS 054), Version 1.0, Juni 2013,
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_054.pdf, zuletzt abgerufen am 05.10.2018

[TR02102] Kryptographische Verfahren

Empfehlungen und Schlüssellängen: BSI TR-02102, Bundesamt für Sicherheit in der Informationstechnik (BSI), Januar 2018, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html , zuletzt abgerufen am 13.09.2018

Umsetzungshinweise zum Baustein OPS.3.1 Outsourcing für Dienstleister

1 Beschreibung

1.1 Einleitung

Immer mehr Institutionen entscheiden sich heutzutage, bestimmte Prozesse und Aktivitäten nicht mehr vollständig selbst zu erbringen, sondern diese an einen externen Dienstleister auszulagern. Diese Entscheidung wird in der Regel aufgrund der vielfältigen Möglichkeiten getroffen, welche ein solches Outsourcing-Vorhaben mit sich bringen kann. So können je nach vorhandenen Rahmenbedingungen eventuell Kosten gespart, externe Ressourcen flexibel genutzt oder eine Entlastung der eigenen Ressourcen erreicht werden, um sich stärker auf die eigenen Kernkompetenzen konzentrieren zu können. Jene Chancen gehen jedoch stets mit zum Teil erheblichen Risiken einher (hohe Abhängigkeit von externen Dienstleistern, Verlust von Kontroll- und Steuerungsmöglichkeiten sowie Risiken für die Informationssicherheit), die eine Outsourcing-Dienstleistung nicht nur scheitern lassen, sondern im schlechtesten Fall auch die Existenz der auslagernden Institution gefährden können. Umso mehr ist es von Bedeutung, jeglichen Risiken, welche mit der Outsourcing-Dienstleistung einhergehen, ausreichend zu begegnen. Um diese Zielsetzung angemessen umsetzen zu können, ist eine enge Zusammenarbeit zwischen dem Outsourcing-Dienstleister und dem Outsourcing-Kunden unerlässlich. Der Erfolg des Outsourcing-Vorhabens liegt dabei nicht nur im Interesse der auslagernden Institution. Vielmehr hat auch der Outsourcing-Dienstleister ein großes Interesse daran, dass die Outsourcing-Ziele des Kunden zu dessen vollsten Zufriedenheit erfüllt werden. Eine Verfehlung der an den Dienstleister gestellten Anforderungen kann mitunter hohe Vertragsstrafen und weitere juristische Auswirkungen zur Folge haben, die sich nicht nur finanziell erheblich auf den Dienstleister auswirken können, sondern auch dessen Reputation nachhaltig schädigen können.

Aufgrund dieser Risiken werden nachfolgend Maßnahmen beschrieben, die der Outsourcing-Dienstleister im Rahmen jeder Phase einer Outsourcing-Dienstleistung beachten bzw. umsetzen sollte.

1.2 Lebenszyklus

Zur Realisierung einer Outsourcing-Dienstleistung sind sowohl von der auslagernden Stelle als auch von Seiten des Outsourcing-Dienstleisters eine Reihe von Maßnahmen umzusetzen, um den ordnungsgemäßen Verlauf und somit den Erfolg einer Outsourcing-Dienstleistung sicherzustellen. Beginnend mit der Erstellung eines Grobkonzepts für die Outsourcing-Dienstleistung über die Vertragsgestaltung mit dem Outsourcing-Kunden bis hin zur sicheren Migration und dem Übergang in den Regelbetrieb ist dabei einer Vielzahl von Sicherheitsrisiken zu begegnen. Im Folgenden werden aus Sicht des Dienstleisters die Schritte eines Outsourcings und deren einzelnen Maßnahmen aufgeführt.

Planung und Konzeption

Um den Erfolg einer Outsourcing-Dienstleistung zu fördern, gilt es bereits im Vorfeld der eigentlichen Auslagerung gleichermaßen für den Dienstleister als auch den Kunden, alle notwendigen Rahmenbedingungen für das gemeinsame Projekt abzustimmen und festzulegen. Das Grobkonzept für die Outsourcing-Dienstleistung ist hierfür die Grundlage (siehe OPS.3.1.M1 Erstellung eines Grobkonzepts für die Outsourcing-Dienstleistung). Individuelle und allgemeine Risiken, die mit der jeweiligen Outsourcing-Dienstleistung verbunden sind, müssen erkannt und deren Behandlung muss – gemeinsam mit dem Kunden – abgestimmt werden.

Umsetzung

Um eine anforderungsgerechte Leistungserbringung sicherzustellen, sind Vereinbarungen wie Leistungsbeschreibungen und Sicherheitsanforderungen etc. im Vorfeld vertraglich festzulegen (siehe OPS.3.1.M2 Vertragsgestaltung mit dem Outsourcing-Kunden). Zudem sollten die Sicherheitsanforderungen des Kunden im Zuge des gesamten Outsourcing-Prozesses erfüllt und die dafür benötigten Ressourcen vorgehalten werden (siehe unter anderem OPS.3.1.M3 Erstellung eines Sicherheitskonzepts für die Outsourcing-Dienstleistung, OPS.3.2.M13 Sichere Migration bei Outsourcing-Vorhaben).

Betrieb

Neben der kontinuierlichen Leistungserbringung gemäß der vertraglich fixierten Service Level Agreements (SLAs) muss für die gesamte Betriebsphase eine mit dem Kunden abgestimmte Sicherheitskultur gelebt werden. Diese ist durch einen regelmäßigen und anlassbezogenen Informationsaustausch und eine regelmäßige Kontrolle der Umsetzung und Wirksamkeit vereinbarter Sicherheitsmaßnahmen zu gewährleisten (OPS.3.1.M10 Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb).

Aussonderung

Des Weiteren müssen Vorbereitungen für eine geplante bzw. ungeplante Beendigung der Outsourcing-Dienstleistung getroffen werden, sodass eine ordnungsgemäße Rückführung der ausgelagerten Prozesse bzw. eine Übertragung dieser auf einen Dritten möglich ist (siehe OPS.3.1.M15 Geordnete Beendigung eines Outsourcing-Verhältnisses).

Notfallvorsorge

Bereits zur Vertragsgestaltung müssen die wesentlichen Aspekte zur Notfallvorsorge besprochen und vertraglich vereinbart werden (siehe OPS.3.1.M2 Vertragsgestaltung mit dem Outsourcing-Kunden). Die genauen Regelungen sollten zwischen beiden Vertragsparteien in einem Notfallvorsorgekonzept erarbeitet, aufeinander abgestimmt und regelmäßig geprüft und getestet werden (siehe OPS.3.1.M14 Notfallvorsorge beim Outsourcing).

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Outsourcing für Dienstleister" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

OPS.3.1.M1 Erstellung eines Grobkonzeptes für die Outsourcing-Dienstleistung

Der Outsourcing-Dienstleister muss gemeinsam mit dem Outsourcing-Kunden in einem Grobkonzept mögliche Interaktionsprozesse, Regelungen und Richtlinien festlegen, auf denen die Zusammenarbeit basiert. Es definiert das Outsourcing-Management mit den Führungs- und Kontrollfunktionen sowie Schnittstellen zwischen den Parteien und zu anderen Prozessen (z. B. Notfallmanagement, Informationssicherheit und Datenschutz), um so eine transparente Outsourcing Governance in nachvollziehbarer Weise abzubilden und eine schnelle Reaktion auf Ereignisse zu ermöglichen.

Das Konzept sollte ebenfalls die Betrachtung der folgenden Faktoren einschließen:

Ziele des Outsourcing-Vorhabens

Es ist zu definieren, welche Chancen und Ziele der Outsourcing-Kunde mit dem Vorhaben verbindet, welche Mehrwerte geschaffen werden sollen und wie der Projekterfolg gemessen werden kann. So sollen spezifische, messbare und realistische Ziele in einem vordefinierten Zeitrahmen erreicht werden. Um eine Aussage darüber treffen zu können, ob die Outsourcing-Dienstleistung erfolgreich verläuft, muss die Leistung des Outsourcing-Dienstleisters gegenüber dem Outsourcing-Kunden nachvollziehbar darstellbar sein.

Bei den Zielen eines Outsourcing-Vorhabens müssen insbesondere die Ziele mit Bezug auf Informationssicherheit berücksichtigt werden. Um diese Ziele messen zu können eignen sich sogenannte Security Service Level Agreements. Diese sollten im Sicherheitskonzept schriftlich fixiert und in regelmäßigen Abständen geprüft werden.

Für den Outsourcing-Dienstleister ist es in jedem Fall von Interesse, bei der Definition dieser Messgrößen mitzuwirken, da mittels dieser die Qualität seiner Leistungserbringung gemessen werden soll.

Mögliche Messgrößen für quantifizierbare Leistungsbewertungen könnten sein:

- Meilensteine des Outsourcing-Vorhabens (z. B. Planung, Migration, Betrieb)
- Security Level Agreements (z. B. Angaben zur Verfügbarkeit)

Qualitäten des Outsourcing-Dienstleisters

Die Anforderungen an die – von den Outsourcing-Dienstleisters erbrachten – Services sind anwenderspezifisch und individuell. Eine Vorabbetrachtung der Erwartungen des Outsourcing-Kunden, z. B. hinsichtlich der Kapazitäten und Verfügbarkeiten der Services, kann vor dem Beginn der Vertragsverhandlungen Missverständnisse vermeiden.

Der Outsourcing-Dienstleister sollte gegenüber dem Outsourcing-Kunden idealerweise Qualitäten präsentieren können. Zu den Qualitäten eines Outsourcing-Dienstleisters kann z. B. gehören, dass eine gültige ISMS-Zertifizierung vorliegt, die bereits den Anwendungsbereich des Outsourcing-Kunden abdeckt. Aber auch Referenz-Kunden, die der Outsourcing-Kunde bei Bedarf vor Vertragsunterzeichnung kontaktieren kann, können sinnvoll sein, um die eigenen Qualitäten im Umgang mit Informationssicherheit zu präsentieren.

Abhängigkeiten von externen Drittparteien

In einer komplex vernetzten Geschäftswelt mit einem hohen Spezialisierungsgrad bestehen viele Abhängigkeiten. In der Regel setzt der Outsourcing-Dienstleister ebenfalls weitere Drittparteien ein, um z. B. Wartungen an verschiedenen Anlagen durchführen zu lassen. Diese Abhängigkeiten sollten von Seiten des Outsourcing-Dienstleisters dem Outsourcing-Kunden bereits vor der Vertragsunterzeichnung mitgeteilt werden.

Diese Interdependenzen bei der Serviceerbringung sollten in der nötigen Detailtiefe dargestellt werden, um auch hier mögliche Risiken zu erfassen und diese entsprechend behandeln zu können. Eine Unterbrechung der Service-Erbringung durch den Outsourcing-Dienstleister kann empfindliche Vertragsstrafen nach sich ziehen und der Reputation schaden. Zudem ist eine offene Kommunikation hinsichtlich möglicher Risiken Grundlage einer erfolgreichen Outsourcing-Beziehung.

Durch den Outsourcing-Dienstleister sind z. B. darzustellen:

- Kritische Geschäftsprozesse, die im Rahmen eines Outsourcings an Dritte vergeben sind
  - Insbesondere bestehende IT-Outsourcing-Verträge
  - Externe Datenhaltung (Dienstleister, Standort[e])
- Telekommunikationsanbieter
- Kooperation mit Dritten im Zusammenhang mit der Notfallvorsorge (z. B. Ausweicharbeitsplätze)

Sicherheitskultur

Ein wichtiger Faktor bei einer langfristigen Bindung im Rahmen einer Outsourcing-Dienstleistung ist die Beachtung der unterschiedlichen Sicherheitskulturen. Hierzu sollte die Sicherheitskultur sowohl des Outsourcing-Dienstleisters als auch des Outsourcing-Kunden reflektierend in den Blick genommen werden. Zu beachten sind beispielsweise:

- Gesellschaftlich-kulturelle Unterschiede und Gemeinsamkeiten, die auch die Organisationskultur prägen
- Unternehmenswerte und -visionen
- Führungs- und Entscheidungsstile
- Formelle und informelle soziale Codes
- Ethische Standards
- Einstellung zu Risiken, Risikoappetit

Insbesondere der sichere Umgang mit Daten und Informationen seitens der Mitarbeiter des Outsourcing-Dienstleisters sollten klar geregelt sein. Der Outsourcing-Kunde verlässt sich in erster Linie auf die Zuverlässigkeit des Outsourcing-Dienstleisters bei der Auswahl seiner Mitarbeiter. Der Outsourcing-Dienstleister sollte bei der Zuordnung von Aufgaben zu Mitarbeitern deshalb auf das Arbeitsklima in den jeweiligen Teams achten.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Outsourcing für Dienstleister".

OPS.3.1.M2 Vertragsgestaltung mit den Outsourcing-Kunden

Bei der Gestaltung von Outsourcing-Verträgen ist darauf zu achten, alle Aspekte eines Outsourcing-Verfahrens bei der Vertragsgestaltung durch sogenannte Service Level Agreements (SLAs) zu berücksichtigen und gemeinsam mit dem Outsourcing-Kunden eine genaue Analyse der Aufgaben und Prozesse, die übernommen werden sollen, durchzuführen. Alle nicht im Vorhinein definierten Merkmale der Leistungserbringung führen meist zu Mehrkosten, insbesondere beim Outsourcing-Kunden. Das schädigt das Geschäftsverhältnis zwischen den Vertragsparteien und schwächt die Verhandlungsposition des Outsourcing-Dienstleisters bei Vertragsverlängerungen.

Um diesem Umstand Rechnung zu tragen, ist es empfehlenswert, alle relevanten Leistungsbeschreibungen für die Outsourcing-Dienstleistung im Vertragswerk zu berücksichtigen und möglichst genau zu definieren. Dies ist insbesondere dahingehend von besonderer Bedeutung, dass eventuelle Diskrepanzen zwischen dem Outsourcing-Dienstleister und dem Outsourcing-Kunden hinsichtlich unterschiedlicher Vorstellungen der Leistungserbringung im Zuge des Outsourcing-Projektes bereits im Vorfeld verhindert werden können. Bei unrechtmäßigen Vorwürfen seitens des Outsourcing-Kunden in Hinsicht auf eine nicht oder nur mangelhaft erbrachte Leistung kann der Outsourcing-Kunde sich auf die entsprechende Leistungsbeschreibung im Rahmen des Vertragswerkes berufen.

Art, Umfang und Detaillierungsgrad der vertraglichen Regelungen hängen dabei immer von der jeweiligen Outsourcing-Dienstleistung ab. Je höher beispielsweise der Schutzbedarf der ausgelagerten IT-Systeme und Anwendungen des Outsourcing-Kunden ist, desto sorgfältiger und detaillierter muss der Vertrag zwischen Outsourcing-Kunden und Outsourcing-Dienstleister in Hinsicht auf die zu ergreifenden Sicherheitsmaßnahmen ausgehandelt werden. So hat der Outsourcing-Dienstleister über die Einhaltung der Anforderungen aus dem IT-Grundschutz-Kompendium hinaus oftmals zusätzliche Sicherheitsanforderungen aufgrund von einem erhöhten Schutzbedarf zu erfüllen (siehe unter anderem OPS.3.1.A3 Erstellung eines Sicherheitskonzepts für die Outsourcing-Dienstleistung).

Folgende aufgelistete Aspekte sollten aus Sicht des Outsourcing-Dienstleisters bei der Vertragsgestaltung geregelt werden, um die Leistungserbringung entsprechend klarer Vorgaben von Seiten des Outsourcing-Kunden gewährleisten zu können. Der Übersicht halber sind die beschriebenen Aspekte den jeweiligen Themenbereichen zugeordnet. Weitere Hinweise und Details können in diversen Bausteinen des IT-Grundschutz-Kompendiums entnommen werden:

Infrastruktur (siehe z. B. Baustein INF.2 Rechenzentrum)

- Umfang der gemeinsam genutzten Infrastruktur
- Anforderungen des Outsourcing-Kunden an die Absicherung der gemeinsam genutzten Infrastruktur
- Verbleib der Eigentumsrechte aller Bestandteile der Infrastruktur

Organisatorische Regelungen / Prozesse (siehe z. B. Baustein ORP.1 Organisation)

- Vertraulichkeitsvereinbarungen (Non-Disclosure Agreements) sind vertraglich zu fixieren. Dies sollte bereits in der Phase der Vertragsgestaltung selbst berücksichtigt werden, da Sicherheitsanforderungen des Outsourcing-Kunden unter Umständen Schlüsse auf die vorhandenen Sicherheitssysteme zulassen.
- Festlegung von Kommunikationswegen und Ansprechpartnern
- Festlegung von Prozessen, Arbeitsabläufen und Zuständigkeiten
- Integration der Dienstleistung in den Wertschöpfungsprozess des Outsourcing-Kunden
- Arbeitsteilung bei der Serviceerbringung / Mitwirkungspflichten des Outsourcing-Kunden
- Verfahren zur Behebung von Problemen, Benennung von Ansprechpartnern mit den nötigen Befugnissen bei beiden Vertragsparteien
- Regelmäßige Abstimmungsrunden
- Vorgehensweise bei der Leistungsanpassung
- Archivierung und Löschung von Datenbeständen (insbesondere bei Beendigung des Vertragsverhältnisses)
- Zugriffsmöglichkeiten des Outsourcing-Dienstleisters auf IT-Ressourcen des Outsourcing-Kunden: Wer greift wie auf welches System zu? Wie sind die Zuständigkeiten und Rechte?
- Zutritts- und Zugriffsberechtigungen für Mitarbeiter des Outsourcing-Dienstleisters zu den Räumlichkeiten und IT-Systemen des Outsourcing-Kunden
- Zutritts- und Zugriffsberechtigungen für Mitarbeiter des Outsourcing-Kunden zu den Räumlichkeiten und IT-Systemen des Outsourcing-Dienstleisters
- physischer Aufbewahrungsort von Daten

Personal (siehe z. B. Baustein ORP.2 Personal)

- Gestaltung der Arbeitsplätze von Mitarbeitern des Outsourcing-Dienstleisters, die zum Outsourcing-Kunden entsandt werden (z. B. die Einhaltung der Bildschirmarbeitsplatzrichtlinie)
- Festlegung und Abstimmung von Vertretungsregelungen bei beiden Vertragspartnern
- Verpflichtung zu Fortbildungsmaßnahmen

Notfallvorsorge (siehe z. B. Baustein DERr.4 Notfallmanagement)

- Kategorien zur Einteilung von Fehlern und Störfällen nach Art, Schwere und Dringlichkeit
- Erforderliche Handlungen beim Eintreten eines Störfalls
- Vom Outsourcing-Kunden geforderte Reaktionszeiten und Eskalationsstufen
- Zeitnahe Information des Outsourcing-Kunden über eingetretene Sicherheitsvorfälle
- Mitwirkungspflicht des Outsourcing-Kunden bei der Behebung von Notfällen
- Art der Einbindung in Notfallübungen und zeitliche Abfolge von Notfallübungen des Outsourcing-Kunden
- Anforderungen des Outsourcing-Kunden an die Art und den Umfang der Datensicherung
- Vereinbarung, ob bzw. welche Systeme redundant ausgelegt sein müssen

Von besonderer Bedeutung können Regelungen für Fälle höherer Gewalt sein. Des Weiteren sollte beispielsweise geklärt sein, wie bei einem Streik des Personals des Outsourcing-Dienstleisters die Verfügbarkeit von Daten und Systemen sichergestellt werden kann. Besonders wenn Outsourcing-Dienstleister und Outsourcing-Kunde unterschiedlichen Branchen angehören oder ihren Sitz in verschiedenen Ländern haben, kann der Outsourcing-Kunden von derartigen Vorkommnissen gänzlich überrascht werden.

Juristische Rahmenbedingungen, Haftung

Die Möglichkeiten des Outsourcing-Dienstleisters Dritte, Subunternehmer und Unterauftragnehmer in die Leistungserbringung einzubinden, sind zu regeln. Allgemein empfiehlt es sich nicht, diese grundsätzlich auszuschließen, sondern sinnvolle Rahmenbedingungen festzulegen.

Die Eigentums- und Urheberrechte an Systemen, Software und Schnittstellen sind festzulegen. Zudem ist die Weiterverwendung der vom Outsourcing-Dienstleister eingesetzten Tools, Prozeduren, Skripte und anderer Software für den Fall der Beendigung des Dienstleistungsverhältnisses zu regeln.

Es sind angemessene Kündigungsfristen zu vereinbaren. In diesem Zusammenhang sollte darauf geachtet werden, dass innerhalb der Kündigungsfristen ausreichend Zeit für den Outsourcing-Kunden bleibt, die ausgelagerten Prozesse wieder selbst zu übernehmen oder auf einen anderen Dienstleister zu übertragen (15 Geordnete Beendigung eines Outsourcing-Verhältnisses).

Oftmals sind Outsourcing-Kunden bestrebt, Sanktionen oder Schadensersatzpflichten für eine eventuelle Nichteinhaltung der Dienstleistungsqualität festzulegen. Aus Sicht des Outsourcing-Dienstleisters sind dahingehend folgende Aspekte zu berücksichtigen bzw. mit dem Outsourcing-Kunden zu regeln:

- Quantifizierbarkeit eines eingetretenen Schadens
- Messbarkeit eines Imageschadens
- Verfahren bei Insolvenz des Outsourcing-Dienstleisters
- Verfahren bei Eintreten von katastrophalen Schäden

Weiterverlagerungen

Die Möglichkeiten zur Einbindung von Dritten, Subunternehmern und Unterauftragnehmern durch den Outsourcing-Dienstleister sind zu regeln. Allgemein empfiehlt es sich, dies nicht grundsätzlich auszuschließen, sondern sinnvolle Bedingungen festzulegen. Grundsätzlich sollte jede Weiterverlagerung nur dann zulässig sein, wenn alle Anforderungen erfüllt werden, die im Rahmen der bestehenden Outsourcing-Beziehung an den Dienstleister gestellt werden.

Mandantenfähigkeit

Die Anforderungen hinsichtlich einer Trennung von IT-Systemen und Anwendungen verschiedener Kunden des Outsourcing-Dienstleisters müssen in einem Mandantenkonzept geregelt werden (siehe OPS.3.1.M10 Planung der Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb). Anhand dieser Regelungen ist es dem Outsourcing-Dienstleister im weiteren Projektverlauf möglich, eine anforderungsgerechte Mandantentrennung zu gewährleisten.

Falls notwendig, muss die physikalische Trennung (d. h. dedizierte Hardware) vereinbart werden.

Falls notwendig, muss vereinbart werden, dass die vom Outsourcing-Dienstleister eingesetzten Mitarbeiter nicht für andere Outsourcing-Kunden eingesetzt werden. Es kann auch sinnvoll sein, diese auf Verschwiegenheit zu verpflichten, sodass die eingesetzten Mitarbeiter nicht mit anderen Mitarbeitern des Outsourcing-Dienstleisters anwenderbezogene Informationen austauschen dürfen.

Änderungsmanagement und Testverfahren

Es müssen Regelungen gefunden werden, die es ermöglichen, dass der Outsourcing-Kunde immer in der Lage ist, sich neuen Anforderungen anzupassen. Dies gilt insbesondere, wenn beispielsweise gesetzliche Vorgaben geändert wurden. Es ist festzulegen, wie auf Systemerweiterungen, gestiegene Anforderungen oder knapp werdende Ressourcen reagiert werden soll.

In diesem Zusammenhang ist auch die Betreuung und Weiterentwicklung bereits vorhandener Systeme zu regeln. Nicht selten übernimmt der Outsourcing-Dienstleister selbst entwickelte Systeme oder Software vom Outsourcing-Kunden, der damit die Fähigkeit verliert, diese in seinem Sinne weiterzuentwickeln. Der Evolutionspfad von Systemen muss daher geregelt werden.

Der vom Outsourcing-Kunden geforderte Zeitrahmen für die Behebung von Fehlern und Störungen ist festzulegen.

In Hinsicht auf Testverfahren für neue Hard- und Software sind die von Seiten des Outsourcing-Dienstleisters einzuhaltenden Regelungen zu vereinbaren. Dabei sollten insbesondere folgende Aspekte geklärt werden:

- Regelungen für Updates und Systemanpassungen
- Trennung von Test- und Produktionssystemen
- Zuständigkeiten bei der Erstellung von Testkonzepten
- Festlegen von zu benutzenden Testmodellen
- Zuständigkeiten bei Outsourcing-Kunden und Outsourcing-Dienstleister für die Erstellung von Testkonzepten und die Durchführung von Tests (z. B. Mitarbeit oder Hilfestellung des Outsourcing-Kunden, Abnahme- und Freigabeprozeduren)
- Informationspflicht und Absprache vor wichtigen Eingriffen ins System (Negativbeispiel: Der Dienstleister spielt eine neue Version des Betriebssystems auf dem Server ein. Durch unerwartete Fehler dabei werden wichtige Anwendungen gestört, ohne dass der Kunde sich vorbereiten konnte.)
- Genehmigungsverfahren für die Durchführung von Tests
- Festlegung zumutbarer Qualitätseinbußen während der Testphase (z. B. Verfügbarkeit)

Kontrollen und Prüfungen

Die Dienstleistungsqualität und Informationssicherheit müssen regelmäßig kontrolliert werden. Der Dienstleister muss daher mit dem Kunden abstimmen, welche Auskunfts-, Einsichts-, Zutritts- und Zugangsrechte eingeräumt werden. Wenn unabhängige Dritte Audits oder Benchmark-Tests durchführen sollen, muss dies ebenfalls im Vertrag geregelt werden.

Der Dienstleister muss allen Institutionen, die beim Kunden Prüfungen durchführen müssen (z. B. Aufsichtsbehörden), entsprechende Kontrollmöglichkeiten (z. B. Zutrittsrechte, Dateneinsicht) einräumen.

OPS.3.1.M3 Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben

Der Outsourcing-Kunde sollte ein eigenes Sicherheitskonzept für das Outsourcing-Vorhaben erstellen (siehe Baustein OPS.2.1 Outsourcing für Kunden). Dieses bildet die Grundlage für die Sicherheitsanforderungen an den Outsourcing-Dienstleister im Rahmen des gemeinsamen Outsourcing-Projektes. Der Outsourcing-Dienstleister sollte aufbauend darauf ein Sicherheitskonzept für das jeweilige Outsourcing-Vorhaben erstellen und kontinuierlich fortschreiben. Die folgenden allgemeinen Aspekte sind darin zu berücksichtigen:

- Einflussbereich und Mitwirkungspflichten des Outsourcing-Kunden
- Schnittstellen und Kommunikation zwischen den Outsourcing-Partnern, aber auch zwischen dem Anwendungsbereich des Outsourcing-Kunden wie auch den Anwendungsbereichen der anderen Kunden
- Abgestimmter Informationsverbund mit klarer Abgrenzung zum Sicherheitskonzept des Outsourcing-Kunden

Der Outsourcing-Kunde sollte alle schutzbedürftigen Informationen entsprechend ihrer strategischen Bedeutung für seine Institution klassifizieren und diesen Schutzbedarf dem Outsourcing-Dienstleister kommunizieren. Darauf aufbauend sollte eine gemeinsame Klassifikation erarbeitet werden. Die umzusetzenden Sicherheitsmaßnahmen basieren auf dieser Klassifikation.

Vertraglich festgelegte Sicherheitsanforderungen (siehe OPS.3.1.M2 Vertragsgestaltung mit dem Outsourcing-Kunden) sind zu erfüllen und dem Outsourcing-Kunden auf dessen Anfrage auch adäquat nachzuweisen. Des Weiteren ist zu beachten, dass während der Migrationsphase Änderungsbedarf entstehen kann. Um darauf zu reagieren, müssen die Vertragsparteien sich zu konkreten Sicherheitsmaßnahmen abstimmen. Hierfür sollten vom Outsourcing-Dienstleister Ressourcen in der Planung berücksichtigt werden.

Die Umsetzung des Sicherheitskonzepts sollte regelmäßig überprüft werden.

OPS.3.1.M4 Festlegung der möglichen Kommunikationspartner

Zwischen Outsourcing-Dienstleister und Outsourcing-Kunden sollte im Vorfeld abgestimmt, dokumentiert und vertraglich vereinbart werden, welche internen und externen Kommunikationsteilnehmer welche Informationen über das jeweilige Outsourcing-Projekt erhalten dürfen. Während des Outsourcing-Projektes ist diese Dokumentation regelmäßig und anlassbezogen auf ihre Aktualität hin zu prüfen. So sollte stets sichergestellt sein, dass die angegebenen Ansprechpartner die ihnen ursprünglich zugeordnete Funktion noch wahrnehmen.

Sollen Informationen an einen Kommunikationspartner außerhalb der Institution des Outsourcing-Dienstleisters übertragen werden, so muss sichergestellt werden, dass der Empfänger die notwendigen Berechtigungen zum Weiterverarbeiten dieser Informationen besitzt. Diesbezüglich müssen Möglichkeiten und Rahmenbedingungen im Vorfeld mit dem Kunden abgestimmt und vertraglich festgelegt werden.

Werden Informationen zwischen mehreren kommunizierenden Stellen ausgetauscht, so sollte für alle Beteiligten ersichtlich sein, wer diese Informationen ebenfalls erhalten hat bzw. erhalten wird.

Um die oben genannten Kriterien zu erfüllen, muss festgelegt werden, welche Kommunikationspartner welche Informationen erhalten dürfen. Hierfür ist es erforderlich, dass alle schutzbedürftigen Informationen entsprechend ihrer strategischen Bedeutung für die Institution klassifiziert sind.

Mittels einer Kommunikationsmatrix können alle Kommunikationspartner entweder den Klassifizierungen oder den Informationen selbst zugeordnet werden. Das ermöglicht eine übersichtliche Darstellung der Informationsverteilung.

Des Weiteren sollten auch die zu nutzenden Kommunikationswege hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit geprüft und überwacht werden, da auch auf diesem Wege Informationen an unberechtigte Empfänger gelangen können.

Die Empfänger sind darauf hinzuweisen, dass die übermittelten Daten nur zu dem Zweck benutzt werden dürfen, zu dem sie weitergegeben wurden. Auch aus Datenschutzgründen (siehe zum Beispiel BDSG, Weitergabekontrolle) sollte eine Übersicht erstellt werden, welche Empfänger berechtigt sind, Informationen – insbesondere personenbezogene Daten – per Datenübertragung oder Datenträgeraustausch zu erhalten.

OPS.3.1.M5 Regelungen für den Einsatz des Personals des Outsourcing-Dienstleisters

Im Zuge einer Outsourcing-Dienstleistung ist es gegebenenfalls erforderlich, dass sich Mitarbeiter des Outsourcing-Dienstleister im Rahmen ihrer Aufgabenerfüllung über einen längeren Zeitraum in den Räumlichkeiten des Outsourcing-Kunden aufhalten müssen.

Jene Mitarbeiter sollten ausreichend eingewiesen und über hausinterne Regelungen und Vorschriften des Outsourcing-Kunden zur Informationssicherheit sowie die organisationsweite Informationssicherheitspolitik unterrichtet werden. Geschieht dies nicht von Seiten des Outsourcing-Kunden aus, sollte der Outsourcing-Dienstleister darauf hinwirken. Es ist von beiderseitigem Interesse, dass allen Beteiligten entsprechende Regelungen und Vorschriften bekannt sind und angewendet werden.

Vor dem Einsatz der Mitarbeiter des Outsourcing-Dienstleisters sollten eventuelle – von Seiten des Outsourcing-Kunden gestellte – Anforderungen (Führungszeugnis, Qualifikationen etc.) an das einzusetzende Personal identifiziert und deren Erfüllung sichergestellt werden.

Zudem sollte der Outsourcing-Dienstleister mit Blick auf alle Mitarbeiter, welche im Rahmen ihrer Aufgabenerfüllung Zugang zu vertraulichen Unterlagen und Daten des Outsourcing-Kunden erhalten, sicherstellen, dass diese sich schriftlich zur Einhaltung der geltenden einschlägigen Gesetze, Vorschriften und Regelungen des Outsourcing-Kunden verpflichten, z. B. über eine Verschwiegenheitserklärung (siehe unter anderem Baustein ORP.5 Anforderungsmanagement).

Es muss Vertretungsregelungen in allen Bereichen geben. Um eine kontinuierliche Verfügbarkeit wichtiger Prozesse zu erreichen, muss insbesondere dafür gesorgt werden, dass Schlüsselpositionen immer besetzt sind, sobald dies von den Abläufen her gefordert wird.

Bei Mitarbeitern, die die Institution verlassen oder andere Funktionen übernehmen, müssen bestehende Regelungen mit erhöhter Sorgfalt überprüft werden. Nachfolger müssen eingearbeitet werden, Unterlagen sind zurückzugeben und erteilte Berechtigungen sind wieder zu entziehen. Vor der Verabschiedung sollte noch einmal explizit auf Verschwiegenheitsverpflichtungen hingewiesen werden.

OPS.3.1.M6 Regelungen für den Einsatz von Fremdpersonal

Auch Outsourcing-Dienstleister greifen ihrerseits häufig auf Dienstleister zurück, um bestimmte Teilaufgaben erledigen zu lassen. Wenn externe Mitarbeiter Zugang zu vertraulichen Unterlagen und Daten des Outsourcing-Kunden bekommen könnten, ist dies dem Outsourcing-Kunden mitzuteilen. Der ISB des Outsourcing-Kunden sollte dann prüfen, ob damit die gestellten Sicherheitsanforderungen weiterhin erfüllbar sind und ob sich dadurch weitere Sicherheitsanforderungen ergeben.

Externe Mitarbeiter, die über einen längeren Zeitraum für den Outsourcing-Dienstleister tätig sind, sind schriftlich auf die Einhaltung der geltenden einschlägigen Gesetze, Vorschriften und internen Regelungen zu verpflichten. Beim Einsatz von externen Mitarbeitern muss außerdem auf jeden Fall sichergestellt sein, dass sie bei Beginn ihrer Tätigkeit in ihre Aufgaben eingewiesen werden. Sie sind – so weit es zur Erfüllung ihrer Aufgaben und Verpflichtungen erforderlich ist – über hausinterne Regelungen und Vorschriften zur Informationssicherheit zu unterrichten.

Daneben sollte sichergestellt sein, dass auch für externe Mitarbeiter Vertretungsregelungen existieren. Ebenso sollte gewährleistet sein, dass sich diese mit den von ihnen eingesetzten IT-Anwendungen auskennen und auch die erforderlichen Sicherheitsmaßnahmen beherrschen.

Wenn im Rahmen der auszuführenden Aufgaben einmalig zum Einsatz kommendes Fremdpersonal (z. B. Wartungstechniker) hinzugezogen werden soll, so sollte dieses Fremdpersonal wie Besucher behandelt werden. Dazu sollten die gängigen Regelungen zum Besuchermanagement eingehalten werden. Es muss nachvollziehbar sein, welche Befugnisse das Fremdpersonal hat und der Einsatz sollte entsprechend dem Schutzbedarf angemessen eingewiesen und begleitet werden.

Bei Beendigung des Auftragsverhältnisses muss eine geregelte Übergabe der Arbeitsergebnisse, erhaltenen Unterlagen und Betriebsmittel erfolgen. Zudem sind dem Outsourcing-Kunden physische Zutrittsmittel zu übergeben (z. B. Schlüssel, Zugangskarten). Eventuell bestehende Verschwiegenheitsverpflichtungen bleiben auch nach der Zusammenarbeit mit dem Outsourcing-Kunden gültig und müssen demnach weiterhin eingehalten werden (siehe auch ORP.2 Personal).

OPS.3.1.M7 Erstellung eines Mandantenkonzeptes durch den Outsourcing-Dienstleister

Häufig werden von mehreren Institutionen zentrale IT-Infrastrukturen oder Dienste eines Outsourcing-Dienstleisters gemeinsam genutzt. Hierbei können auch Anwendungen gemeinsam betrieben und genutzt werden, wobei Datenhaltung und Datenverarbeitung z. B. infolge rechtlicher Anforderungen oder aufgrund von Betriebs- und Geschäftsgeheimnissen getrennt erfolgen müssen. In diesen Fällen wird häufig von mandantenfähigen Anwendungen gesprochen, wobei jeder nutzenden Institution ein Mandantenbereich, kurz Mandant, zugeordnet wird.

In jedem dieser Fälle ist durch ein geeignetes Mandantenkonzept sicherzustellen, dass die Anwendungen mandantenfähig betrieben werden. Dazu gehört, dass jeder Outsourcing-Kunde innerhalb seines Bereichs, also seines Mandantensystems, die fachlichen Vorgaben (z. B. bezogen auf Protokollierungsumfang und Speicherfristen) umsetzen sowie seinen Kontrollpflichten nachkommen kann. Das Mandantenkonzept ist durch den Outsourcing-Dienstleister zu erstellen und dem Outsourcing-Kunden zur Verfügung zu stellen. Dieser muss sich überzeugen, dass das Mandantenkonzept für seinen Schutzbedarf eine angemessene Sicherheit bietet, bevor solche Systeme oder Dienste gemeinsam mit weiteren Kunden genutzt werden. Das Mandantenkonzept ist somit Bestandteil des Sicherheitskonzeptes, das für ein Outsourcingvorhaben zu stellen ist.

Auch unter datenschutzrechtlichen Gesichtspunkten sind Anforderungen an die Trennung von Mandanten zu beachten. Hinweise dazu gibt die "Orientierungshilfe Mandantenfähigkeit" des Arbeitskreises Technik der Datenschutzbeauftragten des Bundes und der Länder.

Wenn eine Anwendung neu beschafft, erstellt oder wesentlich geändert wird, muss außerdem zunächst grundsätzlich sichergestellt sein, dass diese Anwendung Mandanten sauber trennen kann (siehe M 2.552 Erstellung eines Pflichtenheftes).

Ein Mandantenkonzept sollte mindestens folgende Punkte berücksichtigen:

- Geeignete Rechtsgrundlagen: Rechtliche Vorgaben dürfen einem gemeinsamen, mandantenfähigen Verfahrensbetrieb nicht entgegenstehen. Ferner muss sichergestellt werden, dass die technische Ausgestaltung der Mandantentrennung dem Schutzbedarf der Daten in den jeweiligen Mandanten entspricht.
- Abgeschlossenheit von Transaktionen: Datenverarbeitungsschritte, die in einem Mandanten durchgeführt werden, dürfen nicht dazu führen, dass die Daten in anderen Mandanten verändert werden oder lesend auf sie zugegriffen werden kann.
- Konfigurative Unabhängigkeit der Mandanten untereinander: Es sollten mindestens zwei administrative Ebenen vorhanden sein. Die erste Ebene dient der Mandantenadministration: Hier werden Mandantensysteme eingerichtet und gelöscht, mandantenübergreifende konfigurative Einstellungen durchgeführt, die Rollen der Mandantenadministratoren zugewiesen, die mandantenübergreifende Protokollierung angestoßen und deren Revision durchgeführt. Die zweite Ebene dient der Administration eines Mandantensystems: Hier werden die Berechtigungen im Mandantensystem vergeben, mandanteninterne Konfigurationen durchgeführt, die mandanteninterne Protokollierung konfiguriert und die Protokollrevision durchgeführt.
- Trennung von Berechtigungskontexten: Jeder Mandant hat seinen eigenen, abgeschlossenen Berechtigungskontext. Die Vergabe oder Veränderung von Berechtigungen durch die Administratoren der jeweiligen Mandanten darf sich nicht auf Berechtigungen in anderen Mandanten auswirken.
- Es muss eine administrative Ebene zur Mandantenadministration seitens des Betreibers geben, die aber keine Berechtigung zur Verarbeitung von Daten innerhalb eines Mandanten besitzen sollte.
- Trennung von Protokollierungskontexten: Protokollrevisoren eines Mandatensystems dürfen keinen Zugriff auf Protokolldaten anderer Mandantensysteme haben. Beispielsweise können Mandanten eigene Log-Dateien haben. Eine andere Lösung könnte sein, dass eine Institution über vom Dienstleister entsprechend eingerichtete Filter oder Report-Generatoren auf die Protokolldaten ihres Mandanten zugreifen kann.
- Beschränkung der mandantenübergreifenden Datenverarbeitung: Die Ebene der Mandantenadministration sollte grundsätzlich keine Verarbeitung von Daten innerhalb eines Mandanten außerhalb der Mandantenadministration zulassen. Der Datenaustausch zwischen Mandanten sollte über definierte und geeignet abgesicherte Schnittstellen erfolgen.

Die Umsetzung dieser Anforderungen kann auf vielfältige Weise erfolgen. Eine herausragende Rolle spielt dabei ein geeignetes Rollen- und Berechtigungskonzept innerhalb von Anwendungen. Darüber hinaus können auf der Infrastruktur- und Diensteebene hierzu verschiedene Methoden wie z. B. Virtualisierungstechniken eingesetzt werden:

- Einsatz verschiedener Datenbanken (auch Instanzen genannt) in einem gemeinsamen Datenbankmanagementsystem (DBMS)
- VPD (Virtual Private Database) auf der Diensteebene bei Datenbanken
- Speicherung von mit einem Mandantenattribut versehenen Datensätzen in einer gemeinsamen Datenbank und gemeinsamen Tabellen, sodass die Mandantentrennung durch die Anwendung erfolgt.
- Virtuelle Maschinen auf der Systemebene
- VLAN (Virtual LAN), VRF (Virtual Routing and Forwarding), VPN (Virtual Private Network) in der Netzinfrastruktur

Der Outsourcing-Kunde sollte prüfen, ob die vom Outsourcing-Dienstleister gewählte Lösung zur Mandantentrennung effektiv ist.

OPS.3.1.M8 Vereinbarung über die Anbindung an Netze der Outsourcing-Partner

Immer mehr Unternehmen und Behörden schließen ihre bisher nach außen abgeschotteten Netze zu Netzverbünden zusammen, sogenannten Extranets. Bei der Anbindung des Netzes des Outsourcing-Dienstleister an das Netz des Outsourcing-Kunden ist es erforderlich, dass eine detaillierte Vereinbarung (Data Connection Agreement, DCA) geschlossen wird, bevor eine Netzanbindung erfolgt.

Hierdurch müssen die jeweiligen Zugriffsrechte des Outsourcing-Dienstleisters und des Outsourcing-Kunden genau definiert werden. Ebenso wichtig ist dabei die Frage, welcher Anwenderkreis mit welchen Zugriffsrechten und zu welchen Bedingungen Zugriff auf das Netz des Dienstleisters und umgekehrt erhalten soll.

Die Vereinbarung sollte folgende Bestandteile umfassen:

- Eine Beschreibung dessen, was die Vereinbarung insgesamt umfasst, inklusive einer Beschreibung der betroffenen Informationsverbünde
- Eine Abstimmung über den jeweiligen Schutzbedarf und die Klassifikation von Daten (es muss ein gemeinsames Verständnis erzielt werden)
- Eine Festlegung der Verantwortlichen (Wer trägt die Verantwortung für die Einhaltung der Vertragsbedingungen?)
- Die Benennung von Ansprechpartnern sowohl für organisatorische als auch technische Probleme und insbesondere für sicherheitsrelevante Ereignisse
- Die erforderlichen Informationen zur Klassifizierung organisatorischer und technischer Probleme als solche sowie sicherheitsrelevanter Ereignisse
- Informationen und Festlegungen zur netzinternen Verschlüsselung
- Welche Dienste (z. B. SSH, HTTPS) zur Verfügung gestellt werden und welche nicht
- Welche IT-Plattformen, Anwendungen und Datenformate eingesetzt werden
- Ob sich aus der Netzanbindung Anforderungen an die Verfügbarkeit von Netz- oder IT-Komponenten beim jeweiligen Partner ergeben (Performance, maximale Ausfallrate)
- Wer was protokollieren darf bzw. muss, wo die Protokolldaten abgelegt werden und wer auf die Protokolldaten zugreifen darf (dies kann insbesondere in Notsituationen wichtig sein)
- Inwieweit ein regelmäßiger Austausch von Protokolldaten erfolgen soll
- Welche Sicherheitsmaßnahmen gewährleistet werden müssen und wie deren Einhaltung überprüft wird
- Eine Vertraulichkeitsvereinbarung (Non-Disclosure Agreement), d. h. eine Vereinbarung darüber, dass Informationen, die einer der Beteiligten im Rahmen der Zusammenarbeit erhalten hat, nicht an Außenstehende weitergegeben werden
- Eine Haftungs- bzw. Schadensersatzregelung (hierin sollten unter anderem die Bedingungen für die Trennung der Netzanbindung, Haftung bei Schadprogrammen oder Hackerangriffen, Vertragsstrafen bei nicht erfüllter Leistung bzw. Haftungsübernahme bei Inanspruchnahme für fremde Inhalte geklärt sein)
- Eine Regelung über Auskunftspflichten bei aufgetretenen Sicherheitslücken
- Eine Festlegung, welche Daten zu welchen Zwecken genutzt werden dürfen (z. B. bei der Weiterverwendung von Arbeitsergebnissen)
- Eine Beschreibung, inwieweit weitere Vertragspartner in die Vereinbarung eingebunden werden, z. B. durch gemeinsame Nutzung von Applikationen oder als Dienstleister für einen der Vertragspartner
- Die Laufzeit sowie Anpassungsmöglichkeiten der Vereinbarung (Technik entwickelt sich schnell weiter, d. h. auch die Vereinbarungen über deren Nutzung müssen ständig angepasst werden)

Verantwortlich für die Erstellung der Vereinbarung sollten die Personen sein, die auch für die Einhaltung der getroffenen Regelungen verantwortlich sind. Muss aufgrund von Problemen die Verbindung der Netze zeitweise getrennt werden, sollten jedoch alle betroffenen Personen miteinbezogen werden, da sich deren Anforderungen stark unterscheiden können, jedoch berücksichtigt werden sollten.

Eine Netzanbindung an Netze Dritter sollte nur aktiviert werden, wenn bei beiden Partnern alle für den vereinbarten Schutzbedarf angemessenen Sicherheitsmaßnahmen umgesetzt wurden und keine erkennbaren Sicherheitsmängel mehr vorliegen. Outsourcing-Dienstleister sollten sich auch von dem Sicherheitsniveau der Outsourcing-Kunden überzeugen, beispielsweise durch einen IT-Grundschutz-Check oder Stichproben vor Ort. Wird die gemeinsame IT-Infrastruktur durch eine Sicherheitslücke des Outsourcing-Kunden kompromittiert, wird sich im Nachhinein der Outsourcing-Dienstleister ebenfalls mit dem Vorwurf der Nachlässigkeit konfrontiert sehen. Zudem sollte eine sofortige Beseitigung aller identifizierten Sicherheitsmängel angestrebt werden. Im Echtbetrieb ist die Verfügbarkeit eines lauffähigen Produktes meist deutlich höher priorisiert, als die Behebung etwaiger Sicherheitsmängel, die dann zu dauerhaften Schwachstellen werden können.

Dem Outsourcing-Kunden und möglichen Dritten sollten nur die Dienste zur Verfügung gestellt werden, die zum einen vertraglich vereinbart worden sind und zum anderen unbedingt erforderlich sind. Auf welche Bereiche des eigenen Netzes Dritten Zugriff gewährt wird, muss abhängig gemacht werden von der Art der bestehenden Beziehungen zwischen den Vertragspartnern und vom gegenseitigen Vertrauen zwischen diesen. Bei ausländischen Partnern müssen unbedingt deren nationale Gesetze berücksichtigt werden, z. B. in den Bereichen Kryptographie, Datenschutz und Urheberrecht.

Sollte es zu Sicherheitsvorfällen kommen, bei deren Behebung die Verbindung getrennt werden muss, muss klar definiert sein, wer dies wann tun darf. Es ist ebenfalls zu klären, welche Personen über diesen Vorgang zu informieren sind und welche Eskalationsschritte vorgesehen sind.

OPS.3.1.M9 Vereinbarung über Datenaustausch zwischen den Outsourcing-Partnern

Für den regelmäßigen Datenaustausch zwischen dem Outsourcing-Dienstleister und dem Outsourcing-Kunden sollten Vereinbarungen getroffen werden, die dessen reibungslosen und sicheren Ablauf sicherstellen.

Solche Vereinbarungen sollten insbesondere die folgenden Bestandteile umfassen:

- Benennung von Ansprechpartnern sowohl für organisatorische als auch technische Herausforderungen und insbesondere für sicherheitsrelevante Ereignisse
- Festlegung der erforderlichen technischen und organisatorischen Rahmenbedingungen, also beispielsweise darüber,
  - welche Anwendungen und Datenformate unterstützt werden und
  - welche Verfügbarkeit und welche Reaktionsgeschwindigkeit bei den Partnern zu gewährleisten ist (wie häufig sind Nachrichten zu lesen und wie schnell sind sie zu beantworten)
- Festlegung der Sicherheitsmaßnahmen, welche beim Datenaustausch gewährleistet werden müssen, z. B.
  - Überprüfung der Daten auf Schadsoftware vor und nach dem Austausch,
  - Schutz der Daten vor Transportschäden und unbefugtem Zugriff bei der Übermittlung (verschlossene Behältnisse, Checksummen, Verschlüsselung, Signaturen),
  - Regelung des Schlüsselmanagements,
  - Löschung der Daten auf der Senderseite frühestens nach der Bestätigung des korrekten Empfangs (falls die Löschung erforderlich ist)
- Eine Vertraulichkeitsvereinbarung (Non-Disclosure Agreement), d. h. eine Vereinbarung darüber, dass Informationen, die einer der Beteiligten im Rahmen der Zusammenarbeit erhalten hat, nicht an Außenstehende weitergegeben werden
- Festlegung, welche Daten zu welchen Zwecken genutzt werden dürfen (z. B. bei der Weiterverwendung von Arbeitsergebnissen)
- Verpflichtung auf die Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen, also z B. Datenschutz- und Urheberrechtsgesetze bzw. Lizenzregelungen

Weitere Punkte, die in eine solche Vereinbarung aufgenommen werden sollten, finden sich in Baustein OPS.1.2.3 Datenträgertausch und Baustein APP.1 E-Mail/Groupware/Kommunikation.

OPS.3.1.M10 Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb

Nachdem ein Outsourcing-Vorhaben umgesetzt wurde, muss die Informationssicherheit auch im laufenden Betrieb gewährleistet werden. Um dies sicherzustellen müssen Outsourcing-Kunden und Outsourcing-Dienstleister angemessen kooperieren. So hat der Outsourcing-Kunde ein Betriebskonzept zu erstellen, in dem alle relevanten Sicherheitsaspekte berücksichtigt werden. Outsourcing-Dienstleister sollten Outsourcing-Kunden insbesondere hinsichtlich der folgenden Aspekte unterstützen:

- Regelmäßige Aktualisierung der Dokumentationen und Richtlinien.
- Prüfung der geltenden Sicherheitskonzepte (sind diese noch aufeinander abgestimmt und ist das gewünschte Sicherheitsniveau noch gewährleistet?). Insbesondere sollte der Outsourcing-Dienstleister den Outsourcing-Kunden über wichtige Änderungen in seinem Einflussbereich informieren.
- Erstellung eines Mandantenkonzeptes durch den Outsourcing-Dienstleister, in dem beschrieben ist, auf welche Weise die Mandantentrennung im Rahmen des Betriebs von IT-Systemen und Anwendungen sichergestellt wird. Der Outsourcing-Dienstleister hat dabei sicherzustellen, dass Störungen bei anderen Kunden nicht die Abläufe und Systeme des Outsourcing-Kunden beeinträchtigen. Zudem ist sicherzustellen, dass Daten des Outsourcing-Kunden unter keinen Umständen anderen Kunden des Outsourcing-Dienstleisters zugänglich werden.
- Durchführung der vereinbarten Audits zum Umsetzungsstand der vereinbarten Sicherheitsmaßnahmen.
- Bereitstellung von notwendigen Informationen und/oder Kontaktmöglichkeiten zu Subunternehmen des Outsourcing-Dienstleisters, um auch hier Auditierungen zu ermöglichen.
- Dokumentation des (Wartungs-)Zustands von Systemen und Anwendungen (Performance, Verfügbarkeit, Qualitätsniveau, Kapazität).
- Zusammenarbeit bezüglich der Datensicherung (siehe OPS.1.1.5 Datensicherung).
- Des Weiteren sollte der Outsourcing-Dienstleister an regelmäßigen Abstimmungsrunden zu folgenden Punkten teilnehmen:
    - Informationsaustausch (z. B. Personalnachrichten, organisatorische Regelungen, Gesetzesänderungen, geplante Projekte, vorgesehene Tests und Systemänderungen, die zu Beeinträchtigungen der Dienstleistungsqualität führen können)
    - Informationen über Sicherheitsrisiken und den Umgang damit
    - Problemidentifikation und -analyse
    - Gegenseitiges Feedback und das Aufspüren von Verbesserungspotenzialen (zur Motivation der Mitarbeiter können besonders positive Beispiele einer gelungenen Kooperation dargestellt werden)
    - Änderungsmanagement: Änderungswünsche (Hardware, Software, Ausweitung des Dienstleistungsportfolios, gestiegener Ressourcenbedarf etc.) des Outsourcing-Kunden sollten frühzeitig besprochen werden, um deren rechtzeitige Umsetzung zu gewährleisten.
- Planung, Durchführung und Auswertung von Übungen und Tests zu folgenden Themen:
    - Reaktion auf Systemausfälle (Teilausfall, Totalausfall)
    - Wiedereinspielen von Datensicherungen
    - Beherrschung von Sicherheitsvorfällen

OPS.3.1.M11 Zutritts-, Zugangs- und Zugriffskontrolle

Bei einem Outsourcing-Dienstleister werden typischerweise mehrere Outsourcing-Kunden gleichzeitig betreut, die eigenes Personal, aber auch Auditoren und andere Prüfer vorbeischicken. Dabei muss sichergestellt sein, dass Kunden nicht auf IT-Systeme, Netze oder Daten anderer Kunden Zugriff erhalten.

Um die Geschäftsprozesse, Informationen und IT-Systeme des Outsourcing-Dienstleisters ebenso wie die verschiedenen Outsourcing-Kunden angemessen zu schützen, sind Zutritts-, Zugangs- und Zugriffsberechtigungen zu regeln und ein geeigneter organisatorischer Rahmen zu schaffen (siehe auch ORP.4 Identitäts- und Berechtigungsmanagement).

Auf den verschiedenen Ebenen müssen angemessene und praktikable Berechtigungen vergeben werden (z. B. für den Zutritt zu Räumen, Zugang zu IT-Systemen, Zugriff auf Anwendungen). Es sollten immer nur so viele Rechte vergeben werden, wie es für die Aufgabenwahrnehmung notwendig ist. Es muss ein geregeltes Verfahren für die Vergabe, die Verwaltung und den Entzug von Berechtigungen geben.

Wenn Personen Aufgaben neu übernehmen oder abgeben, müssen Berechtigungen zeitnah angelegt, geändert oder gelöscht sowie ihre Benutzerkennungen aktiviert bzw. deaktiviert werden. Der Zutritt zu Räumen, der Zugriff auf Informationen und der Zugang zu IT-Systemen sollte so abgesichert sein, dass Personen nur auf die Informationen zugreifen können, die sie benötigen. Grundsätzlich sollte der Zugriff auf alle IT-Systeme und Dienste durch Identifikation und Authentisierung der zugreifenden Benutzer oder IT-Systeme abgesichert sein.

Es sollte Vorgaben an Art und Ausgestaltung der jeweiligen Authentisierung geben, z. B. zur Art der Authentisierung über Besitz, Wissen oder biometrische Eigenschaften sowie Mindestanforderungen an Passwörter. Voreingestellte Standardpasswörter müssen direkt nach der Installation, spätestens bei erstmaliger Inbetriebnahme von Hard- oder Software geändert werden. Die Mitarbeiter müssen für die korrekte Nutzung von Authentisierungsmechanismen geschult werden.

Die Vergabe von Berechtigungen sollte sich an den Funktionen der Berechtigten orientieren. Rollen und somit auch Berechtigungen sollten geeignet getrennt werden. Vergabe, Änderung sowie Entzug von Berechtigungen und Authentisierungsmitteln müssen dokumentiert werden.

OPS.3.1.M12 Änderungsmanagement [IT-Betrieb, Änderungsmanager]

Bei der Komplexität heutiger IT-Systeme können bereits kleine Änderungen an laufenden Systemen zu Sicherheitsproblemen führen, z. B. durch unerwartetes Systemverhalten oder Systemausfälle. In Bezug auf Informationssicherheit ist es Aufgabe des Änderungsmanagements, neue Sicherheitsanforderungen zu erkennen, die sich aus Änderungen an IT-Systemen ergeben. Bei Ausfällen oder Minderleistungen durch den Outsourcing-Dienstleister können empfindliche Vertragsstrafen fällig werden. Zudem leidet der Wertschöpfungsprozess des Outsourcing-Kunden und somit auch die Beziehung zwischen den Outsourcing-Partnern, was einen nachhaltigen Reputationsverlust für den Outsourcing-Dienstleister bedeuten könnte.

Sind signifikante Hardware- oder Software-Änderungen an einem IT-System geplant, so sind die Auswirkungen auf die Sicherheit des Gesamtsystems zu untersuchen. Änderungen an einem IT-System dürfen nicht zu einer Verringerung der Effizienz von einzelnen Sicherheitsmaßnahmen führen.

Daher sollten Richtlinien für die Durchführung von Änderungen an IT-Komponenten, Software oder Konfigurationsdaten vorhanden sein (siehe Baustein OPS.1.2.1 Änderungsmanagement). Alle Änderungen an IT-Komponenten, Software oder Konfigurationsdaten sollten nach einem standardisierten Prozess ablaufen. Dieser Prozess muss sicherstellen, dass Änderungen

- geplant,
- priorisiert,
- bewertet,
- implementiert,
- geprüft/getestet,
- freigegeben,
- dokumentiert,

und nach ihrer Umsetzung einem Review unterzogen werden. Es ist dafür Sorge zu tragen, dass auf alle sicherheitsrelevanten Änderungen angemessen reagiert wird. Dazu gehören zum Beispiel:

- Änderungen an IT-Systemen (neue Hardware, Erweiterung oder Modifikation des Netzes, neue Applikationen und Modifikationen an der eingesetzten Software, Einspielen von Sicherheitspatches, usw.),
- Räumliche Änderungen, z. B. nach einem Umzug,
- Änderungen in der Aufgabenstellung oder in der Wichtigkeit der Aufgabe für die Institution,
- Änderungen in der Benutzerstruktur (neue, etwa externe oder anonyme, Benutzergruppen),
- Änderung des Benutzerverhaltens (Nachfrage zu bestimmten Zeiten oder Terminen, nachgefragte Mengen oder Kapazitäten, usw.)

Bevor Änderungen genehmigt und durchgeführt werden, muss durch Prüfungen und Tests der geplanten Aktionen sichergestellt werden, dass das Sicherheitsniveau während und nach der Änderung erhalten bleibt. Wenn Risiken, insbesondere für die Verfügbarkeit, nicht ausgeschlossen werden können, muss die Planung auch eine Rückfalllösung vorsehen und Kriterien vorgeben, wann diese zum Tragen kommen soll. Alle Änderungen und die dazugehörigen Entscheidungsgrundlagen sind zu dokumentieren. Dies gilt sowohl in der Betriebs- als auch in einer Testumgebung. Beim Änderungsmanagement ist das Berechtigungskonzept zur Durchführung von Änderungen ein wichtiger Punkt:

- Nur diejenigen, die Änderungen durchführen dürfen, sollten Zugriffsberechtigungen auf die dafür relevanten Systembereiche haben.
- Es sollte Mechanismen geben, die sicherstellen, dass alle wesentlichen Änderungen vorher abgestimmt wurden.

Hinweis: Bei der Durchführung von Änderungen sollte immer beachtet werden, dass Änderungen eines IT-Systems oder seiner Einsatzbedingungen Änderungen in der Umsetzung einzelner Sicherheitsmaßnahmen, die Erstellung eines neuen Sicherheitskonzepts oder sogar die Überarbeitung der organisationsweiten Leitlinie zur Informationssicherheit erforderlich machen können. Bei größeren Änderungen sollte daher das Informationssicherheitsmanagement des Outsourcing-Dienstleisters und des Outsourcing-Kunden involviert werden.

OPS.3.1.M13 Sichere Migration bei Outsourcing-Vorhaben

Die Migrationsphase beginnt nach dem Vertragsabschluss. Im Zuge der Migration werden folgende vertragliche Regelungen umgesetzt:

- Vereinbarungen hinsichtlich Services und Lösungen gemäß der vertraglichen Regelungen und den allgemeinen Geschäftsbedingungen,
- Service-Vereinbarungen, Anforderungsspezifikationen, Servicekatalog und Beschreibungen, Service-Level,
- detailliertes Outsourcing-Modell und aktualisierter Business Case,
- Migrationsplan.

Nach Beauftragung durch den Outsourcing-Kunden sollte ein Sicherheitsmanagement-Team speziell für die Migrationsphase von Seiten des Outsourcing-Kunden eingerichtet werden. Dieses sollte durch qualifizierte Mitarbeiter des Outsourcing-Dienstleisters ergänzt werden. Die Größe des (gemeinsamen) Sicherheitsmanagement-Teams sollte von Art und Größe des Outsourcing-Vorhabens abhängig gemacht werden, als Minimum kann es aus je einem Sicherheitsexperten des Kunden und des Dienstleisters bestehen. Als Hauptansprechpartner für die Informationssicherheit muss seitens des Kunden und und des Dienstleisters der Informationssicherheitsbeauftragte benannt werden.

Um den Erfolg der Migrationsphase zu fördern, sollte der Outsourcing-Kunde – insbesondere dessen Sicherheitsmanagement-Team – während der gesamten Migrationsphase durch den Outsourcing-Dienstleister aktiv in das Projektgeschehen mit einbezogen werden. Demnach sollte insbesondere sichergestellt werden, dass dieser rechtzeitig über aktuelle Fortschritte, Entwicklungen und eventuelle Komplikationen informiert wird.

Hierzu sollte ein Komitee mit fachlich qualifizierten Ansprechpartnern beider Seiten für das Migrationsmanagement etabliert sowie die Häufigkeit von Arbeitstreffen festgelegt werden. Die jeweiligen Verantwortlichkeiten sind im Vorfeld zu definieren und schriftlich zu fixieren, sowie mögliche Stellen, die das Komitee unterstützen.

Unter "fachlich qualifizierten Ansprechpartnern" werden in diesem Kontext jene Personen verstanden, die über das erforderliche Fachwissen und die benötigten Kompetenzen für die Outsourcing-Dienstleistung verfügen und für die speziellen Aufgaben und Herausforderungen im Rahmen eines Projekts zum Outsourcing geschult sind (Organisation, Kommunikation, Konfliktmanagement).

Alle Mitglieder des Komitees sollten im kommunikativen Umgang mit Mitarbeitern und weiteren Outsourcing-Partnern erfahren sein. Die zum Teil beträchtlichen organisationsinternen Änderungen, an die sich alle beteiligten Mitarbeiter des Outsourcing-Kunden gewöhnen müssen, können zu Widerständen führen, die sich nicht nur nachteilig auf die unmittelbare Zusammenarbeit auswirken, sondern auch den Erfolg des Outsourcing-Vorhabens beeinflussen. Um das Outsourcing-Vorhaben nicht zu gefährden und Widerständen vorzubeugen und/oder sie abzubauen, ist eine sensible Kommunikation aller Maßnahmen notwendig.

Der Outsourcing-Kunde hat das berechtigte Interesse, während der Migrationsphase deren Durchführung zu überwachen. Hierzu sollten die notwendigen Strukturen und Ressourcen geschaffen und bereitgestellt werden, wie z. B. definierte Kommunikationskanäle und –Verfahren sowie Eskalationsvorlagen und eine regelmäßige Berichterstattung. So kann die Migration transparent durchgeführt werden, was die Erreichung von Zielen durch beide Seiten messbar macht und zu einer nachhaltigen vertrauensvollen Outsourcing-Beziehung führt.

Außerdem sollte in dieser Phase gegebenenfalls eine Schulung der Mitarbeiter des Outsourcing-Kunden geplant werden. Diese arbeiten künftig an neu entstandenen Schnittstellen. Der Outsourcing-Dienstleister sollte hierbei unterstützen. Die Durchführung von Schulungen und deren Nachhaltigkeit liegen im Interesse des Outsourcing-Dienstleisters, da dieser aufgrund ungenügender Zuarbeit seinen Service nicht in dem vereinbarten Umfang bzw. mit dem geforderten Qualitätsniveau erbringen kann. Dies wiederum kann sich negativ auf die Outsourcing-Beziehung und somit auf die Reputation des Outsourcing-Dienstleisters auswirken.

Im Zuge der Migration kommt dem Testbetrieb eine hohe Bedeutung zu. Besonders zu Testzwecken und in Phasen großer Arbeitsbelastung werden gerne "flexible" und "unkomplizierte" Lösungen gewählt, die oftmals unsicher sind. Dies gilt es zu vermeiden. So ist beispielsweise sicherzustellen, dass Produktivdaten nicht ohne besonderen Schutz als Testdaten verwendet werden. Dies muss durch das Sicherheitskonzept entsprechend ausgeschlossen werden.

Folgende Aspekte sollten von Seiten des Outsourcing-Dienstleisters im Zuge der Migrationsphase berücksichtigt werden:

- Für die Migrationsphase muss eine Sicherheitskonzeption erstellt werden.
- Der Outsourcing-Dienstleister hat klare Verantwortlichkeiten und Hierarchien für die Migrationsphase festzulegen. Klare Führungsstrukturen sind eine Voraussetzung. Zudem sollten Ansprechpartner und Verantwortlichkeiten auch auf hohen Ebenen definiert werden. Nur so kann sichergestellt werden, dass im Zweifelsfall mit entsprechendem Nachdruck gehandelt werden kann.
- Die erforderlichen Tests müssen geplant und durchgeführt, Abnahmeprozeduren erarbeitet und die Produktionseinführung geplant werden.
- Der Outsourcing-Dienstleister muss geeignete interne Mitarbeiter für die Test-, Einführungsphase und den späteren Betrieb auszuwählen. Es ist zu prüfen, inwieweit dem Outsourcing-Kunden vertraglich ein Mitspracherecht bei der Personalauswahl eingeräumt werden sollte.
- Der Outsourcing-Dienstleister muss die relevanten Abläufe, Applikationen und IT-Systeme des Outsourcing-Kunden genau kennenlernen und gegebenenfalls aktiv eine Einweisung fordern.
- Der störungsfreie Betrieb ist durch eine genaue Ressourcenplanung und Tests im Vorfeld sicherzustellen. Die produktiven Systeme dürfen dabei nicht vernachlässigt werden. Zudem müssen Störungen durch notwendige Tests einkalkuliert werden.
- Anwendungen und IT-Systeme, die der Outsourcing-Dienstleister übernehmen soll, müssen ausreichend dokumentiert sein. Die Dokumentation neuer Systeme oder Teilsysteme muss dabei ebenfalls sichergestellt sein.
- Während der Migration muss ständig überprüft werden, ob die SLAs oder die vorgesehenen Sicherheitsmaßnahmen angepasst werden müssen.

In der Einführungsphase des Outsourcing-Vorhabens und der ersten Zeit des Betriebs muss dem Notfallkonzept besondere Aufmerksamkeit geschenkt werden. Bis sich bei allen Beteiligten die notwendige Routine, beispielsweise in der Behandlung von Fehlfunktionen und sicherheitsrelevanten Vorkommnissen, eingestellt hat, sollten verstärkt Mitarbeiter zu Bereitschaftsdiensten verpflichtet werden.

Nach Abschluss der Migration muss sichergestellt werden, dass das Sicherheitskonzept aktualisiert wird, da sich erfahrungsgemäß während der Migrationsphase immer Änderungen ergeben. Dies bedeutet insbesondere:

- Alle Sicherheitsmaßnahmen müssen konkretisiert werden.
- Interne und externe Ansprechpartner und Zuständigkeiten sollten mit Namen und notwendigen Kontaktdaten (Telefon, Zeiten der Erreichbarkeit, eventuell erforderliche Zuordnungsbegriffe wie Kundennummern) dokumentiert werden.
- Die Systemkonfigurationen sind zu dokumentieren, wobei auch die eingestellten sicherheitsrelevanten Parameter zu erfassen sind.
- Das Personal ist durch Schulungsmaßnahmen auf den Regelbetrieb vorzubereiten.
- Alle Ausnahmeregelungen müssen am Ende der Migrationsphase aufgehoben werden.

Als letzte Aufgabe muss die Outsourcing-Dienstleistung nach der Migrationsphase in den sicheren Regelbetrieb (siehe OPS.3.1.M10 Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb) überführt werden.

OPS.3.1.M14 Notfallvorsorge beim Outsourcing [Notfallbeauftragter]

Für ausgelagerte Aufgaben und Prozesse des Outsourcing-Kunden gelten die gleichen Anforderungen an die Notfallvorsorge wie im Falle einer Eigenerbringung. Das bedeutet, dass der Outsourcing-Dienstleister seine Maßnahmen zur Notfallvorsorge im Rahmen der entsprechenden Auslagerung an die Anforderungen des Outsourcing-Kunden anpassen muss – insbesondere mit Blick auf Wiederanlauf- und Wiederherstellungszeiten.

Eine wirksame gemeinsame Notfallvorsorge stärkt nachhaltig das Vertrauen in der Outsourcing-Beziehung und kann die eigene Notfallvorsorge des Outsourcing-Dienstleisters verbessern. Es können Synergien entstehen, da der Outsourcing-Kunde möglicherweise Notfallarbeitsplätze für Mitarbeiter des Outsourcing-Dienstleisters im eigenen Haus zur Verfügung stellt.

Grundsätzlich sollten die Notfallkonzepte beider Parteien aufeinander abgestimmt sein. Da dieser Zustand nicht statisch ist, sollte diese Abstimmung regelmäßig und anlassbezogen wiederholt werden. Schnittstellen (z. B. Netzverbindung, Router, Telekommunikationsprovider) zwischen den Vertragsparteien und Dritten müssen identifiziert und im Rahmen der Notfallvorsorge berücksichtigt werden. In OPS.3.1.M2 Vertragsgestaltung mit dem Outsourcing-Kunden wird beschrieben, welche Aspekte bereits im Service Level Agreement geregelt werden sollten.

Im Notfallvorsorgekonzept müssen folgende Aspekte genau spezifiziert und im Detail beschrieben werden:

- Zuständigkeiten, Ansprechpartner und Abläufe müssen klar geregelt und vollständig dokumentiert werden.
- Detailregelungen für die Datensicherung (siehe Baustein OPS.1.1.5 Datensicherung) sind zu erstellen (z. B. getrennte Backup-Medien für jeden Klienten, Verfügbarkeit, Vertretungsregelungen, Eskalationsstrategien, Virenschutz).
- Es sind detaillierte Arbeitsanweisungen mit konkreten Anordnungen für bestimmte Fehlersituationen zu erstellen.
- Es muss ein Konzept für regelmäßig durchzuführende Notfallübungen erarbeitet und mit dem Outsourcing-Kunden abgestimmt werden.

Tritt ein Notfall im Haus des Outsourcing-Kunden ein, ist die Qualität der Arbeitsanweisungen für den Notfall von entscheidender Bedeutung für die Wirksamkeit der Notfallmaßnahmen. Der Outsourcing-Kunde sollte aus diesem Grund daran interessiert sein, die zu ergreifenden Notfallmaßnahmen mit dem Outsourcing-Dienstleister abzustimmen. Es ist jedoch auch im Interesse des Outsourcing-Dienstleisters, eine kompetente und schnelle Reaktion auf Notfälle des Outsourcing-Kunden zu garantieren, da der Fortbestand des Kunden und die eigene Reputation gefährdet sein können.

Dem Outsourcing-Dienstleister muss bewusst sein, dass der Outsourcing-Kunde im Zuge einer Auslagerung gegebenenfalls wesentliches Know-how für den ausgelagerten Bereich verliert und eine adäquate Notfallreaktion dadurch oft nur mit der Unterstützung des Outsourcing-Dienstleisters möglich ist.

Möglich ist zudem, dass IT-Systeme des Outsourcing-Kunden von Mitarbeitern des Outsourcing-Dienstleisters betrieben werden, ohne dass diese über Detailkenntnisse bezüglich der Anwendungen besitzen, welche auf den IT-Systemen betrieben werden. Tritt ein Fehler in einer Anwendung auf, muss der Outsourcing-Dienstleister unter Umständen eine Fehlerbehebung durchführen, ohne umfangreiche Kenntnisse über das Gesamtsystem zu besitzen. Der Outsourcing-Dienstleister sollte daher dafür sorgen, dass das Notfallvorsorgekonzept genaue Anweisungen enthält, wie er im Rahmen der Notfallbewältigung vorzugehen hat. Es kann dabei auch sinnvoll sein, Aktionen zu definieren, die explizit verboten sind (z. B. Reboot einer Maschine).

Ein Fehlverhalten einer Anwendung kann technische (z. B. voller Datenträger, Netzprobleme) oder anwendungsspezifische Ursachen haben (z. B. Verarbeitung eines falschen Datensatzes, Programmfehler, falsche Parametereinstellung). Bei technischen Fehlern ohne Auswirkungen auf andere Anwendungen wird der Outsourcing-Dienstleister den Fehler zwar selbst beheben können, eine Kooperation mit dem Outsourcing-Kunden ist meist aber dennoch notwendig, um unerwünschte Nebeneffekte auf Applikationsebene zu verhindern. Besonders bei Problemen mit komplizierten Anwendungen oder bei umfangreichen Batch-Prozessen sind häufig Kenntnisse erforderlich, über welche nur einer der Vertragspartner verfügt. Darum müssen kooperative Vorgehensweisen, Kommunikations- und Eskalationspläne im Vorhinein geplant werden.

Des Weiteren sollten der Outsourcing-Dienstleister und der Outsourcing-Kunde regelmäßig gemeinsame Übungen durchführen, die die Wirksamkeit der Notfallvorsorge der übertragenen Aufgaben und Prozesse prüft bzw. nachweist. Der Outsourcing-Dienstleister sollte die in diesem Zusammenhang benötigten Ressourcen zur Planung, Durchführung und Nachbereitung der Übungen bei seiner Kalkulation berücksichtigen.

OPS.3.1.M15 Geordnete Beendigung eines Outsourcing-Verhältnisses [Institutionsleitung]

Die Empfehlungen dieser Maßnahme lassen sich in der Regel nur umsetzen, wenn bereits im Vertrag mit dem Outsourcing-Kunden alle relevanten Themen zum Vertragsende geregelt wurden (siehe OPS.3.1.M2 Vertragsgestaltung mit dem Outsourcing-Kunden). So ist die ordnungsgemäße Rückintegration der ausgelagerten Prozesse bzw. die Übertragung dieser auf einen anderen Outsourcing-Dienstleister nur möglich, wenn ausreichend Zeit innerhalb der festgelegten Kündigungsfristen bleibt.

Zudem müssen ausreichend Vorkehrungen getroffen werden, dass durch das Vertragsende des Outsourcing-Vertrags die Geschäftstätigkeit des Outsourcing-Kunden nicht beeinträchtigt wird.

Folgende Gesichtspunkte sind zu beachten:

- Eigentumsrechte an Hard- und Software (Schnittstellenprogramme, Tools, Batchabläufe, Makros, Lizenzen, Backups) müssen geregelt werden.
- Die Weiterverwendung der vom Outsourcing-Dienstleister eingesetzten Tools, Prozeduren, Skripte und anderer Software ist für den Fall der Beendigung des Vertragsverhältnisses zu regeln.
- IT-Systeme, IT-Anwendungen und Arbeitsabläufe sollten ausreichend dokumentiert sein, um dem Outsourcing-Kunden die Reintegration der ausgelagerten Prozesse und Aktivitäten zu erleichtern.
- Alle notwendigen Informationen und Daten müssen vom Outsourcing-Dienstleister an den Outsourcing-Kunden übertragen bzw. übergeben werden.
- Alle Datenbestände des Outsourcing-Kunden beim Outsourcing-Dienstleisters müssen sicher gelöscht werden.
- Alle Berechtigungen, die im Rahmen des Outsourcing-Projekts eingerichtet wurden, sind zu überprüfen. Der Outsourcing-Dienstleister sollte alle Berechtigungen löschen, die für den Outsourcing-Kunden oder Dritte eingerichtet wurden.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

OPS.3.1.M16 Sicherheitsüberprüfung von Mitarbeitern [Leiter Personal] (CI)

Die Möglichkeiten, die Vertrauenswürdigkeit von neuem oder fremdem Personal überprüfen zu lassen, sind in Deutschland, aber auch in vielen anderen Ländern, rechtlich sehr eingeschränkt. Dazu kommt, dass die Ergebnisse meist wenig aussagekräftig sind, wie z. B. bei polizeilichen Führungszeugnissen.

Darüber hinaus kann es sinnvoll sein, sich akademische und berufliche Qualifikationen bestätigen zu lassen, beispielsweise durch Nachfragen bei der Universität oder früheren Arbeitgebern oder Kunden. Auch die Identität des Bewerbers sollte verifiziert werden, z. B. durch Vorlage von Ausweispapieren.

Der Outsourcing-Dienstleister sollte sich daher im Vorfeld der Leistungserbringung mit den Outsourcing-Kunden in Hinsicht auf die Anforderungen an das einzusetzende Personal abstimmen. Diese Anforderungen sollten bei jedem Personalwechsel oder -neuzugang berücksichtigt werden.

Bei der Vertragsgestaltung zwischen dem Outsourcing-Dienstleister und dem Outsourcing-Kunden sollte festgehalten werden, welche Seite im Bedarfsfall welche Überprüfungen durchzuführen hat und in welcher Tiefe diese zu erfolgen haben.

3 Weiterführende Informationen

3.1 Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Outsourcing für Dienstleister" finden sich unter anderem in folgenden Veröffentlichungen:

[27001A15] ISO/IEC 27001:2013

Information technology - Security techniques - Information security management systems - requirements, insbesondere Annex A, A.15 Supplier relationships, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/SC 27, Oktober 2013

[BVIT2005] Leitfaden Business Process Outsourcing

BPO als Chance für den Standort Deutschland, Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V. (Bitkom), Version 10.1, September 2005, https://www.bitkom.org/Bitkom/Publikationen/Leitfaden-Business-Process-Outsourcing.html, zuletzt abgerufen am 26.07.2018

[BVIT2008] Leitfaden Rechtliche Aspekte von Outsourcing in der Praxis

Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V. (Bitkom), Januar 2008, https://www.bitkom.org/Bitkom/Publikationen/Rechtliche-Aspekte-von-Outsourcing-in-der-Praxis.html, zuletzt abgerufen am 26.07.2018

[ISFSC1.2] The Standard of Good Practice for Information Security

Area SC1.2 Outsourcing, Information Security Forum (ISF), June 2018

[LDINRW12] Technische und organisatorische Anforderungen an die Trennung von automatisierten Verfahren bei der Benutzung einer gemeinsamen IT-Infrastruktur

Orientierungshilfe für Mandantenfähigkeit, Ständige Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Arbeitskreis Technische und organisatorische Datenschutzfragen, Version 1.0, Oktober 2012, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/04/Mandantenf%C3%A4higkeit.pdf, zuletzt abgerufen am 05.10.2018

[NIST80053F145] Security and Privacy Controls for Federal Information Systems and Organizations

NIST Special Publication 800-53, Revision 4, insbesondere Appendix F-PS Page F-145, Family: System and Services acquisition, Family: System and communications protection and Family: System and information integrity, April 2013

Umsetzungshinweise für die Bausteinschicht DER

DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle **380**

Umsetzungshinweise zum Baustein DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle

1 Beschreibung

1.1 Einleitung

Bei Advanced Persistent Threats (APT) handelt es sich um zielgerichtete Cyber-Angriffe auf ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer dauerhaften Zugriff zu einem Netz verschafft und diesen in der Folge auf weitere IT-Systeme ausweitet. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten aufseiten der Angreifer aus und sind in der Regel schwierig zu detektieren.

1.2 Lebenszyklus

Um ein APT-Vorfall erfolgreich bereinigen zu können, muss strategisch geplant und dann konsequent vorgegangen werden. Dies bedeutet, zunächst IT-Systeme gezielt abzuschalten, um den Angreifer auszusperren, dann planmäßig zu bereinigen und schließlich die bereinigte Umgebung wieder in einen produktiven Zustand zu überführen.

Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werde müssen, sind im Folgenden aufgeführt:

Planung und Konzeption

Ein APT-Vorfall kann erst bereinigt werden, nachdem dieser detektiert und korrekt als APT eingestuft wurde. Dies geschieht im Rahmen der Detektion (siehe DER.1 *Detektion von Sicherheitsrelevanten Ereignissen*), einer initialen forensischen Untersuchung (siehe DER.2.2 *Vorsorge für die IT-Forensik* und des klassischen Incident Managements (siehe Baustein DER.2.1 *Incident Management*). Die Maßnahmen des vorliegenden Bausteins müssen daher erst umgesetzt werden, nachdem die anderen Bausteine durchlaufen worden sind.

Die Bereinigung eines APT-Vorfalls stellt ein umfangreiches, arbeitsintensives Projekt dar. Daher ist zur erfolgreichen Bearbeitung ein Leitungsgremium notwendig, das dafür verantwortlich ist, die notwendigen Maßnahmen zu planen, zu konzipieren und nachzuverfolgen (siehe DER.2.3.M1 *Einrichtung eines Leitungsgremiums*). Ein APT-Vorfall stellt immer einen Notfall dar, weswegen eine Verzahnung mit dem Notfallmanagement und die Anwendung der dort definierten Maßnahmen erfolgen sollte (siehe DER.4 *BCM, Notfallmanagement*). Stellt sich heraus, dass der Vorfall unternehmensbedrohende Ausmaße hat, müssen sich die Verantwortlichen mit dem Krisenmanagement abstimmen.

Üblicherweise geht der Bereinigung eines APT-Vorfalls, nachdem er entdeckt und klassifiziert ist, zunächst eine Phase der Beobachtung des Angreifers voraus. Diese Phase dient dazu, ausreichend Informationen zu sammeln, um den Angreifer effektiv aussperren und alle von ihm etablierten Zugriffskanäle beseitigen zu können. Das Leitungsgremium legt im Rahmen einer Bereinigungsstrategie fest, ob eine Beobachtungsphase durchgeführt wird, wie lange diese andauert und welche Maßnahmen getroffen werden, um den Angreifer zu beobachten (siehe DER.2.3.M2 *Entscheidung für eine Bereinigungsstrategie*). Weiterhin wird in dieser Strategie über die genaue Vorgehensweise entschieden, mit der IT-Systeme bereinigt werden. Diese kann von der gezielten Beseitigung einzelner Infektionen, über das erneute Aufsetzen von IT-Systemen bis hin zum Austausch betroffener IT-Systeme (siehe DER.2.3.M9 *Hardwareaustausch betroffener IT-Systeme*) reichen.

Da der Angreifer potenziell vollständig auf die bestehende Kommunikationsinfrastruktur der betroffenen Institution zugreifen kann und diese aktiv beobachtet, ist es notwendig die Beobachtungsphase und die Vorbereitung der Bereinigung über sichere, unabhängige Kommunikationskanäle zu koordinieren (siehe DER.2.3.M8 *Etablierung sicherer, unabhängiger Kommunikationskanäle*).

Beschaffung

Es müssen üblicherweise verschiedene Hard- und Softwarekomponenten kurzfristig beschafft werden, um einen APT-Vorfall zu bereinigen. Beispielsweise müssen eventuell Mechanismen für die sichere Kommunikation geschaffen werden (siehe DER.2.3.M8 *Etablierung sicherer, unabhängiger Kommunikationskanäle*), Hardware für forensische Untersuchungen muss beschafft werden und eventuell ist ein Hardwaretausch von IT-Systemen mit hohem Schutzbedarf notwendig (siehe DER.2.3.M9 *Hardwareaustausch betroffener IT-Systeme*). Da die Beschaffungen sehr kurzfristig erfolgen müssen, ist es gegebenenfalls notwendig, die üblichen Beschaffungswege der Institution zu umgehen. Weiterhin soll eventuell vermieden werden, dass der Vorfall vorzeitig in der Institution oder gar darüber hinaus bekannt wird. Auch das spielt bei der Beschaffung unter Umständen eine Rolle. Durch die genannten Anforderungen entstehen eventuell Konflikte zu den üblichen Vorgaben und Prozessen für die Beschaffung. Das Leitungsgremium muss daher über weitreichende Entscheidungskompetenzen verfügen.

Umsetzung

Die Umsetzung der Bereinigung beginnt damit, den Angreifer gezielt auszusperren. Dieser Vorgang wird häufig als Cut-Off bezeichnet. Der Cut-Off wird üblicherweise dadurch realisiert, dass die betroffenen Netzbereiche isoliert werden (siehe DER.2.3.M3 *Isolierung der betroffenen Netzabschnitte*).

Anschließend kann die zuvor geplante und beschlossene Strategie zur Bereinigung der betroffenen IT-Systeme umgesetzt werden (siehe DER.2.3.M2 *Entscheidung für eine Bereinigungsstrategie*). Neben der eigentlichen Bereinigung der IT-Systeme muss zusätzlich der initiale Einbruchsweg geschlossen (siehe DER.2.3.M5 *Schließen des initialen Einbruchswegs*) und sämtliche potenziell kompromittierten Zugangsdaten und Schlüsselmaterialien müssen geändert werden (siehe DER.2.3.M4 *Sperrung und Änderung von Zugangsdaten und kryptografischen Schlüsseln*).

Bevor die Umgebung wieder in den Produktivbetrieb übergeht, sollten Maßnahmen getroffen werden, um eine erneute Kompromittierung zu erschweren, bzw. die Wahrscheinlichkeit einer zeitnahen Detektion zu erhöhen. Hierzu sollten gezielte Härtungsmaßnahmen durchgeführt werden (DER.2.3.M7 *Gezielte IT-Systemhärtung*). Außerdem sollten erneute Angriffe durch denselben Angreifer erschwert werden (siehe DER.2.3.M10 *Umbauten zur Erschwerung eines erneuten Angriffs durch denselben Angreifer*).

Erst wenn die Umgebung komplett bereinigt ist, kann sie wieder in den Produktivbetrieb überführt werden (DER.2.3.M6 *Rückführung in den Produktivbetrieb*).

Aussonderung

Während die Bereinigungsstrategie erarbeitet wird und parallel die forensischen Untersuchungen laufen, werden üblicherweise zusätzliche Detektions- und Protokollierungsmechanismen geschaffen. Hierbei handelt es sich oftmals um Ad-hoc-Lösungen, die nicht immer den Anforderungen eines langfristigen produktiven Betriebs genügen. Meistens werden die getroffenen Maßnahmen durch Datenschutzbeauftragte, Betriebsrat oder Unternehmensführung auch nur temporär genehmigt, da beispielsweise Datenschutzaspekte nicht ausreichend berücksichtigt werden können. Aus diesen Gründen müssen diese IT-Systeme häufig wieder ausgesondert werden. Es sollte jedoch nach der Bereinigung eine Phase der intensiven Beobachtung der betroffenen Umgebung eingeplant werden. Wenn möglich, sollte in dieser Phase die temporär geschaffene Infrastruktur weiter genutzt werden. Auch eine teilweise Überführung von Ad-hoc-Monitoring-Infrastruktur in den produktiven Betrieb zur Ergänzung bereits vorhandener Detektionsmechanismen (siehe auch DER.1 *Detektion von sicherheitsrelevanten Ereignissen*) sollte geprüft werden.

Bei der Aussonderung von IT-Systemen, mit denen der Angreifer beobachtet wurde oder die für forensische Analysen benutzt wurden, muss unbedingt auf die sichere Löschung oder Vernichtung sämtlicher Speichermedien geachtet werden, da auf diesen meist schützenswerte Daten enthalten sind. Weiterhin ist gegebenenfalls zu prüfen, ob forensische Daten sicher archiviert werden müssen, um nachgelagerte weitergehende Untersuchungen zu ermöglichen oder um sie als Beweismittel sicherzustellen.

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Bereinigung weitreichender Sicherheitsvorfälle" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

DER.2.3.M1 Einrichtung eines Leitungsgremiums [Informationssicherheitsbeauftragter (ISB)]

Einen Informationsverbund nach einem APT-Angriff zu bereinigen, ist ein komplexes und umfangreiches Projekt. Üblicherweise müssen verschiedene Parteien bei der Aufklärung und Bereinigung koordiniert, taktische und strategische Entscheidungen auf einer teils unklaren Informationsbasis getroffen und gleichzeitig die Bereinigungstätigkeiten zumindest kurz bis mittelfristig geheimgehalten werden. Um diese Anforderungen zu gewährleisten, müssen kompetente Ansprechpartner die Bereinigungstätigkeiten steuern. Dafür sollte ein Leitungsgremium einberufen werden, das über die folgenden Kompetenzen verfügt:

- **Entscheidungskompetenz:** Die Verantwortlichen müssen zahlreiche Entscheidungen darüber treffen, wie bei der Bereinigung konkret vorgegangen werden soll. Oftmals müssen dabei die üblichen Prozesse und Vorgaben umgangen werden, damit der Vorgang geheim bleibt und zeitkritische Prozesse umgehend durchgeführt werden können. Deshalb sollten Mitarbeiter der Leitungsebene der Institution in das Gremium miteinbezogen werden. Auch der Informationssicherheitsbeauftragte muss aufgrund seiner Schnittstellenfunktion zwischen Technik und Management und seiner grundsätzlichen Zuständigkeit dem Leitungsgremium angehören.
- **Sachkompetenz:** APT-Angriffe sind zumeist technisch sehr komplex. Die Vorfälle zu analysieren, eine wirksame Bereinigungsstrategie zu erarbeiten und Maßnahmen zu entwickeln, mit denen sich erneute Kompromittierungen vermeiden lassen, erfordern daher viel technische Expertise und umfangreiches Wissen über Informationssicherheit. Deshalb sollten zum einen erfahrene Administratoren mit möglichst bereichsübergreifenden Kenntnissen in das Gremium einbezogen werden. Zum anderen sollten interne oder externe Forensikexperten zumindest in beratender Funktion in das Gremium eingebunden sein.
- **Verwaltungskompetenz:** Die Bereinigung eines APT-Vorfalls erfordert ein komplexes Projektmanagement. Unterschiedliche Parteien müssen koordiniert und zahlreiche Aufgaben müssen unter hohem Zeitdruck aufeinander abgestimmt und umgesetzt werden. Während der Beobachtungsphase ist die Faktenlage oft noch unklar. Deswegen sollte aufgrund der sich ständig verändernden Informationsbasis und der daraus abzuleitenden Aktionen iterativ vorgegangen werden. Somit ist es notwendig, Mitarbeiter mit viel Kompetenz beim Projektmanagement in das Gremium einzubinden. Diese sind dafür zuständig, Zeitpläne zu erstellen, Aufgaben zu vergeben und nachzuverfolgen sowie die Gremiumsmitglieder mit den durchführenden Mitarbeitern zu koordinieren.

Das Leitungsgremium übernimmt das gesamte Projektmanagement für die Bereinigung. Sämtliche Entscheidungen, z. B. über die Dauer der Beobachtungsphase, zu analysierende IT-Systeme, Zeitpunkt des Cut-Offs, werden durch das Leitungsgremium getroffen. Allgemein ist das Gremium dafür zuständig, die Bereinigungsstrategie zu entwerfen, und die Durchführung zu planen und nachzuverfolgen.

Um diese Aufgaben zu bewältigen, sollte sich das Leitungsgremium regelmäßig treffen. Darüber hinaus sollten alle Gremiumsmitglieder ausschließlich über sichere Kommunikationskanäle miteinander kommunizieren (siehe DER.2.3.A7 *Etablierung sicherer, unabhängiger Kommunikationskanäle*).

Ist die IT zu stark kompromittiert oder sind die notwendigen Bereinigungsmaßnahmen sehr umfangreich, kann es sein, dass die betroffene Institution einen Krisenstab einrichtet. In diesem Fall muss das Leitungsgremium die Bereinigungsmaßnahmen überwachen. Das Leitungsgremium muss dann dem Krisenstab berichten.

DER.2.3.M2 Entscheidung für eine Bereinigungsstrategie [Informationssicherheitsbeauftragter (ISB), Leiter IT]

Bevor die Bereinigung technisch umgesetzt wird, müssen einige strategische Entscheidungen getroffen werden. Meistens wird die Bereinigungsstrategie nicht vollständig definiert, sondern vom Leitungsgremium basierend auf neuen Erkenntnissen immer wieder ergänzt und angepasst. Entscheidungen zu Eckpunkten der Bereinigungsstrategie sollten vom Leistungsgremium dokumentiert werden. Auch ist es für die praktische Arbeit hilfreich, wenn der jeweils aktuelle Stand der gesamten Strategie festgehalten und den Mitgliedern des Leitungsgremiums sowie in Ausschnitten den umsetzenden Mitarbeitern zur Verfügung gestellt wird.

Im Folgenden werden die wichtigsten Entscheidungen für eine Bereinigungsstrategie in der Reihenfolge ihrer Anwendung beschrieben. Die Entscheidungen bedingen sich teilweise, sodass später umzusetzende Entscheidungen bereits sehr früh getroffen werden müssen.

- Vor der eigentlichen Bereinigung stehen die Beobachtungsphase und der Cut-Off. Wie lang und ausführlich die Beobachtungsphase sein soll, ist bereits der erste Teil der Bereinigungsstrategie. Es sollte bestimmt werden, welche Erkenntnisse für den Cut-Off und die Bereinigung benötigt werden. Wird bereits in dieser Phase von einem vollständigen Neuaufbau der Infrastruktur ausgegangen, kann auf Detailerkenntnisse verzichtet werden. Wenn jedoch nicht ausgeschlossen wird, dass Malware später gezielt gelöscht werden soll, also die IT-Systeme möglicherweise nicht neu installiert werden müssen, werden sehr viele Informationen darüber benötigt, wie sich der Angriff ausgebreitet und wie er funktioniert hat. Außerdem werden dann Indikatoren für betroffene IT-Systeme (Indicators of Compromise, IoC) erforderlich.Das Ergebnis der Beobachtungsphase sollte eine Übersicht über die zu bereinigenden Assets sein. Stehen noch Untersuchungen aus, sollten die betroffenen Assets mit ihrem Status ebenfalls dokumentiert und die Übersichten regelmäßig aktualisiert werden. Die Übersichten sind später die Basis für die Bereinigung.
- Der Cut-Off (siehe auch DER.2.3.A3 *Isolierung der betroffenen Netzabschnitte* und DER2.3.A4 *Sperrung und Änderung von Zugangsdaten und kryptografischen Schlüsseln*) sollte grundsätzlich ohne Rücksicht auf die spätere Wiederinbetriebnahme geplant werden. Durch den Cut-Off werden betroffene IT-Systeme, Netzabschnitte und Netzgeräte teilweise oder ganz abgeschaltet, sodass nicht mehr darauf zugegriffen werden kann. In der Regel werden Cut-Off und technische Bereinigung gemeinsam geplant. Wie ein Cut-Off umgesetzt werden kann, ist in DER.2.3.M3 *Isolierung der betroffenen Netzabschnitte* beschrieben.Vor dem Cut-Off sollte geprüft werden, wie er sich auf die Institution auswirkt. Schäden, die durch die Bereinigung entstehen, können den Schaden des eigentlichen Angriffs deutlich übersteigen und existenzbedrohend sein. Das Leitungsgremium sollte, gegebenenfalls gemeinsam mit dem Krisenstab, geeignete temporäre Ausweichlösungen prüfen und die Prioritäten festlegen, nach denen die Anwendungen wieder bereitgestellt werden sollen. Hierbei kann auf den Baustein DER.4 *BCM, Notfallmanagement* zurückgegriffen werden.
- Während der Beobachtungsphase kann ein APT-Vorfall noch vertraulich behandelt werden. Nach einem Cut-Off und während der technischen Bereinigung ist der Vorfall bzw. sind die Auswirkungen typischerweise auch für Mitarbeiter, Kunden und Geschäftspartner sichtbar. Es sollte daher rechtzeitig definiert werden, wie lange der APT-Vorfall geheim gehalten werden muss, um eine effektive technische Bereinigung sicherzustellen. Für die Zeit nach der Beobachtungsphase sollte eine Kommunikationsstrategie entworfen werden, die beispielsweise eine Legende für die sichtbaren Ausfälle, vorgefertigte Antworten auf mögliche Anfragen oder eine begleitende Pressemitteilung enthält. Die Strategie ist allen direkt beteiligten Mitarbeitern bekannt zu geben. Sie kann auch mithilfe von PR-Mitarbeitern oder externen PR-Agenturen erstellt werden.
- Während der Bereinigung kommt es wahrscheinlich zu vermehrten Anfragen an den Helpdesk. Das Leitungsgremium sollte sicherstellen, das in allen Phasen ausreichend fachkundiges Personal bereitsteht, das die Bereinigungsmaßnahmen umsetzt und die Benutzer unterstützt. Auch wenn die Bereinigungsmaßnahmen zu größeren Betriebsunterbrechungen führen, muss der Helpdesk arbeitsfähig bleiben.
- Über die Beobachtungsphase hinaus müssen geeignete Monitoring-Maßnahmen etabliert werden, um bewerten zu können, ob der Cut-Off erfolgreich war und um erkennen zu können, ob es während oder nach der Bereinigung neue Angriffsaktivitäten gibt. Es ist darauf zu achten, dass diese Beobachtungsmöglichkeit durchgehend erhalten bleibt, auch wenn im Zuge der Bereinigung Systembestandteile verändert oder ausgetauscht werden. Um dies sicherzustellen, sollten die Monitoring-Maßnahmen in der Bereinigungsstrategie dokumentiert werden.
- Direkt nach dem Cut-Off können weitere forensische Untersuchungen vorgenommen werden, die zuvor nicht möglich waren, ohne den Angreifer zu warnen. Daraus können sich weiterführende Erkenntnisse für die Bereinigung ergeben.
- Basierend auf der Übersicht der betroffenen IT-Systeme und der Analyseergebnisse wird entschieden, wie die Bereinigung konkret durchgeführt wird. Für jedes IT-System ist dabei zu entscheiden und zu dokumentieren, ob es komplett neu installiert wird (eventuell zusammen mit neuer Hardware, siehe DER.2.3.A9 *Hardwaretausch betroffener IT-Systeme*), ob die Schadsoftware und andere Änderungen des Angreifers gezielt entfernt bzw. bereinigt werden oder ob keine Bereinigung notwendig ist. Grundsätzlich ist es besser die IT-Systeme neu zu installieren, als sie nur gezielt zu bereinigen, da sonst Artefakte des Angreifers auf dem IT-System verbleiben könnten. Die Maßnahmen können sich von IT-System zu IT-System unterscheiden und sind daher für jedes IT-System oder jeweils für kleinere Gruppen abzustimmen.
- Das Leitungsgremium muss einen Zeitplan für die Bereinigung ausarbeiten und abstimmen. Dabei sollten die Verantwortlichen z. B. darauf achten, dass die Institution funktionsfähig bleibt bzw. die Ausfälle so kurz wie möglich sind.
- Das Leitungsgremium sollte Vorgaben erstellen, ob und wie Datensicherungen bei der Bereinigung

DER.2.3.M3 Isolierung der betroffenen Netzabschnitte

Die Bereinigungsmaßnahmen beginnen damit, dass die betroffenen Netzbereiche isoliert werden. Ziel ist es, dem Angreifer den Zugriff auf die IT-Umgebung vollständig zu entziehen. Das sollte möglichst auf einen Schlag geschehen, damit der Angreifer nicht vorzeitig bemerkt, dass er entdeckt wurde und eventuell Gegenmaßnahmen ergreifen kann. Deshalb müssen die Netzabschnitte in einer konzertierten Aktion isoliert werden, dem sogenannten Cut-Off.

Die Verantwortlichen sollten insbesondere sämtliche Internetzugänge auf einen Schlag abschalten, um die Kommunikation des Angreifers mit kompromittierten IT-Systemen zu verhindern. Zu diesem Zwecke müssen sämtliche Zugangswege identifiziert werden (siehe DER.2.3.M2 *Entscheidung für eine Bereinigungsstrategie*). Dazu zählen beispielsweise zentrale Zugänge, eventuell vorhandene Internet-Breakouts, z. B. DSL-Anschlüsse an einzelnen Standorten, redundante Anschlüsse und Notfallverbindungen, z. B. über UMTS/LTE. Es muss jedoch unbedingt vermieden werden, dass die IT-Umgebung versehentlich erneut an das Internet angeschlossen wird, bevor die Bereinigungsarbeiten abgeschlossen sind.

Um IT-Systeme und Netze zu isolieren, sollte die Verbindung möglichst physisch getrennt werden, beispielsweise indem das entsprechende Netzkabel herausgezogen wird. Diese Vorgehensweise ist sicherer als Firewallregeln, Access Control Lists oder VLANs zu konfigurieren, um das Netz zu isolieren. Besteht der Verdacht, dass Netzgeräte kompromittiert wurden, müssen entweder die Verbindungen physisch getrennt oder die Geräte ausgeschaltet werden.

Sollte die forensische Untersuchung hinreichend sicher ergeben haben, dass nur einzelne Netzbereiche kompromittiert sind, beispielsweise eine einzelne Windows Domäne, so kann die Bereinigung auf diese Segmente begrenzt werden. In diesem Fall muss jedoch gewährleistet werden, dass die Bereiche zuverlässig von anderen Netzsegmenten abgeschottet sind.

Besonders mobile Clients sind schwer zu isolieren, da die IT zum Zeitpunkt der Isolation eventuell nicht auf alle Endgeräte zugreifen kann. Sollen mobile Endgeräte bereinigt werden, muss zunächst sichergestellt werden, dass sämtliche Zugänge (VPN, E-Mail usw.) dieser Geräte zum internen Netz getrennt werden. Es muss zudem sichergestellt sein, dass die Zugänge getrennt bleiben, bis die Bereinigungsmaßnahmen abgeschlossen sind. Anschließend müssen die Benutzer aufgefordert werden, ihr Endgerät zur Bereinigung einzureichen oder einzuschicken.

DER.2.3.M4 Sperrung und Änderung von Zugangsdaten und kryptografischen Schlüsseln

Das wesentliche Ziel der Bereinigung eines weitreichenden Sicherheitsvorfalls ist es, den Zugriff des Angreifers auf die betroffene Umgebung zu beenden und zukünftig zu unterbinden. Hierzu reicht es nicht aus, ausschließlich die Schwachstelle zu schließen, die der Angreifer zur initialen Kompromittierung ausgenutzt hat. Vielmehr muss davon ausgegangen werden, dass er alle Zugangsdaten kennt, die auf den kompromittierten Rechnern vorhanden waren. Daher müssen alle Zugangsdaten geändert werden, nachdem das Netz isoliert wurde.

Zugangsdaten sind dabei zum einen lokal gespeicherte IT-System- und Anwendungskennwörter, aber auch Passwörter von Benutzern, die sich im betroffenen Zeitraum an dem IT-System angemeldet haben, da ihre Kennwörter oder davon abgeleitete Zugangsdaten gegebenenfalls aus dem Arbeitsspeicher des IT-Systems extrahiert wurden. Weiterhin müssen auch zentral verwaltete Zugangsdaten zurückgesetzt werden, z. B. in Active-Directory-Umgebungen oder wenn Lightweight Directory Access Protocol (LDAP) benutzt wurde. Wurde einer der zentralen Authentisierungsserver (Domaincontroller oder LDAP-Server) kompromittiert, so müssen sämtliche dort vorhandenen Zugänge gesperrt und ihre Passwörter ausgetauscht werden.

Wenn ein zentraler Authentisierungsserver zurückgesetzt wird, muss dabei besonders sorgfältig vorgegangen werden. Hierbei handelt es sich um selten durchgeführte Administrationsvorgänge, die zudem oft über technische Fallstricke verfügen. Um sich beispielsweise vor sogenannten Golden Tickets zu schützen, ist es notwendig, das Kennwort des KRBTGT-Accounts zweimal zurückzusetzen. Ein Golden Ticket ist ein gefälschtes Kerberos-Ticket, mit dem für einen Zeitraum von zehn Jahren neue Zugriffstickets ausgestellt werden können. Wird das zugehörige Kennwort nicht oder lediglich einmalig zurückgesetzt, so kann ein Angreifer mit einem zuvor erstellten Golden Ticket weiterhin Zugriffstickets ausstellen und damit auf das IT-System zugreifen. Deshalb sollten ausschließlich erfahrene Administratoren mit Unterstützung durch interne oder externe Forensikexperten die entsprechenden Maßnahmen durchführen.

Üblicherweise müssen in einer solchen Situation große Teile der vorhandenen Zugangsdaten neu aufgesetzt werden. Oftmals findet dies zu einem Zeitpunk statt, zu dem die meisten Benutzer nichts oder nur sehr wenig von dem Sicherheitsvorfall wissen. Eine vorige Information der Benutzer ist oft nur schwer zu realisieren, da die IT-Infrastruktur kompromittiert ist und der Angreifer nicht vorzeitig über die anstehende Bereinigung informiert werden soll. Aus diesem Grund ist mit vermehrten Anfragen an den Helpbzw. Servicedesk zu rechnen. Wenn möglich, sollten für die erwartbaren Passwort-Anfragen zusätzliche Mitarbeiter bereitgestellt werden. Diese sollten möglichst über ein Skript verfügen, das die Vorgehensweise und die Antworten auf die erwarteten Fragen enthält. Dieses Skript sollte im Rahmen des Krisenmanagements entworfen werden, eventuell mithilfe von PR-Mitarbeitern oder externen PR-Agenturen. Die Mitarbeiter müssen insbesondere darauf hingewiesen werden, dass keine alten Passwörter wiederverwendet werden dürfen und sie auch keine Passwörter wählen sollen, die einfach aus alten Passwörter abgeleitet werden können.

Gegebenenfalls müssen auf den betroffenen IT-Systemen nicht nur Benutzerkonten und deren Passwörter zurückgesetzt werden, sondern auch Dienstkonten. Diese Änderungen müssen durch die Administratoren der jeweiligen IT-Systeme vorgenommen werden.

Weiterhin muss darauf geachtet werden, dass sämtliches kryptografisches Schlüsselmaterial, das auf kompromittierten IT-Systemen gespeichert ist, ausgetauscht werden muss. Hierzu gehören beispielsweise TLS oder SSH-Schlüssel. Wenn zentrale Schlüsselspeicher, wie z. B. eines Certification-Authority-(CA)-Servers einer selbst betriebenen Public Key Infrastructure (PKI) kompromittiert wurden, müssen sie neu aufgesetzt werden. Das impliziert auch, dass dort vorhandene Schlüssel gesperrt werden und eventuell alles abgeleitete Schlüsselmaterial neu ausgerollt werden muss. Die Zertifikate sind durch einen entsprechenden Eintrag in einer Certificate Revocation List (CRL) oder auf einem OCSP-Server zu sperren. Je nach Anwendungsfall der kompromittierten Schlüssel ist gegebenenfalls auch eine globale Sperrung durch einen externen Validierungsdienst notwendig. In diesem Fall muss bedacht werden, dass durch die Veröffentlichung von Sperrlisteneinträgen bei einem externen Validierungsdienst, öffentlich gemacht wird, dass der Schlüssel möglicherweise kompromittiert ist. Daher muss der Zeitpunkt für diese Maßnahme sorgfältig gewählt werden. Eventuell sollte auch eine entsprechende begleitende Kommunikationsstrategie erarbeitet werden.

DER.2.3.M5 Schließen des initialen Einbruchswegs

Um zu verhindern, dass ein Angreifer erneut auf eine kompromittierte Umgebung zugreift, muss der initiale Einbruchsweg des APT-Angriffs geschlossen werden. Das darf jedoch erst geschehen, nachdem die betroffenen Netzumgebungen isoliert wurden. So wird verhindert, dass der Angreifer vorzeitig gewarnt wird und eventuell noch IT-Systeme sabotiert, Spuren verschleiert oder sich zusätzliche Hintertüren schafft.

Der initiale Angriffsweg muss im Rahmen der forensischen Analyse identifiziert werden. Wurden für die Kompromittierung mehrere Schwachstellen ausgenutzt, so kann, wenn nötig, eine priorisierte Beseitigung der Schwachstellen erfolgen.

Die möglichen Einbruchswege lassen sich grundsätzlich in zwei Klassen gliedern: technische Schwachstellen und Angriffe auf Mitarbeiter. Für alle technischen Schwachstellen muss die Hauptursache identifiziert und behoben werden. Typische Beispiele sind:

- Der Angreifer hat eine bekannte Schwachstelle in veralteter Software benutzt, um auf das IT-System zuzugreifen. In diesem Fall muss geprüft werden, ob es eine aktualisierte Version der Software gibt, die nicht mehr verwundbar ist. Der Einbruchsweg ist meist geschlossen, wenn die Software aktualisiert wird.
- Der Angreifer hat eine Schwachstelle benutzt, für die keine Patches existieren oder die völlig unbekannt ist (Zero-Day-Exploit). Wenn die Schwachstelle nicht öffentlich bekannt ist, sollte Kontakt mit dem Hersteller der Software oder den internen Entwicklern aufgenommen werden, damit sie einen Patch oder andere Gegenmaßnahmen entwickeln können. Die Entwicklung eines Patches kann allerdings länger dauern. In der Zwischenzeit müssen deswegen andere Sofortmaßnahmen umgesetzt werden. Das betroffene IT-System kann z. B. vom Netz genommen oder durch Firewall-Regeln unerreichbar gemacht werden. Auch ein für die beobachtete Schwachstelle speziell entwickelter Schutz durch vorgelagerte IT-Systeme, beispielsweise mithilfe maßgeschneiderter Regeln in einer Web-Application-Firewall oder einem Intrusion-Prevention-System, kann erwogen werden. Hierfür ist allerdings spezielle Expertise notwendig.
- Der Angreifer hat ein falsch konfiguriertes IT-System ausgenutzt. Beispiele hierfür sind etwa die versehentliche Veröffentlichung schützenswerter Informationen im Internet, die Nutzung von Standard- oder leicht erratbaren Passwörtern auf extern erreichbaren IT-Systemen oder ein ungeschützter Dienst über das Internet. Hier muss das grundlegende Problem durch eine Konfigurationsänderung beseitigt werden.

Bei Angriffen auf Mitarbeiter ist es nicht einfach, die ursprüngliche Schwachstelle zu beseitigen, da sich solche Angriffe nicht vollständig durch technische Maßnahmen verhindern lassen. Beispiele für solche Angriffe sind etwa:

- Die Angreifer versenden äußerst glaubhafte Phishing-E-Mails, die entweder Schadsoftware enthalten oder den Mitarbeiter dazu bringen, schützenswerte Informationen auf nicht vertrauenswürdigen Seiten einzugeben.
- Die Angreifer benutzen sogenannte Water-Hole-Angriffe, bei denen Schadsoftware oder Phishing-Links gezielt auf Seiten hinterlegt werden, die für einzelne Mitarbeiter interessant erscheinen, sodass sie mit erhöhter Wahrscheinlichkeit darauf zugreifen.

Vor solchen Angriffen können sich Institution durch Awareness-Maßnahmen (siehe ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit*) für Mitarbeiter schützen. Sensibilisierte Mitarbeiter werden auch eher Angriffsversuche bemerken, melden und so dazu beitragen, dass Attacken frühzeitig detektiert werden können. Awareness-Maßnahmen sind nach einem erfolgreichen APT-Vorfall sinnvoll, sollten allerdings erst nach der Bereinigung durchgeführt werden.

Es können aber auch technische Maßnahmen ergriffen werden, um Angriffe auf Mitarbeiter abzuwehren. So sollten beispielsweise die IT-Systeme gezielt gehärtet (siehe DER.2.3.A7 *Gezielte IT-Systemhärtung*) und Maßnahmen umgesetzt werden, mit denen sich die IT-Umgebung überwachen lässt (Monitoring). Weitere technische Maßnahmen sind:

- Ausbau der Antivirus-Infrastruktur durch zusätzliche Prüfungen von E-Mails, ausgehendem Internetverkehr oder der Client-Endgeräte,
- die Entkopplung der Endgeräte vom Internet (beispielsweise durch ReCoBS-Systeme) oder
- die Einführung von Zwei-Faktor-Authentisierung für besonders schützenswerte Zugänge.

Es sollte jedoch vermieden werden, erfolgreich angegriffene Mitarbeiter zu bestrafen. Die Qualität der APT-Angriffe ist sehr hoch und die eingesetzten E-Mails oder Internetseiten sind oft äußerst glaubwürdig gestaltet, sodass die Angriffe nur schwer zu erkennen sind. Disziplinarische Maßnahmen wären in einem solchen Fall nicht nur unfair, sondern würden auch zu einem Vertrauensverlust führen, sodass künftige Angriffe nicht mehr frühzeitig gemeldet und erkannt werden.

DER.2.3.M6 Rückführung in den Produktivbetrieb

Nachdem die Bereinigungsarbeiten abgeschlossen sind, sollte die abgekoppelte IT-Umgebung wieder in den Produktivbetrieb überführt werden. Damit die Bereinigung möglichst wenig die Verfügbarkeit einschränkt, kann dieser Schritt stufenweise für einzelne Netzsegmente erfolgen. Hierbei muss jedoch zwingend sichergestellt sein, dass noch nicht bereinigte Netzabschnitte auf keinen Fall mit bereits bereinigten verbunden werden.

Häufig ist es erst in dieser Phase möglich, neue Passwörter und Zugangsdaten für Endanwender zu verteilen. Hierbei ist mit vermehrten Supportanfragen zu rechnen (siehe DER.2.3.M4 *Sperrung und Änderung von Zugangsdaten und kryptografischen Schlüsseln*). Auch hier kann ein stufenweiser Wiederanlauf die Anfragen reduzieren bzw. über die Zeit verteilen. Wenn möglich, sollten vor dem Neustart des Produktivbetriebs funktionale Tests durchgeführt werden, um Supportanfragen oder als Angriffssymptome missverstandene Fehlersymptome zu vermeiden.

Die zurückgeführten IT-Systeme sollten durch ein verstärktes Monitoring begleitet werden. So lassen sich erneute Zugriffsversuche des Angreifers und eventuell bisher übersehene Hintertüren identifizieren. Dazu können die während der Beobachtungsphase eingerichteten Monitoringsysteme weiter benutzt werden. Die temporär eingerichteten Überwachungs- und Analysesysteme sollten daher für einen im Rahmen der Bereinigungsstrategie definierten und mit Datenschutz und Personalvertretung abgestimmten Zeitraum weiter betrieben werden. Für diesen Zeitraum ist ein erhöhter Aufwand für die Überwachung einzuplanen.

Nachdem diese Überwachungsperiode abgeschlossen ist, sollten die Überwachungs- und Analysesysteme entsorgt oder aber in den Produktivbetrieb überführt werden. Wenn sie entsorgt werden, ist zu entscheiden, ob und gegebenenfalls welche Beweismittel zur weiteren Verwendung (beispielsweise vertiefende Analysen, für Nachweispflichten oder eventuelle Weitergabe an Strafverfolgungs- oder Ermittlungsbehörden) archiviert werden. Sollen die IT-Systeme archiviert werden, so darf dies nur in einer ausreichend gesicherten, dem Schutzbedarf der Beweismittel angemessenen Umgebung erfolgen. Nicht mehr benötigte Beweismittel und IT-Systeme, die ausgesondert werden, müssen sicher gelöscht oder vernichtet werden (siehe DER.2.3.M9 *Hardwaretausch betroffener IT-Systeme*). Auch temporär eingerichtete Kommunikations- und Kollaborationslösungen sollten wieder zurückgebaut werden.

Wenn die Monitoring- und Analysesysteme in den produktiven Betrieb übergehen, ist zu prüfen, ob diese für den gedachten Anwendungsfall auch geeignet sind. Oftmals werden in der Aufklärungsphase von APT-Vorfällen Ad-hoc-Installationen durchgeführt, die den Anforderungen an einen mittel- oder langfristigen Produktivbetrieb nicht genügen. Eventuell müssen daher Projekte zur Überarbeitung der IT-Systeme aufgesetzt werden.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Bereinigung weitreichender Sicherheitsvorfälle".

DER.2.3.M7 Gezielte Systemhärtung

Häufig nutzt ein Angreifer nicht nur eine einzelne Schwachstelle aus, sondern bedient sich über den Verlauf eines APT-Angriffs hinweg unterschiedlicher Lücken. Insbesondere kombinieren und benutzen Angreifer häufig verschiedene Schwachstellen, mangelnde IT-Systemhärtung und unzureichende Detektionsmechanismen, um sich im internen Netz zu bewegen und ihre Berechtigungen auszuweiten (privilege escalation). Neben der Beseitigung des initialen Einbruchsweges (siehe DER.2.3.A5 *Schließen des initialen Einbruchsweg*), sollten daher die IT-Systeme gehärtet werden, um die vom Angreifer genutzten Techniken zur Ausbreitung im internen Netz zu erschweren oder zu verhindern. Dabei sollten Maßnahmen, die sich mit wenig Aufwand realisieren lassen, möglichst schon während der Bereinigung durchgeführt werden. Aufwändige und weitreichende Maßnahmen können nach der Bereinigung als mittel- und langfristige Projekte umgesetzt werden.

Grundsätzlich gibt es zahlreiche unterschiedliche Möglichkeiten, einzelne IT-Systeme und gesamte Netzumgebungen zu härten. Die Auswahl der konkreten Maßnahmen hängt von den benutzen Techniken des Angreifers ab. Im Rahmen der forensischen Analyse sollten seine Werkzeuge und Vorgehensweisen zur Rechteausweitung und Bewegung innerhalb des Netzes identifiziert und konkrete Maßnahmen erarbeitet werden, mit denen APT-Angriffe zukünftig erschwert und besser detektiert werden können. Hierzu sollte der ISB gemeinsam mit den Forensikern und den für die jeweiligen IT-Systeme zuständigen Administratoren die Ergebnisse der forensischen Analysen auswerten und Gegenmaßnahmen erarbeiten.

Sinnvolle Härtungsmaßnahmen können beispielsweise auf Basis des IT-Grundschutz-Kompendiums identifiziert werden. Es sollte geprüft werden, ob für die IT-Umgebung bisher nicht erfüllte IT-Grundschutz-Anforderungen die Angriffe verhindert oder zumindest erschwert hätten. Die Umsetzung der jeweiligen Maßnahmen sollte erneut geprüft werden.

Härtungsmaßnahmen sind sehr spezifisch für die jeweilige Einzelumgebung und sollten auch möglichst individuell an diese Umgebung angepasst werden, z. B.:

- **Netzsegmentierung:** Nutzte der Angreifer eine flache oder nur grob segmentierte Umgebung aus, um Zugriff auf zahlreiche IT-Systeme zu erhalten, so bietet es sich an, das Netz in kleinere Segmente mit klar definierten und überwachten Übergängen aufzuteilen. Hierdurch wird die Anzahl der aus einem einzelnen Segment erreichbaren (und damit angreifbaren) IT-Systeme reduziert. Auch lassen sich oft die Übergänge zwischen kleineren, wohldefinierten Segmenten besser überwachen. Eine sehr feingranulare Netzsegmentierung erfordert detaillierte Kenntnisse des Netzes und insbesondere der betrieblich notwendigen Übergänge. Diese ist oftmals in Institutionen nicht vorhanden, weswegen eine feingranulare Segmentierung nur mittel- bis langfristig umsetzbar ist. Eine grobe Segmentierung lässt sich jedoch bereits im Zuge der Bereinigungsmaßnahmen umsetzen und erschwert die Bewegung eines Angreifers innerhalb des Netzes bereits erheblich.
- **Abschottung von Administrationssystemen:** Ein Spezialfall der zuvor genannten Segmentierung ist die Abschottung von administrativen IT-Systemen. Aufgrund ihrer hohen Privilegien und ihres zumeist weitreichenden Zugriffs innerhalb einer Netzumgebung sind Administratoren oftmals ein Zwischenziel bei APT-Angriffen. Deshalb sollten Administrationssysteme abgeschottet und administrative Tätigkeiten auf anormale Verhaltensmuster überwacht werden, z. B. durch ein geeignetes Monitoring. Das kann beispielsweise durch ein spezielles Admin-Netz, aus dem heraus alle Zugänge über (gehärtete und überwachte) Jumphosts oder Terminalserver erfolgen, umgesetzt werden. Administrative Zugriffe (beispielsweise über RDP oder SSH) dürfen dabei nur von diesen IT-Systemen aus erfolgen. Abweichungen hiervon sollten zu einer Alarmierung führen. Eine sehr weitreichende Architektur zur Abschottung von privilegierten Nutzern sind Microsofts Red-Forest- und ESAE-Architekturen. Die Konzepte dieser Architekturen können für eine Zielumgebung adaptiert werden, wobei viele der dort beschriebenen Maßnahmen nur mittel- bis langfristig umsetzbar sind.
- **Beschränkung von Dienstkonten:** Wurden bei einem APT-Angriff Dienstkonten missbraucht, sollten diese Konten gehärtet werden. Übliche Beispiele für solche Maßnahmen sind etwa der Betrieb von Diensten mit minimalen Privilegien. Dienste sollten möglichst nicht als *root* oder *SYSTEM* betrieben werden, sondern nur mit den Privilegien, die tatsächlich für den konkreten Einsatzzweck benötigt werden. Beispielsweise sollte das Konto für den Betrieb einer Datenbank nicht in das Stammverzeichnis des Webservers schreiben dürfen, falls beide Dienste auf demselben Server betrieben werden. Diese Prinzipien können mithilfe unterschiedlicher Techniken umgesetzt werden. Zum Beispiel können Dienste durch Container isoliert werden oder aber es können spezielle Techniken zur Steuerung von Dienstrechten genutzt werden, wie *managed service accounts* oder *group managed service accounts* unter Windows oder MAC-Systemen, wie SELinux oder AppArmor unter Linux.
- **Zusätzliche Absicherung externer Zugänge:** Konnte der Angreifer legitime externe Zugänge nutzen, beispielsweise die VPN-Zugänge von Mitarbeitern, sollten diese Zugänge gehärtet werden. Mögliche Maßnahmen könnten etwa die Einführung einer Zwei-Faktor-Authentisierung, ein Monitoring auf den Transfer größerer Datenmengen oder aber die Beschränkung der Zugriffszeiten sein.

Häufig müssen Maßnahmen im Rahmen der Bereinigung unter hohem Zeitdruck umgesetzt werden, um den Zeitraum der Isolation und damit der nicht- oder stark eingeschränkten Verfügbarkeit der Umgebung zu minimieren. Daher werden häufig zunächst Ad-hoc-Lösungen ohne die sonst üblichen Prozesse und Maßnahmen zur Qualitätssicherung umgesetzt. Es ist deswegen wichtig, die umgesetzten Maßnahmen zu überprüfen, nachdem der Regelbetrieb wieder aufgenommen wurde und Projekte für die Überarbeitung und Qualitätssicherung der entsprechenden Maßnahmen aufzusetzen. Dabei sollte auch geplant werden, wie sich Maßnahmen umsetzen lassen, für die während der Bereinigung keine Zeit mehr war.

DER.2.3.M8 Etablierung sicherer, unabhängiger Kommunikationskanäle

Bei einem APT-Angriff kann die Kommunikationsinfrastruktur kompromittiert sein. Gerade in der Beobachtungsphase, wenn das genaue Ausmaß des Angriffs unbekannt ist, sollten daher die bestehenden Kommunikationskanäle nicht benutzt werden. Andernfalls kann der Angreifer frühzeitig gewarnt werden oder ist über die angedachten Gegenmaßnahmen informiert und kann darauf reagieren.

Möglicherweise betroffene Kommunikationskanäle können sein:

- Telefonie (insbesondere mit VoIP oder bei Integration mit der IT),
- E-Mail (bei Einsatz eines E-Mail-Gateways für die Verschlüsselung auch verschlüsselte Mailserver),
- Chat und Kollaborationswerkzeuge.

Auch wenn der Angreifer nicht den Inhalt der Kommunikation kennt, kann er jedoch beispielsweise aus Kommunikationsmustern ableiten, dass er entdeckt wurde. Genauso kann der Angreifer davon über Seitenkanäle, wie abgespeicherte Anrufnotizen oder Kalendereinträge von Kommunikationsbeziehungen, erfahren.

Das Leitungsgremium und alle mit der Bereinigung beauftragten Mitarbeiter sollten daher über unabhängige Kommunikationskanäle und gegebenenfalls auch über unabhängige Kollaborationswerkzeuge verfügen. Darüber hinaus sollte geregelt werden, wann über die etablierten Kanäle kommuniziert werden darf und wann zwingend die unabhängigen Kanäle zu benutzen sind.

Es ist nicht notwendig, alle entfallenen Kommunikationskanäle zu ersetzen. Eine einfache Möglichkeit bieten persönliche Treffen und ein räumlich nahes Zusammenarbeiten des Leitungsgremiums und der direkten Unterstützer.

Üblicherweise ist es nicht möglich, neben den laufenden Untersuchungs- und Bereinigungsaktivitäten noch eine parallele Kommunikationsinfrastruktur aufzubauen. Daher wird in einer solchen Situation häufig auf Kommunikationsdienste Dritter zurückgegriffen. Bei der Auswahl eines geeigneten Kommunikationskanals ist darauf zu achten, dass die Vertraulichkeit und Integrität der Kommunikation möglichst gut geschützt wird.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

DER.2.3.M9 Hardwaretausch betroffener IT-Systeme (CIA)

Bei einem APT-Angriff können Angreifer auch über die üblichen Wege hinaus (Betriebssystem, Anwendungen) die IT-Systeme manipulieren. Dazu gehören:

- hardwarenahe Software (z. B. UEFI),
- Firmware von Systemkomponenten (z. B. CPU, GPU, Zusatzhardware),
- nicht direkt betroffene Zusatzkomponenten (z. B. Fernwartungslösungen wie ILO)
- Firmware von Netzgeräten und eingebetteten Geräten (z. B. USV),
- sicherheitskritische Einstellungen der genannten Software (z. B. nicht dokumentierte Optionen und nicht in den Wartungsprogrammen abrufbare Optionen).

Da es häufig zu diesen Komponenten jeweils nur einen eingeschränkten Zugang über die Firmware selbst gibt, kann ein Angreifer seine Manipulationen leicht verschleiern.

Diese Art von Angriffen ist für den Angreifer jedoch zeitlich, technisch und organisatorisch aufwändig. Zusätzlich muss er über weitreichenden Zugriff auf dem IT-System verfügen und den Angriff stark an die jeweilige Zielplattform anpassen. Ein solcher Angriffsvektor ist eher unwahrscheinlich, aber gerade bei einem APT-Angriff nicht auszuschließen.

Solche Manipulationen können von einer Institution nur mit hohem Aufwand und Spezialkenntnissen entdeckt werden. Da der Selbstauskunft der Komponenten nicht vertraut werden kann, müssen die Einstellungen und Firmwaredateien unabhängig von der laufenden Komponente extrahiert und analysiert werden.

Bei der Entscheidung über die Bereinigungsstrategie (siehe DER.2.3.A2 *Entscheidung für eine Bereinigungsstrategie*) sollte mindestens für Geräte mit hohem Schutzbedarf und solchen, die in Netzen mit hohem Schutzbedarf eingesetzt werden, überlegt werden, die potenziell manipulierte Hardware zu ersetzen. Grundsätzlich gibt es drei mögliche Behandlungsstrategien:

- **Keine besondere Behandlung:** Die forensische Analyse hat ergeben, dass eine Manipulation ausgeschlossen ist, da der Angreifer nicht über den nötigen Zugriff verfügte, die Komponente verlässlich gegen Manipulation gesichert ist und eine Extraktion der Firmware auch keine Hinweise auf eine Manipulation gegeben hat. Nur wenn alle diese Punkte gegeben sind, kann die Komponente für die Neuinstallation genutzt werden.
- **Software und Einstellungen zurücksetzen:** Es ist laut forensischer Analyse möglich, die IT-Systeme zu bereinigen, indem sie in den Auslieferungszustand zurückgesetzt werden oder die Firmware erneut eingespielt wird. Die Komponente ist so gestaltet, dass ein Zurücksetzen in den Auslieferungszustand oder das erneute Einspielen der Firmware unabhängig von der potenziell manipulierten Software selbst möglich ist (z. B. auf einem gesonderten Datenträger oder über einen Bootloader im ROM). In diesem Fall kann die Komponente so auch bereinigt und dann für die Neuinstallation genutzt werden.
- **Hardware tauschen:** Da eine verlässliche Erkennung unwirtschaftlich ist, sollte im Zweifel von einer Manipulation ausgegangen werden. In diesem Fall ist das gesamte System, mindestens jedoch die betroffene Komponente gegen ein Neugerät auszutauschen.

Jedes potenziell betroffene IT-System sollte in eine der drei Gruppen klassifiziert werden. Wenn es ausreichend Gründe gibt, auf einen Hardwaretausch zu verzichten, ist die Entscheidung im Rahmen der Bereinigungsstrategie begründet zu dokumentieren.

Werden neue oder zurückgesetzte IT-Systeme wieder eingerichtet, kann dabei auf bestehende Wiederanlaufpläne zurückgegriffen werden. Können hierfür Datensicherungen der Komponenten benutzt werden, sollten diese jedoch nur eingesetzt werden, wenn sie zweifelsfrei vor der Kompromittierung angelegt wurden. Da diese Sicherungen häufig in einem undokumentierten Format angelegt werden, ist es sehr aufwändig, diese zu überprüfen. Im Zweifel sollte daher neu konfiguriert und das Backup nicht verwendet werden.

Ausgesonderte Geräte müssen geeignet entsorgt werden. Sie sollten möglichst nicht an Leasingpartner zurückgegeben oder als Gebrauchtgeräte verkauft werden.

DER.2.3.M10 Umbauten zur Erschwerung eines erneuten Angriffs durch denselben Angreifer (CI)

Während eines APT-Angriffs erwirbt ein Angreifer üblicherweise detailliertes Wissen darüber, wie die Zielumgebung aufgebaut und konfiguriert ist. Im Rahmen der Netzerkundung (Reconnaissance) lernt er, wie Netzabschnitte sowie Namensschemata für IT-Systeme aufgebaut sind. Auch kennt er Benutzer- und Dienstkonten, eingesetzte Software und Services sowie Methoden für Administration und Wartung. Dieses detaillierte Wissen erleichtert es ihm, dieselbe Umgebung erneut anzugreifen. Gelingt es dem Angreifer nach der Bereinigung, sich erneut Zugang zur IT-Umgebung zu verschaffen, z. B. indem er eine neue Schwachstelle oder eine übersehene Hintertür ausnutzt, kann er sein Wissen dazu benutzen, um innerhalb kurzer Zeit wieder weitreichende Kontrolle über die Zielumgebung zu erlangen.

Um einem APT-Angreifer die erneute tiefgreifende Kompromittierung einer Umgebung zu erschweren, kann die IT-Umgebung gezielt umgebaut werden, sodass das Wissen des Angreifers über den internen Aufbau nutzlos ist. Beispiele für solche Maßnahmen sind:

- Nutzung anderer IP-Adressbereiche für Netzsegmente und/oder anderer IP-Adressen für einzelne IT-Systeme,
- Änderung von Namensschemata für Computer und/oder Änderung von Namen einzelner IT-Systeme,
- Änderung von Namensschemata für Anwender- und Dienstkonten und/oder Änderung von Namen für einzelne Konten,
- Änderung von URL-Pfaden für Webanwendungen und/oder Web-Services.

Werden die Maßnahmen umgesetzt, müssen die relevanten Dokumentationen aktualisiert sowie die Nutzer benachrichtigt und durch Administratoren begleitet werden.

Bei den beschriebenen Maßnahmen handelt es sich nicht um Sicherheitsmaßnahmen im eigentlichen Sinne. Es sind vielmehr Verschleierungsmaßnahmen, die jedoch einen gewissen Schutz bieten können. Zum einen ist dann eine erneute Kompromittierung für den Angreifer aufwändiger, da er zuvor gewonnenes Wissen nicht wiederverwerten kann. Zum anderen können die beschriebenen Maßnahmen durch gezielte Detektion ergänzt werden. Werden Detektionsmechanismen etabliert, die auf die Nutzung des alten Angreiferwissens abzielen, steigt die Chance, einen wiederkehrenden Angreifer zu erkennen. Setzt er beispielsweise eine ehemals verwendete IP-Adresse oder einen alten Kontonamen ein, wird darüber der IT-Betrieb alarmiert. Solche Alarmierungen führen in der Anfangsphase nach einer Umstellung häufig zu vielen Fehlalarmen, da noch nicht alle Konfigurationen von benachbarten IT-Systemen angepasst wurden oder Benutzer und Administratoren sich noch nicht an die geänderten Gegebenheiten angepasst haben. Diese Fehlalarme lassen sich jedoch typischerweise mit überschaubarem Aufwand aussortieren und nehmen mit der Zeit ab, sodass letztlich ein hochwertiges Alarmierungskriterium etabliert werden kann.

Ebenso sollte gezieltes Monitoring eingesetzt werden, wenn das *KRBTGT*-Passwort zweimal zurückgesetzt wurde, um Golden-Ticket-Angriffe zu vermeiden (siehe auch DER.2.3.A4 *Sperrung und Änderung von Zugangsdaten und kryptografischen Schlüsseln*). Anschließend sollte überwacht werden, ob ungültige Kerberos-Tickets eingesetzt werden. Die Nutzung entsprechender Tickets lässt sich über Einträge mit der Event-ID *4769* im Security-Event-Log der Domänencontroller erkennen. Ist hier der Fehler-Code auf den Wert *0x1f* gesetzt, deutet das auf *Golden Tickets* hin und sollte zu einer umgehenden Alarmierung führen.

3 Weiterführende Informationen

3.1 Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Bereinigung weitreichender Sicherheitsvorfälle" finden sich unter anderem in folgenden Veröffentlichungen:

[CS072] Erste Hilfe bei einem APT Angriff

BSI-Veröffentlichungen zur Cyber-Sicherheit (BSI-CS 072), Version 3.0, Januar 2016, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_072_TLP-White.pdf, zuletzt abgerufen am 05.10.2018

[DRP] Data Breach Response Guide

Experian Data Breach Resolution, 2013
https://www.experian.com/assets/data-breach/brochures/response-guide.pdf, zuletzt abgerufen am 05.10.2018

[GMSA] Windows Server 2012: Group Managed Service Accounts

Microsoft TechNet,
https://blogs.technet.microsoft.com/
askpfeplat/2012/12/16/windows-server-2012-group-
managed-service-accounts/, zuletzt abgerufen am 05.10.2018

[KGT] CERT-EU Security Whitepaper Protection from Kerberos Golden Ticket

Mitigating pass the ticket on Active Directory, CERT-EU, Juli 2014,
https://cert.europa.eu/static/WhitePapers/CERT-EU-
SWP_14_07_PassTheGolden_Ticket_v1_1.pdf, zuletzt abgerufen am 05.10.2018

[MSMSA] Managed Service Accounts: Understanding, Implementing, Best Practice and Troubleshooting

Microsoft, September 2009, https://blogs.technet.microsoft.com/
askds/2009/09/10/
managed-service-accounts-understanding-implementing-best-practices-and-
troubleshooting/, zuletzt abgerufen am 05.10.2018

[PARM] Securing Privileged Access Reference Material

Microsoft TechNet, Dezember 2016,
https://docs.microsoft.com/de-de/
windows-server/identity/securing-privileged-access/securing-privileged-ac-
cess-reference-material, zuletzt abgerufen am 05.10.2018

[ReCoBS] Common Criteria Protection Profile for Remote-Controlled Browsers System (ReCoBS)

BSI-PP-0040, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 1.0, Februar 2008,
https://www.commoncriteriaportal.org/files/ppfiles/pp0040b.pdf, zuletzt abgerufen am 11.09.2018

[SANS1] Whitepaper When Breaches Happen: Top Five Questions to Prepare For

SANS Institute, June 2012, https://www.sans.org/reading-room/whitepapers/analyst/breaches-happen-top-questions-prepare-35220, zuletzt abgerufen am 05.10.2018

[SANS2] Detection and Recovery from a Major security Breach

Richard Hanschu, SANS Institute, 2000, https://giac.org/paper/gcux/50/detection-recovery-major-security-breach/100810, zuletzt abgerufen am 05.10.2018

Umsetzungshinweise für die Bausteinschicht APP

APP.1: Client-Anwendungen

Umsetzungshinweise zum Baustein APP.1.1 Office-Produkte

1 Beschreibung

1.1 Einleitung

Office-Produkte sind seit Langem fester Bestandteil der Standardausstattung der IT im Büroumfeld. Schriftstücke digital zu bearbeiten und Kalkulationen sowie Präsentationen am PC zu erstellen, hat den Büroalltag stark verändert. Entsprechend betrachten die meisten Mitarbeiter Office-Produkte als Grundausstattung der IT. Gerade wegen der großen Verbreitung von Office-Produkten werden diese auch als Angriffsweg genutzt, beispielsweise um mittels Makros in Office-Dokumenten Schadsoftware zu verbreiten.

Daher sollten für einen sicheren Einsatz von Office-Produkten Sicherheitsmaßnahmen geplant und umgesetzt werden, die dem Schutzbedarf der Institution angemessen sind.

Die nachfolgenden Umsetzungshinweise beziehen sich in einigen Beispielen, falls nicht anders erwähnt, auf Microsoft Office ab Version 2010 und LibreOffice ab Version 5.1. Ältere Versionen von Microsoft Office und LibreOffice werden von den Herstellern nicht mehr mit Updates versorgt und sollten daher nicht mehr im produktiven Betrieb eingesetzt werden.

1.2 Lebenszyklus

Planung und Konzeption

In der Planungs- und Konzeptionsphase sollen Grundsätze definiert werden, wie Office-Produkte in der Institution zu verwenden sind und welche Anforderungen die Institution an Office-Produkte hat. Damit sollen für die Institution und die Anforderungen der Mitarbeiter passende Office-Produkte ausgewählt werden (siehe APP.1.1.M5 Auswahl geeigneter Office-Produkte). Ebenso sollte bereits in der Planungs- und Konzeptionsphase definiert werden, wie mit Aktiven Inhalten (z. B. Makros) in Office-Dokumenten umgegangen werden soll (siehe APP.1.1.M2 Einschränken von Aktiven Inhalten) und ob Erweiterungen der ausgewählten Office-Produkte eingesetzt werden sollen (APP.1.1.M11 Geregelter Einsatz von Erweiterungen für Office-Produkte).

Beschaffung

Bei der Beschaffung von Office-Produkten spielt die Lizenzverwaltung eine große Rolle. Die Hersteller bieten meist mehrere Lizenzmodelle an, von denen je nach Umfang der benötigten Installationen für die Institution andere Modelle sinnvoll sind (siehe APP.1.1.M8 Versionskontrolle von Office-Produkten).

Umsetzung

Vor dem Einsatz in der Institution sollten neue Versionen von Office-Produkten getestet werden (siehe APP.1.1.M6 Testen neuer Versionen von Office-Produkten), um zu gewährleisten, dass bestehende Arbeitsmittel der Institution (z. B. Dokumentvorlagen oder Formblätter) auch mit der neuen Version korrekt funktionieren. Je nach den festgelegten Grundsätzen, wie innerhalb der Institution mit Office-Produkten gearbeitet werden soll, muss die eingesetzte Software anders konfiguriert werden. Bei der Konfiguration sollte sichergestellt sein, dass auf allen Arbeitsplätzen der Institution eine möglichst einheitliche Konfiguration der Office-Produkte eingespielt ist.

Betrieb

Um die Sicherheitsanforderungen der Institution im täglichen Einsatz von Office-Produkten zu erfüllen, müssen die Benutzer der Office-Produkte mit eingebunden werden. So müssen sie über Sicherheitsmaßnahmen informiert werden, die nicht rein technisch umgesetzt werden können und die Mitwirkung der Benutzer benötigen. Relevante Themen sind hierbei das Öffnen von Office-Dokumenten aus externen Quellen, der Umgang mit Meta- oder Restinformationen in Office-Dokumenten, der Umgang mit Möglichkeiten zur Cloud-Speicherung sowie die Integritätsprüfung von Office-Dokumenten und der Umgang mit signierten oder passwortgeschützten Office-Dokumenten, siehe z. B. APP.1.1.M9 Beseitigung von Restinformationen vor Weitergabe von Dokumenten und APP.1.1.M12 Verzicht auf Cloud-Speicherung.

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Office-Produkte" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

APP.1.1.M1 Sicherstellen der Integrität von Office-Produkten

Office-Produkte sollte grundsätzlich nur aus bekannten Quellen, wie Originaldatenträgern oder der Webseite des Herstellers, bezogen werden. Es sollte dokumentiert werden, welche Quelle für die eingesetzten Office-Produkte gewählt wird und wie der Prozess zur Integritätssicherung der Installationsquellen gestaltet ist.

In der Vergangenheit kam es immer wieder zu Vorfällen, bei denen Angreifer Softwarepakete auf den Downloadseiten von Softwareherstellern manipulieren konnten. Um zu verhindern, dass manipulierte Software in der Institution ausgerollt wird, sollte die Authentizität von Softwarepaketen der eingesetzten Office-Produkte streng überprüft werden.

Um zu verhindern, dass unberechtigt modifizierte Versionen der Office-Produkte in der Institution installiert werden, sollte die Software vor der Installation auf Integrität und Authentizität geprüft werden. Für diese Prüfung stellen viele Hersteller signierte Prüfsummen zur Verfügung, mittels derer verifiziert werden kann, dass die Software ausschließlich durch den Hersteller verändert wurde.

Die Authentizität von Microsoft Office wird beim Installieren durch den Installationsagenten sichergestellt. Zusätzlich kann die Signatur über die Dateieigenschaften der Softwarepakete unter *Digitale Signaturen | Details* überprüft werden. Microsoft bietet außerdem das Kommandozeilenprogramm SignTool an, mit dem Signaturen von Programmen überprüft werden können. Wird Microsoft Office über den Windows-Update-Mechanismus aktuell gehalten, wird die Signatur bei Aktualisierungen automatisch geprüft.

Für LibreOffice sind mehrere Methoden verfügbar, um die Integrität der Softwarepakete zu prüfen:

1. Für alle angebotenen Softwarepakete auf der Webseite zu LibreOffice werden PGP-Signaturen bereitgestellt. Der zugehörige öffentliche PGP-Schlüssel der LibreOffice-Enwickler hat die Schlüssel-ID AFEEAEA3 und kann über Schlüsselserver bezogen werden:
   gpg --keyserver hkp://keys.gnupg.net --recv-keys AFEEAEA3
   Der Fingerabdruck des PGP-Schlüssels ist
   C283 9ECA D940 8FBE 9531 C3E9 F434 A1EF AFEE AEA3.
   Die PGP-Signatur-Dateien haben die Endung .ASC. Mit dem öffentlichen PGP-Schlüssel und der veröffentlichten Signatur-Datei kann die Authentizität und Integrität der Softwarepakte beispielsweise folgendermaßen geprüft werden:
   gpg --verify LibreOffice_5.2.0_Win_x86.msi.asc LibreOffice_5.2.0_Win_x86.msi
2. Die veröffentlichten Softwarepakete für Windows sind mit einer Digitalen Signatur versehen, die mit dem ebenfalls eingebetteten X509-Zertifikat der LibreOffice-Entwickler geprüft werden kann. Die Signatur kann über die Dateieigenschaften des Softwarepaketes unter *Digitale Signaturen | Details* überprüft werden.
3. Falls LibreOffice über den Paketmanager (zum Beispiel rpm oder yum) einer Linux-Distribution installiert wird, wird die Authentizität und Integrität in der Regel durch Paketmanager sichergestellt.

Wird die Integrität der Office-Produkte manuell geprüft, sollte die Prüfung auf einem gehärteten System erfolgen. Die Programme, mit denen die Integrität geprüft wird, sollten vor Manipulation geschützt werden.

Das gewählte Vorgehen für die Integritätsprüfung der Office-Produkte sollte an geeigneter Stelle (beispielsweise im Betriebshandbuch) für Dritte nachvollziehbar dokumentiert werden. Bei hohen Anforderungen an die Integrität der Office-Produkte kann es Sinn machen, die Protokolle über die durchgeführten Integritätsprüfungen aufzubewahren.

APP.1.1.M2 Einschränken von Aktiven Inhalten [Benutzer]

Office-Produkte bieten häufig die Möglichkeit, Dokumente um Aktive Inhalte zu erweitern. Aktive Inhalte sind beispielsweise Makros, mit denen aufwändigere Berechnungen durchgeführt werden oder Aktive-X-Steuerelemente, mit denen in Office-Dokumenten umfangreiche Formulare eingebettet werden können. In integrierten Programmierumgebungen der Office-Produkte können Aktive Inhalte mit beliebig komplexen Funktionen entwickelt werden.

Allerdings werden Aktive Inhalte auch sehr häufig genutzt, um Schadcode in Office-Dokumente einzubetten und so zu verbreiten. Daher sollte das automatische Ausführen von Aktiven Inhalten in den Einstellungen der Office-Produkte verhindert werden.

In Microsoft Office kann der Umgang mit Aktiven Inhalten im Sicherheitscenter konfiguriert werden. Das Sicherheitscenter ist zu finden unter *Datei | Optionen | Sicherheitscenter | Einstellungen für das Sicherheitscenter*. Dort kann konfiguriert werden, wie Microsoft Office mit Makros und Aktive-X-Komponenten umgehen soll.

In LibreOffice kann in den Optionen eingestellt werden, wie Aktive Inhalte behandelt werden. Die Sicherheitsoptionen zu den Makros sind zu finden unter *Extras | Optionen | LibreOffice | Sicherheit | Makrosicherheit*.

Bei manchen Office-Produkten besteht die Möglichkeit, digital signierte Aktive Inhalte, die von vertrauenswürdigen Quellen stammen, zu aktivieren. Diese Funktion ist vor allem dann sinnvoll, wenn Makros in organisationseigenen Office-Dokumenten benötigt werden. So werden Benutzer nicht unnötig oft mit der Warnung vor Aktiven Inhalten konfrontiert, was der Sensibilisierung der Benutzer zugute kommt.

Zudem müssen Benutzer auf die Gefahren, die sich durch Aktive Inhalte ergeben, hingewiesen werden. Keinesfalls dürfen die Benutzer die Aktiven Inhalte beim Öffnen leichtfertig aktivieren. Im Zweifel sollten die Benutzer sich an den IT Service Desk der Institution wenden, der gemeinsam mit dem IT-Betrieb entscheiden kann, wie mit den Dokumenten zu verfahren ist. Beispielsweise ist es möglich, Dokumente mit Aktiven Inhalten in abgeschotteten IT-Umgebungen zu prüfen.

Auch Aktive Inhalte in PDF-Dateien eröffnen Sicherheitsrisiken, werden aber nur selten tatsächlich benötigt. Daher sollte die automatische Ausführung solcher Inhalte in den PDF-Anzeige-Programmen deaktiviert werden.

APP.1.1.M3 Öffnen von Dokumenten aus externen Quellen

Office-Dokumente, die aus externen Quellen stammen (z. B. von Webseiten heruntergeladen, von externen Mitarbeitern oder Geschäftspartnern erhalten) müssen mit besonderer Vorsicht behandelt werden. Es dürfen keine Dokumente geöffnet werden, die unerwartet erhalten wurden oder deren Absender bzw. Herkunft unbekannt ist. Grundsätzlich müssen Office-Dokumente aus externen Quellen wie ausführbare Dateien behandelt werden und vor dem ersten Öffnen zumindest auf Schadsoftware geprüft werden.

Aktuelle Versionen von Microsoft Office verwenden das Open XML Dateiformat als Standard. Dateien im Open XML Dateiformat, die Makros enthalten, sind mit einem "M" in der Dateiendung gekennzeichnet. Beispielsweise haben Word-Dokumente mit Makros die Endung .DOCM statt .DOCX. Enthält eine Office Open XML Datei Makros, ohne entsprechend gekennzeichnet zu sein, so verweigert Microsoft Office, die Datei zu öffnen (beispielsweise wenn Makros in einer Datei mit der Endung .DOCX enthalten sind). Ältere Dokumentenformate (z. B. .DOC) können grundsätzlich Makros enthalten und werden von Microsoft Office gemäß der Einstellungen im Sicherheitscenter behandelt (siehe APP.1.1.M2 Einschränken von Aktiven Inhalten). In der folgenden Auflistung sind Dokumententypen von Microsoft Office aufgeführt, die Makros enthalten können und daher besonders aufmerksam behandelt werden sollten:

- .DOC
- .DOT
- .DOCM
- .DOTM
- .XLA
- .XLS
- .XLT
- .XLSB
- .XLSM
- .XLTM
- .XLAM
- .PPT
- .PPTM
- .POTM
- .PPSM
- .PPAM
- .PPA

Bei Microsoft Office kann zusätzlich die Office-Dateiüberprüfung aktiviert werden. Dabei werden ältere Office-Dateiformate beim Öffnen gegen ein Binärschema verglichen, um mögliche Angriffe auf noch unbekannte Softwarefehler in Microsoft Office zu erkennen. Entspricht die geöffnete Datei nicht dem bekannten Binärschema, wird eine Warnung ausgegeben. Bei strengeren Sicherheitsanforderungen kann die Office-Dateiüberprüfung so konfiguriert werden, dass Dokumente, die die Prüfung nicht bestehen, nicht geöffnet werden können.

Betriebssystem, Webbrowser und E-Mail Client sollten so konfiguriert werden, dass vor dem Öffnen von Dateien aus externen Quellen (z. B. USB-Sticks von Dritten, Downloads von Websites, oder E-Mails) die Überprüfung auf Schadsoftware obligatorisch ist (siehe Baustein OPS.1.1.4 Schutz vor Schadprogrammen).

Auch bei im alltäglichen Einsatz weniger geläufigen Dateiformaten ist Vorsicht geboten. Beispielsweise ist das im Druckumfeld nach wie vor verbreitete PostScript neben einer Seitenbeschreibungssprache, die beschreibt, wie Informationen exakt auf Papier oder in entsprechenden Anzeige-Programmen dargestellt werden sollen, auch eine vollständige Programmiersprache. So kann es zu Problemen ähnlich wie bei Makro-Viren kommen.

APP.1.1.M4 Absichern des laufenden Betriebs von Office-Produkten

Die meisten Hersteller von Office-Anwendungen bieten auf ihren Webseiten Empfehlungen für eine sichere Konfiguration der Produkte sowie über den Umgang mit identifizierten Sicherheitslücken. Diese sollten genutzt werden. Verfügbare Patches und Updates sollten zeitnah eingespielt werden.

Office-Software und andere Standardsoftware sollte nie mit Administratorrechten gestartet werden. Es sollten nur solche Dateien direkt in den Anwendungen geöffnet werden, deren Herkunft als vertrauenswürdig eingeschätzt wird. Bevor Dateien aus externen Quellen geöffnet werden, müssen sie vorab durch ein aktuelles Virenschutzprogramm überprüft werden.

Standardsoftware ist im Allgemeinen nicht auf ein hohes Sicherheitsniveau ausgelegt. Alle Mitarbeiter sollten daher darauf hingewiesen werden, dass besonders schutzbedürftige Informationen nicht beliebig auf einem Standard-Büroarbeitsplatz verarbeitet werden sollten. Einige Standardprodukte bieten eine Reihe von Sicherheitsfunktionen an, die aber meist deutlich weniger Sicherheit bieten als spezielle Sicherheitsprodukte für den erhöhten Schutzbedarf. Die Benutzer sollten über diese Sicherheitsfunktionen und deren Wirksamkeit informiert werden. Dabei ist vor allen Dingen sicherzustellen, dass die Benutzer sich nicht in einer falschen, trügerischen Sicherheit wiegen und dass die Nutzung dieser Sicherheitsfunktionen keine Sicherheitslücken öffnet. Benutzer sollten darüber informiert werden, dass Office-Produkte nicht für jeden beliebigen Einsatzzweck geeignet sind.

Für die Weitergabe von Dokumenten an Externe sollten bevorzugt Dateiformate verwendet werden, die weniger Restinformationen enthalten und mit denen die nachträgliche Änderungen bzw. auszugsweise Weiterverarbeitung erschwert werden kann. Hierfür können z. B. PDF-Dateien verwendet werden, die über die Sicherheitsoptionen der erstellenden Anwendung entsprechend eingeschränkt wurden.

Auch PDF-Dateien können Schadcode enthalten, der Sicherheitslücken ausnutzt. In PDF-Dateien lassen sich Funktionen wie Programmaufrufe einbetten, die ein Sicherheitsrisiko für die Dateien des lokalen IT-Systems darstellen. Häufig wird für solche Angriffe JavaScript verwendet. Vor allem ältere Versionen von PDF-Anwendungen sind für eine solche Infiltration anfällig. Häufig werden die Benutzer dafür auf eine manipulierte Webseite gelockt, wo dann eine präparierte PDF-Datei im Hintergrund geladen wird. Mit dem in der Datei versteckten Code wird Schadsoftware auf dem Rechner des Benutzers installiert. Dafür muss die Datei nicht einmal manuell geöffnet werden.

Antiviren-Programme erkennen infizierte PDF-Datei in vielen, aber nicht in allen Fällen, da die Angreifer den Schadcode ständig variieren. Umso wichtiger ist es, die eingesetzten Anwendungen regelmäßig auf Aktualität zu prüfen und Sicherheitsupdates schnell zu installieren.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Office-Produkte".

APP.1.1.M5 Auswahl geeigneter Office-Produkte

Die Funktionen der Office-Produkte sollten sich an den Bedürfnissen der Benutzer orientieren. Um dies zu gewährleisten, sollten die zukünftigen Benutzer der Office-Produkte in den Auswahlprozess in geeigneter Form eingebunden werden. So ist es beispielsweise sinnvoll, dass die Kriterien für die Auswahl der Office-Produkte gemeinsam von IT-Betrieb und Anwendern aufgestellt werden. Bei einer Neubeschaffung sollte hierfür vorab eine Marktanalyse durch die IT-Abteilung durchgeführt werden, um eine Vorauswahl zu definieren.

Auf Basis der Marktanalyse und der Erfahrungen der Benutzer sollte ein Anforderungskatalog erstellt werden, der die Auswahl der passenden Office-Produkte unter den verschiedenen Alternativen unterstützt. Die Anforderungen können hierbei in die beiden Klassen MUSS-Anforderungen und SOLL-Anforderungen gegliedert werden. MUSS-Anforderungen sind von dem zur Auswahl stehenden Office-Produkt zwingend zu erfüllen, um in die nähere Betrachtung zu kommen. SOLL-Anforderungen sind optional, dienen aber dazu, zwischen mehreren Office-Produkten in der näheren Auswahl zu entscheiden. SOLL-Anforderungen können zudem mit einem Gewichtungsfaktor versehen werden, um die Rangfolge der Anforderungen anzugeben. So können die Office-Produkte ausgewählt werden, die alle MUSS-Anforderungen erfüllen und die meisten Punkte in den SOLL-Anforderungen erzielen.

Die nachfolgende Tabelle zeigt eine beispielhafte Auswertung der Anforderungsanalyse.

Anforderung	MUSS/SOLL	Gewicht	Office-Produkt 1	Office-Produkt 2	Office-Produkt 3
Viewer-Funktion (Geschützter Modus)	MUSS	-	Ja	Nein	Ja
Aktive Inhalte einschränkbar	MUSS	-	Ja	Ja	Ja
Unterstützt Dateiformate XYZ	MUSS	-	Ja	Ja	Ja
Multi-Plattform-fähig	SOLL	10	Nein	Ja	Ja
Unterstützung digitaler Signaturen in Dokumenten	SOLL	20	Ja	Nein	Nein
Ergebnis	-	-	20 Punkte	K.O.	10 Punkte

In obigem Beispiel scheidet Office-Produkt 2 aus, da eine MUSS-Anforderung nicht erfüllt ist. Office-Produkt 1 und Office-Produkt 3 erfüllen alle MUSS-Anforderungen, wobei Office-Produkt 1 die meisten Zusatzpunkte aufgrund der SOLL-Anforderungen erhält.

Die am meisten verbreitete Anwendungen zur Arbeit mit PDF-Dateien sind Adobe Reader bzw. Adobe Acrobat. An Marktführern orientieren sich auch Schadsoftware-Entwickler. Daher kann es sinnvoll sein, weniger verbreitete PDF-Betrachter einzusetzen oder zumindest vorzuhalten, um bei akuten Warnmeldungen ausweichen zu können.

APP.1.1.M6 Testen neuer Versionen von Office-Produkten

Für einen geordneten Betriebsübergang von Office-Produkten und bei wesentlichen Änderungen ist ein geeignetes Vorgehen bei Test und Freigabe erforderlich. Die Tests dienen dazu, Probleme mit neuen Versionen von Office-Produkten frühzeitig zu erkennen. Für die Planung und Umsetzung von Tests sowie der darauf basierenden Freigabe sind üblicherweise die folgenden Ebenen zu berücksichtigen, bei denen jeweils andere Funktionsträger mit ihrer fachlichen Perspektive einzubeziehen sind:

- die fachliche Ebene (Vertreten durch Fachverantwortliche)
- die Ebene des IT-Betriebs (Vertreten durch den IT-Leiter)
- die Ebene der Informationssicherheit (Vertreten durch den Informationssicherheitsbeauftragten)

Für alle genannten Ebenen sind Test- und Überprüfungsszenarien sowie Kriterien für die Freigabe zu entwickeln. Hierbei sollte Berücksichtigung finden:

- Auf der fachlichen Ebene muss geprüft werden, ob die neue Version des Office-Produkts mit den etablierten Arbeitsmitteln (wie Dateiformate, Standardvorlagen, Formulare und Auswertungsbögen) kompatibel ist.
- Der IT-Betrieb sollte sicherstellen, dass neue Versionen der Office-Produkte in die IT-Infrastruktur und die IT-Betriebsabläufe integriert werden können.
- Konzeption und Betrieb der Office-Produkte müssen konform mit dem Regelwerk (Leitlinien, Richtlinien), den Konzepten (z. B. Kryptokonzept) und den Best Practices zur Informationssicherheit sein. Es ist insbesondere darauf zu achten, dass die benötigten Sicherheitsfunktionen umgesetzt wurden und einwandfrei funktionieren.

Vor der Durchführung von Tests sollte die Art und Weise der Ergebnissicherung und -auswertung festgelegt werden, insbesondere im Hinblick auf die Wiederholbarkeit von Prüfungen. Es muss geklärt werden, welche Daten während und nach der Prüfung festzuhalten sind.

Für die Tests der Office-Produkte sollten vor der Testdurchführung die Testfälle definiert werden. Dabei sollten die folgenden Kategorien berücksichtigt werden:

- Standardfälle sind Fälle, mit denen die korrekte Verarbeitung der definierten Funktionalitäten überprüft werden soll.
- Fehlerfälle sind Fälle, in denen versucht wird, mögliche Fehlermeldungen der Office-Produkte zu provozieren.
- Ausnahmefälle sind Fälle, bei denen die Office-Produkte ausnahmsweise anders reagieren müssen als bei Standardfällen. Es muss daher überprüft werden, ob das Programm diese Fälle als solche erkennt und korrekt bearbeitet.

Auf der fachlichen Ebene können pro zu prüfendem Arbeitsmittel für jede Kategorie Testfälle definiert werden. Beispielsweise können für einen Auswertungsbogen als Standardfälle Eingabedaten und erwartete Auswertungsergebnisse vorab definiert werden.

Zur Testdurchführung sollte der IT-Betrieb eine geeignete Testumgebung zur Verfügung stellen. Die Umgebung sollte möglichst nahe an der Arbeitsumgebung sein, in der die Office-Produkte eingesetzt werden.

Die Durchführung der Tests muss anhand des Testplans erfolgen. Jede Aktion sowie die Testergebnisse müssen ausreichend dokumentiert und bewertet werden. Insbesondere wenn Fehler auftreten, sind diese derart zu dokumentieren, dass sie reproduziert werden können. Die für den späteren Produktionsbetrieb geeigneten Betriebsparameter müssen ermittelt und für die spätere Erstellung einer Installationsanweisung festgehalten werden.

Zeigt sich bei Bearbeitung einzelner Testinhalte, dass eine oder mehrere Anforderungen des Anforderungskataloges nicht konkret genug waren, sind diese gegebenenfalls zu konkretisieren.

Anhand der festgelegten Entscheidungskriterien sind die Testergebnisse zu bewerten, alle Ergebnisse zusammenzuführen und mit der Testdokumentation den Testverantwortlichen vorzulegen.

Nach Abschluss der Tests ist ein Pilotbetrieb der neuen Version der Office-Produkte sinnvoll, also ein Einsatz unter realen Bedingungen. Erfolgt der Pilotbetrieb in der Produktionsumgebung mit Echtdaten, muss vorab durch eine ausreichende Anzahl von Tests die korrekte und fehlerfreie Funktionsweise der Office-Produkte bestätigt worden sein, um die Integrität der Produktionsumgebung nicht zu gefährden. Dabei kann das Produkt beispielsweise bei ausgewählten Benutzern installiert werden, die es dann für einen gewissen Zeitraum im echten Produktionsbetrieb einsetzen.

Werden in der Testphase Inkompatibilitäten mit den Arbeitsmitteln der Institution erkannt, sollte entschieden werden, wie damit verfahren wird. Hierfür ist es sinnvoll, Fehlerklassen zu definieren, nach denen eingestuft werden kann, ob der Fehler den flächendeckenden Einsatz der neuen Version der Office-Produkte verhindert oder ob für eine Übergangsfrist die Inkompatibilitäten akzeptiert werden können. Für die Fehlerbehebung sollte definiert werden, welche Anpassungen an den Arbeitsmitteln für die neue Version der Office-Produkte erforderlich sind. Für die Umsetzung der Änderungen siehe Maßnahme APP.1.1.M10 Regelung der Software-Entwicklung durch Endbenutzer.

APP.1.1.M7 Installation und Konfiguration von Office-Produkten

Um eine standardisierte Installation der Office-Produkte zu gewährleisten, sollte eine Installations- und Konfigurationsanleitung erstellt werden, die auch die nötigen Schritte zur Anpassung der Konfiguration enthält. Die Office-Produkte sollten ausschließlich nach der dokumentierten Anleitung auf den dafür vorgesehenen IT-Systemen installiert und konfiguriert werden. Idealerweise erfolgt die Konfiguration über zentralisierte Verfahren.

Abweichungen von der Installationsanweisung und insbesondere der dort angegebenen Standardkonfiguration müssen in jedem Fall genehmigt und dokumentiert werden.

Wenn die Benutzer die Software selbst installieren sollen, sollte mindestens die Pilot-Installation durch einen ausgewählten typischen Benutzer durch die IT-Abteilung begleitet werden, um die Verständlichkeit der Installationsanweisung zu überprüfen. Anhand der Erkenntnisse aus der Pilot-Installation sowie weiterer Rückmeldungen der Benutzer sollte die Installationsanweisung aktualisiert und verbessert werden.

Sowohl vor als auch nach der Installation von Software sollte eine vollständige Datensicherung durchgeführt werden. Die erste Datensicherung kann bei nachfolgenden Problemen während der Installation zur Wiederherstellung eines konsolidierten Aufsetzpunktes verwendet werden. Nach der erfolgreichen Installation sollte erneut eine vollständige Datensicherung durchgeführt werden, damit bei späteren Problemen wieder auf den Zustand nach der erfolgreichen Installation des Produktes aufgesetzt werden kann.

Da Office-Produkte meist auf fast allen Arbeitsplätzen einer Institution installiert sind, empfiehlt es sich, die Konfiguration zentral zu verwalten. Hierfür existieren je nach eingesetztem Betriebssystem auf den Arbeitsplätzen mehrere Möglichkeiten:

- Im Windows-Umfeld kann die einheitliche Konfiguration der Office-Produkte in der Regel per Gruppenrichtlinien auf die Arbeitsplätze verteilt werden.
- Im Mac OS- und Unix-Umfeld kann eine einheitliche Konfiguration mit Anwendungen zum Konfigurations-Management verwaltet werden.

Die Standardkonfiguration der Office-Produkte sollte in regelmäßigen Abständen überprüft und bei Bedarf angepasst werden. Die angepasste Standardkonfiguration sollte anschließend auf den Arbeitsplätzen der Institution ausgerollt werden.

APP.1.1.M8 Versionskontrolle von Office-Produkten

Es sollte erfasst werden, welche Versionen von Office-Produkten in der Institution installiert sind und in welcher Konfiguration diese vorliegen. Werden verschiedene Versionen von Office-Produkten eingesetzt, kann es zu Kompatibilitätsproblemen beim Bearbeiten von Dokumenten kommen, und die Wartung und Pflege wird erschwert. Die Dokumentation der ausgerollten Versionen und Konfigurationen von Office-Produkten kann bei der schnellen Fehlerbehebung sehr hilfreich sein. Für die Übersicht der Konfigurationen kann eine Dokumentation der Standardkonfiguration erstellt werden (beispielsweise im Betriebs- oder Installationshandbuch der Office-Produkte). So müssen nur noch Abweichungen von der Standardkonfiguration gesondert dokumentiert werden. Bei jeder Änderung der Standardinstallation oder Standardkonfiguration sollte die Dokumentation angepasst werden. Wird eine Konfiguration eingespielt, die von der Standardkonfiguration abweicht, sollte die abweichende Konfiguration, der Grund dafür sowie der Arbeitsplatz dokumentiert werden, auf dem die abweichende Konfiguration vorhanden ist.

Es sollten regelmäßige Kontrollen erfolgen, bei denen geprüft wird, ob die eingesetzten Versionen der offiziell freigegebenen Standardversion der Institution entsprechen.

Die konkrete Ausgestaltung der Bestandsführung und der Kontrollen richtet sich nach dem Umfang der Installationen und der Größe der Institution. So können für kleinere Organisationen mit wenigen Installationen von Office-Produkten einfache Listen ausreichten, die manuell in Stichproben gegen die tatsächlichen Installationen von Office-Produkten geprüft werden. In größeren Institutionen ist eine Bestandsführungssoftware sinnvoll, mit der es möglich ist, automatisierte Kontrollen der eingesetzten Versionen durchzuführen.

APP.1.1.M9 Beseitigung von Restinformationen vor Weitergabe von Dokumenten [Benutzer]

Office-Dokumente können in der Regel um eine Vielzahl an Meta-Informationen angereichert werden. Diese umfassen beispielsweise Angaben zum Autor, zur letzten Freigabe oder zur Version des Dokuments. Sie können aber auch schützenswerte Informationen enthalten. Bei der Veröffentlichung von Office-Dokumenten oder der Weitergabe an Dritte ist es daher erforderlich, nicht erwünschte Restinformationen zu entfernen.

Es sollte genau überlegt werden, welche Metadaten die Datei enthalten soll. Hier kann es beispielsweise erwünscht sein, einer Datei eine Vielzahl von Metadaten mitzugeben, damit diese über Suchmaschinen gefunden werden kann. Es kann aber auch sinnvoll sein, keine Metadaten weiterzugeben. Beispielsweise sollte der Name des Autors entfernt werden, wenn ein Dokument anonymisiert weitergegeben werden soll.

Hier ist es sinnvoll, den Benutzern eine Checkliste an die Hand zu geben, die ihnen ermöglicht, unerwünschte Restinformationen zu identifizieren und nach einem definierten Prozess zu löschen.

Beispielhafte Checkliste:

Eingebettete Dokumente entfernen Prüfen, ob in dem Office-Dokument weitere Dokumente als Objekte eingebettet sind. Eingebettete Dokumente sollten entfernt, als Anlage referenziert werden und gegebenfalls als eigenes Dokument mitgeliefert werden.	
Überarbeitungs-Informationen entfernen Text, der im Änderungen-Nachverfolgen-Modus eingefügt wurde, sollte entweder akzeptiert werden oder verworfen werden. Die Änderungsinformationen selbst dürfen nicht in veröffentlichten Dokumenten enthalten sein.	
Kommentare entfernen Kommentare im Text müssen vor der Veröffentlichung von Dokumenten entfernt werden.	
Überflüssige Dokumenteneigenschaften entfernen In der Regel sind nur die Dokumenteneigenschaften Autor, Titel, Version und Datum relevant. Die restlichen Dokumenteneigenschaften sollten vor der Veröffentlichung entfernt werden.	
Auf nicht-sichtbaren Inhalt prüfen Abschließend sollte das Dokument auf Inhalte geprüft werden, die nicht sichtbar sind. Das können beispielsweise ausgeblendete Tabellenspalten, Textpassagen, die von einem Bild verdeckt werden oder auch Text in derselben Farbe wie der Hintergrund sein.	

Viele Office-Produkte bieten Funktionen, mit denen die Prüfung auf Restinformationen weitestgehend automatisiert erfolgen kann oder in gewissem Umfang vor vorhandenen Restinformationen gewarnt wird. Für speziellere Überprüfungen kann auch auf Zusatzsoftware oder Eigenentwicklungen zurückgegriffen werden.

Beispielsweise können in LibreOffice Warnungen zu Restinformation in Dokumenten aktiviert werden. Die Einstellungen hierzu sind zu finden unter *Extras | Optionen | LibreOffice | Sicherheit | Sicherheitsoptionen und -warnungen*.

In Microsoft Office können Warnungen zu Restinformationen im Sicherheitscenter aktiviert werden. Optionen hierzu sind unter *Datei | Optionen | Sicherheitscenter | Einstellungen für das Sicherheitscenter* zu finden. Hier können Warnungen unter Datenschutzoptionen im Bereich Dokumentspezifische Einstellungen aktiviert werden. Außerdem stellt Microsoft Office eine Prüffunktion bereit. Diese kann unter *Datei | Informationen | Auf Probleme überprüfen | Dokument prüfen* durchgeführt werden. Bei der Prüffunktion werden bestimmte Restinformationen im Dokument automatisch geprüft und in einem Bericht angezeigt, der gleichzeitig Optionen zum Bereinigen bietet. Bei der Prüffunktion sollte definiert werden, welche Prüfungen sinnvoll sind und welche Bereinigungen durchgeführt werden können.

Häufig sollen in einem Dokument vor dessen Veröffentlichung zudem einzelne Passagen unkenntlich gemacht werden. Abhängig vom Dateiformat sind geeignete Methoden zu ergreifen. Eine beliebte, aber extrem fehlerträchtige Methode ist es, Textpassagen elektronisch zu "schwärzen". Die so übermalten Informationen sind allerdings in vielen Fällen einfach auslesbar. Daher ist dies unbedingt zu unterlassen.

Ein weiteres Beispiel für mögliche Restinformationen ist OLE (Object Linking And Embedding, Dienst zum Verknüpfen und Einbetten von Objekten). Über OLE-Funktionen können Objekte in Dateien eingebettet werden. Diese werden in vielen Office-Produkten benutzt, um Informationen anderen Programmen zur Verfügung zu stellen. Hierüber kann beispielsweise eine in Excel erstellte Tabelle in einem Word-Dokument eingebettet werden. Damit werden aber nicht nur die in dem Tabellenausschnitt dargestellte Informationen, sondern unter Umständen alle in der Excel-Datei enthaltenen Informationen in die Word-Datei übertragen. Wenn die Word-Datei dann weitergegeben wird, kann der Empfänger dann auch die Excel-Datei einsehen und sogar verändern, auch wenn diese durch ein Passwort lese- oder schreibgeschützt war. Um dies zu verhindern, sollte in diesem Beispiel die Tabelle als Text in die Word-Datei kopiert werden. Nur wenn die Ursprungs-Excel-Datei keine anderen Informationen enthält, als solche, die weitergegeben werden sollen, sollte sie in einer andere Datei eingebettet werden. Dies kann z. B. durch Anlegen einer neuen Excel-Datei erreicht werden.

Der Umgang mit Restinformationen in Office-Dokumenten sollte Teil der Anwenderschulungen sein. Insbesondere sollte der Umgang mit Software zur automatisierten Entfernung von Restinformationen geschult werden, falls diese eingesetzt wird. In Sensibilisierungskampagnen sollte zusätzlich auf die Gefahren durch Restinformationen hingewiesen werden.

APP.1.1.M10 Regelung der Software-Entwicklung durch Endbenutzer [Benutzer]

In Office-Dokumenten kann unter anderen mit Makros in Dokumenten oder Berechnungen und Zellenbezügen in Tabellenkalkulationen umfangreiche und komplexe Programmlogik implementiert werden. Dabei besteht die Gefahr, dass solche Office-Dokumente von Benutzern in Fachabteilungen als Werkzeuge immer weiterentwickelt werden, aber weder eine nachvollziehbare Dokumentation erstellt wird, noch Funktionstests durchgeführt werden. So werden eigenentwickelte Makros oder Programme auf Basis von Office-Anwendungen im schlimmsten Fall unerlässliche Werkzeuge in der Abteilung, können aber nicht mehr gewartet werden oder enthalten gar unentdeckte Fehler.

Um dies zu verhindern, sollte vom Management entschieden werden, in welchem Umfang solche Softwareentwicklungen durch die Endbenutzer in der Institution zulässig sind. Bei der Entscheidung sollte der Schutzbedarf der zu verarbeitenden Daten einbezogen werden. So kann es sinnvoll sein, ein Schutzbedarfslimit zu definieren, bis zu dem die Daten in Eigenentwicklungen verarbeitet werden können. Übersteigt der Schutzbedarf der Daten dieses Limit, sind Eigenentwicklungen in zentral durch den IT-Betrieb verwaltete Lösungen zu migrieren.

Werden Eigenentwicklungen grundsätzlich erlaubt, sollte definiert werden, wie diese zu dokumentieren und zu testen sind und welche Qualitätsanforderungen für Eigenentwicklungen in Form von Office-Dokumente bzw. Werkzeugen gelten. Hierfür ist es empfehlenswert, die Eigenentwicklungen je Abteilung in einem Katalog bzw. einer Liste zu erfassen und je Anwendung/Office-Werkzeug einen Verantwortlichen mit Vertreter zu benennen. Dieser Verantwortliche ist für die Einhaltung der Qualitätsanforderungen sowie Pflege, Dokumentation und Tests seiner Werkzeuge verantwortlich. Weitere Hinweise zu Tests von Office-Produkten finden sich in Maßnahme APP.1.1.M6 Testen neuer Versionen von Office-Produkten.

APP.1.1.M11 Geregelter Einsatz von Erweiterungen für Office-Produkte

Viele Office-Produkt können mit Erweiterungen an die Bedürfnisse der Institution angepasst werden. Diese Erweiterungen können nicht ohne die zugehörigen Office-Produkte verwendet werden, stellen aber aufgrund ihrer Komplexität eigene Softwareprodukte dar. Daher müssen eingesetzte Erweiterungen ebenso wie die Office-Produkte selbst in geregelter Form eingesetzt werden. Hierzu zählen:

- Geregelte Auswahl geeigneter Erweiterungen
- Bezug der Erweiterungen aus offiziellen Quellen
- Nach Möglichkeit Überprüfung der Prüfsummen bzw. der Signaturen der Erweiterungen bei der Installation
- Patch-Management der Erweiterungen
- Dokumentation der Konfiguration der Erweiterungen
- Testen der Erweiterungen auf Kompatibilität mit den eingesetzten Versionen der Office-Produkte

Besonderer Fokus liegt hierbei auf dem Testen der Erweiterungen auf Kompatibilität mit der eingesetzten Version. Hierbei ist zu beachten, dass sich die Entwicklungszyklen von Office-Produkten und deren Erweiterungen unterscheiden und so möglicherweise sehr viel häufiger neue Versionen der Erweiterungen erscheinen, als es neue Versionen der Office-Produkte gibt.

Die Tests der Erweiterungen sollten wie für die Office-Produkte selbst auf isolierten Testsystemen nach klar dokumentierten Testabläufen mit Ergebnisdokumentation durchgeführt werden. Hierbei sollten die Hinweise zum Testen der Software aus APP.1.1.M6 Testen neuer Versionen von Office-Produkten beachtet werden.

In Microsoft-Office besteht die Möglichkeit, nur signierte Erweiterungen (Add-Ins) von vertrauenswürdigen Herausgebern zu erlauben. Diese Funktion kann im Sicherheitscenter aktiviert werden. Zu finden ist die Funktion unter *Datei | Optionen | Sicherheitscenter | Einstellungen für das Sicherheitscenter... | Add-Ins*.

APP.1.1.M12 Verzicht auf Cloud-Speicherung [Benutzer]

In einigen Office-Produkten sind Funktionen integriert, die es ermöglichen, Dokumente direkt online zu speichern, zu synchronisieren und für Dritte freizugeben. Diese Funktionen können für den Privatanwender durchaus komfortabel sein, stellen im geschäftlichen Einsatz allerdings mehr Gefahr als Nutzen dar. So können beispielsweise schützenswerte Daten ungewollt veröffentlicht werden, wenn die Funktion unbedarft benutzt wird.

Alle Funktionen von Office-Produkten zur Cloud-Speicherung von Dokumenten sollten daher deaktiviert werden.

Der Bedarf für einen Austausch und eine gemeinsame Bearbeitung von Dokumenten sollte dabei nicht komplett ignoriert werden. Dies führt meist dazu, dass die Benutzer sich selbst helfen und nicht freigegebene Software oder unerlaubte Cloud-Lösungen nutzen. Daher sollten die Benutzer in Schulungen auf die in der Institution erlaubten Möglichkeiten zum Backup von Dokumenten, zum Datenaustausch mit Externen und zur Nutzung von Cloud-Diensten hingewiesen werden. Um Dokumente für Dritte zur Sichtung oder Bearbeitung freizugeben, sollten beispielsweise geeignete Kollaborationsplattformen eingesetzt werden, die über Sicherheitsfunktionen wie eine verschlüsselte Datenablage und -versendung und ein geeignetes System zur Benutzer- und Rechteverwaltung verfügen.

In Microsoft Office 2013 ist die Cloud-Speicher-Option SkyDrive integriert. Um diese zu deaktivieren, sollte bei der Installation darauf geachtet werden, dass die Komponente "Microsoft SkyDrive Pro" in den Installationsoptionen deaktiviert ist. Zusätzlich sollten unter *Datei | Optionen | Speichern* die Punkte *"Backstage beim Öffnen oder Speichern von Dateien nicht anzeigen"* und *"Standardmäßig auf Computer speichern"* markiert werden. Der Punkt *"Zusätzliche Speicherorte anzeigen, auch wenn eine Anmeldung erforderlich ist"* sollte deaktiviert werden. Die Cloud-Speicherung kann auch über eine Gruppenrichtlinie deaktiviert werden. Dazu ist die Option *"Show SkyDrive Sign In"* in *User Configuration | Administrative Templates | Microsoft Office 2013 | Miscellaneous* auf *"Disabled"* zu setzen.

APP.1.1.M13 Verwendung von Viewer-Funktionen [Benutzer]

Dokumente aus potentiell unsicheren Quellen, wie dem Internet oder E-Mails, können Schadsoftware enthalten, die beim Öffnen ausgeführt wird. Dies können sowohl Makros sein, als auch Code der Schwachstellen der eingesetzten Office-Produkt-Versionen ausnutzt. Um diese Gefahr zu reduzieren, sollten Viewer eingesetzt werden.

Das können einerseits gesonderte Anwendungen sein, die speziell für den Zweck entwickelt wurden, Office-Dokumente ausschließlich anzuzeigen. Viele Office-Produkte beinhalten aber auch einen sogenannten geschützten Modus, bei dem nur ein geringer Teil der Funktionen des Office-Produkts aktiviert ist.

Je nach Einsatzbereich und Schutzbedarfsanforderungen sollte abgewogen werden, welche Alternative zweckmäßig ist. In Bereichen mit erhöhten Sicherheitsanforderungen ist es stets empfehlenswert, gesonderte Viewer-Anwendungen einzusetzen.

Die Einstellungen für den integrierten geschützten Modus kann bei Microsoft Office unter *Datei | Optionen | Sicherheitscenter | Einstellungen für das Sicherheitscenter... | Geschützte Ansicht* verwaltet werden. Die Einstellungen sollten möglichst zentral per GPO gesteuert werden. Microsoft stellt hierfür für jede Microsoft Office Version Administrative Vorlagendateien für Gruppenrichtlinien zur Verfügung.

Im Adobe Reader ab Version Zehn (Adobe Reader X) ist eine Sandbox (oder "Geschützter Modus") integriert, um Angriffen entgegen zu wirken. Daher sollten Anwender, die zur Betrachtung und Bearbeitung von PDF-Dokumenten Adobe Reader nutzen, Adobe Reader X oder neuer einsetzen und den "Geschützten Modus" nutzen.

APP.1.1.M14 Schutz gegen nachträgliche Veränderungen von Informationen [Benutzer]

Viele Anwendungsprogramme bieten Sicherheitsmechanismen an, um den weiteren Umgang mit den erstellten Dateien einzuschränken. Da die Sicherheitsmechanismen der verschiedenen Anwendungsprogramme sehr unterschiedlich ausgeprägt sind und teilweise sogar von Version zu Version variieren, ist es wichtig, die Mitarbeiter darüber zu informieren, wie diese zu benutzen sind und welche Schritte vor der Weitergabe von elektronischen Dokumenten zu beachten sind. Es ist häufig sinnvoll, einen Mitarbeiter (plus Vertreter) gründlich hierzu auszubilden. Dieser sollte dann alle weiterzugebenden Dokumente entsprechend der Sicherheitsvorgaben bearbeiten oder als Ansprechpartner zur Verfügung stehen.

Im Folgenden werden einige solcher Sicherheitsmechanismen am Beispiel von PDF-Dateien vorgestellt.

Schutz von PDF-Dokumenten

Mit Adobe Acrobat, also der verbreitetsten Anwendung, mit der PDF-Dateien erstellt und nachbearbeitet werden können, ist die Vergabe von zwei Arten von Passwörtern möglich. Die einen werden zum Öffnen des Dokuments, die anderen zum Ändern der Sicherheitsattribute benötigt. Bei der Vergabe eines Passwortes wird zunächst danach gefragt, zu welchen Programmversionen die Schutzfunktion kompatibel sein soll. Bis zur Version "Adobe 5.0 und höher" ist dabei nur eine 40-Bit-Verschlüsselung mit RC4 möglich, ab "Adobe 5.0 und höher" ist eine 128-Bit-Verschlüsselung mit RC4 und ab "Adobe 7.0 und höher" ist eine 128-Bit-Verschlüsselung mit AES vorgesehen. Es sollte darauf geachtet werden, mindestens mit 128 Bit zu verschlüsseln, da der Dokumentenschutz sonst einfach ausgehebelt werden kann.

Über die Sicherheitsattribute können unter anderem folgende Funktionen eingeschränkt werden:

- Öffnen des Dokuments
- Drucken
- Ändern des Dokuments
- Kopieren von Texten, Bildern oder anderen Inhalte
- Zugriff auf Metadaten eines Dokuments
- Notizen und Formularfelder hinzufügen oder ändern

So können sehr einfach die Rechte beschränkt werden, so dass niemand mit Cut and Paste die Inhalte einer Veröffentlichung übernehmen kann. Wenn im Extremfall sogar das Ausdrucken verhindert wird, kann die Datei nur online gelesen werden.

Leider bietet dies nur einen rudimentären Schutz, da PDF-Dateien (abhängig von der Programmversion, mit der sie erstellt wurden) auch mit Programmen geöffnet werden können, die diese Sicherheitsattribute ignorieren. Solange z. B. Drucken erlaubt wird, kann das Dokument sogar jederzeit wieder in eine PDF-Datei ohne jegliche Einschränkungen verwandelt werden.

Es können PDF-Sicherheitsrichtlinien erstellt werden. Diese kann jeder Benutzer für sich erstellen oder es können von der Institution vorgegebene Sicherheitsrichtlinien verwendet werden, hierfür ist ein Adobe Policy Server erforderlich.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

APP.1.1.M15 Einsatz von Verschlüsselung und Digitalen Signaturen (CI)

Bei erhöhten Anforderungen an die Authentizität, Integrität und Vertraulichkeit von Office-Dokumenten sollten Digitale Signaturen eingesetzt werden, um die Authentizität und Integrität sicherzustellen. Zudem sollten die Dokumente verschlüsselt werden, um die Vertraulichkeit zu gewährleisten. Entscheidend für die Sicherheit der Signatur- und Verschlüsselungsverfahrens ist die Güte des verwendeten Algorithmus und die Schlüsselauswahl.

Hohe Integritätsanforderungen:

Bestehen hohe Anforderungen an die Integrität der Office-Dokumente, beispielsweise um die Nicht-Abstreitbarkeit zu gewährleisten, können digitale Signaturen eingesetzt werden. Beim Einsatz von digitalen Signaturen, die in die Office-Dokumente eingebettet werden, sollte beachtet werden, dass die eingesetzte Methode zum Kryptokonzept (siehe Baustein CON.1 Kryptokonzept) der Institution passt. Es kann erforderlich sein, das Kryptokonzept um die Methode zum Signieren der Office-Dokumente zu erweitern. In der Regel muss eine institutionsweite Schlüsselverwaltung etabliert sein, um die Signaturfunktionen sinnvoll zu nutzen. Falls zudem Benutzer außerhalb der Institution mit den signierten Dokumenten arbeiten, muss außerdem beachtet werden, dass die eingesetzte Lösung einen etablierten Standard implementiert, der auch von weiteren Institutionen problemlos genutzt werden kann.

In Microsoft Office können Dokumente mit einer integrierten Funktion signiert werden. Diese ist zu finden unter *Datei | Informationen | Dokument schützen | Digitale Signatur* hinzufügen. Damit wird dem Dokument eine Digitale Signatur zugewiesen, die beim Öffnen in Microsoft Office geprüft werden kann. Zusätzlich ist es möglich, ein im Dokument sichtbares Signaturfeld einzufügen. Das ist über *Einfügen | Signaturzeile* möglich. Um das Dokument zu signieren, muss der Unterzeichner seine Signatur über Rechtsklick auf die jeweilige Signaturzeile im Kontextmenü im Punkt *"Signieren..."* einfügen.

In LibreOffice ist es ebenfalls möglich, ein Dokument digital zu signieren. Hier findet sich die Funktion unter *Datei | Digitale Signaturen*. Die Digitalen Signaturen werden nach der XML Signature Spezifikation erzeugt und in die LibreOffice Dokumente eingebettet.

Hohe Vertraulichkeitsanforderungen:

Office-Dokumente mit hohen Anforderungen an die Vertraulichkeit sollten bei der Übertragung verschlüsselt werden. Teilweise bieten Office-Produkte integrierte Funktionen zur Verschlüsselung von Dokumenten. Integrierte Verschlüsselungsfunktionen von Office-Produkten sollten allerdings nicht ohne vorherige Analyse eingesetzt werden. So sollte sicherstellt werden, dass die angebotene Verschlüsselungsfunktion auch die Anforderungen der Institution erfüllt (siehe Baustein CON.1 Kryptokonzept). Es muss bereits in der Planung darauf geachtet werden, dass Algorithmen und Verfahren eingesetzt werden, die aktuell dem Stand der Technik entsprechen, auch noch auf absehbare Zeit einen angemessenen Schutz bieten können. Zudem ist zu beachten, dass je nach eingesetzten Office-Produkten Meta-Informationen nicht mit verschlüsselt werden. Falls die integrierten Verschlüsselungsfunktionen der Office-Produkte den Ansprüchen der Institution nicht genügen, sollten alternative Möglichkeiten eingesetzt werden.

Microsoft-Office Dokumente können über die Funktion *Datei | Informationen | Dokument schützen | Mit Kennwort verschlüsseln* verschlüsselt werden. Aktuelle Versionen von Microsoft Office setzen AES mit einer Schlüssellänge von 128 Bit im CBC-Modus ein. Versionen vor Microsoft Office 2007 setzen standardmäßig schwächere Algorithmen mit kürzeren Schlüssellängen ein. Die integrierte Verschlüsselungsfunktion dieser Versionen sollte daher nicht genutzt werden.

LibreOffice-Dokumente können über die Funktion *Datei | Eigenschaften | Sicherheit | Schützen* verschlüsselt werden. Alternativ kann der Haken bei der Option "Mit Kennwort speichern" im Speichern-Dialogfenster gesetzt werden. LibreOffice setzt in der aktuellen Version standardmäßig AES mit einer Schlüssellänge von 256 Bit im CBC-Modus ein. In früheren Versionen wurden ebenfalls Blowfish sowie AES mit Schlüssellängen von 128 und 192 Bit eingesetzt.

APP.1.1.M16 Integritätsprüfung von Dokumenten (I)

Dokumente, für die hohe Anforderungen an die Integrität bestehen, sollten bei der Übertragung mittels Prüfsummen (beispielsweise CRC, MD5 Hash oder SHA Hash) oder digitalen Signaturen (siehe Maßnahme APP.5.2.M15 Einsatz von Verschlüsselung und Digitalen Signaturen) abgesichert werden. Wichtig zu beachten ist dabei, dass nur digitale Signaturen zuverlässig absichtliche Veränderungen erkennen lassen.

Für unbeabsichtigte Änderungen (Bitfehler etc.) stellen viele Office-Produkte automatisierte Reparaturfunktion zur Verfügung, mit denen defekte Office-Dokumente teilweise wiederhergestellt werden können. Hierbei ist zu beachten, dass die Möglichkeit Dokumente wiederherzustellen, abhängig vom Dateiformat des Office-Dokuments ist. So besteht für Office-Dokumente, die im Office Open XML Format (ab Office 2007) gespeichert wurden, eine größere Wahrscheinlichkeit zur Wiederherstellung nach Integritätsverlusten.

3 Weiterführende Informationen

3.1 Wissenswertes

LizenzverwaltungAuf allen IT-Systemen der Institution müssen korrekt lizenzierte Office-Produkte eingesetzt werden. Daher sollten die Lizenzen der Installationen regelmäßig kontrolliert werden. Es ist sinnvoll, die Bestandsführung der Software-Lizenzen im Rahmen der Versionskontrolle vorzunehmen.

Werden Office-Produkte ohne gültige Lizenz eingesetzt, kann das im schlimmsten Fall Strafzahlungen und Kosten für die Nachlizenzierung zur Folge haben. Daher muss eine Übersicht erstellt werden, aus der ersichtlich ist, wie viele Lizenzen für die eingesetzten Office-Produkte vorhanden sind und wie viele Lizenzen bereits verbraucht wurden. Diese Übersicht hilft ebenfalls bei der Planung für künftig benötigte Lizenzen.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Office-Produkte" finden sich unter anderem in folgenden Veröffentlichungen:

[KB2501584] Microsoft-Sicherheitsempfehlung

Microsoft Office-Dateiüberprüfung für Office 2003, Office 2007 und Office 2010, https://support.microsoft.com/de-de/kb/2501584, zuletzt abgerufen am 06.09.2018

[LODS] Digitale Signaturen anwenden

LibreOffice, https://help.libreoffice.org/Common/Applying_Digital_Signatures/de, zuletzt abgerufen am 06.09.2018

[LORP] Libre Office Release Plan

The Document Foundation, https://wiki.documentfoundation.org/Release-Plan, zuletzt abgerufen am 06.09.2018

[MS35554] Office 2013 Administrative Template files (ADMX/ADML) and Office Customization Tool

Microsoft, https://www.microsoft.com/en-us/download/details.aspx?id=35554, zuletzt abgerufen am 06.09.2018

[MSD35811] Visio 2013 Viewer

Microsoft, https://www.microsoft.com/en-us/download/details.aspx?id=35811, zuletzt abgerufen am 06.09.2018

[MSDN338205] Introducing the Office (2007) Open XML File Formats

Microsoft, https://msdn.microsoft.com/en-us/library/aa338205.aspx, zuletzt abgerufen am 06.09.2018

[MSDN368289] Digital Signatures and Windows Installer

Microsoft, https://msdn.microsoft.com/en-us/library/windows/desktop/aa368289.aspx, zuletzt abgerufen am 06.09.2018

[MSDN380259] Cryptography Tools

Microsoft, https://msdn.microsoft.com/en-us/library/aa380259.aspx, zuletzt abgerufen am 06.09.2018

[MSDN387764] SignTool

Microsoft, https://msdn.microsoft.com/en-us/library/aa387764.aspx, zuletzt abgerufen am 06.09.2018

[MSFSD] Office 2013 - can I disable the "SkyDrive" save option under Word

Microsoft, http://answers.microsoft.com/en-us/office/forum/office_2013_release-word/office-2013-can-i-disable-the-skydrive-save-option/e358c2e0-0c10-4251-b1b5-aabe59407ed7, zuletzt abgerufen am 06.09.2018

[MSODS] Hinzufügen oder Entfernen einer digitalen Signatur in Office-Dateien

Microsoft, https://support.office.com/de-de/article/Hinzuf%C3%BCgen-oder-Entfernen-einer-digitalen-Signatur-in-Office-Dateien-70d26dc9-be10-46f1-8efa-719c8b3f1a2d, zuletzt abgerufen am 06.09.2018

[TN179125] Planen von Kryptografie - und Verschlüsselungseinstellungen für Office 2013

Microsoft, https://technet.microsoft.com/de-de/library/cc179125.aspx, zuletzt abgerufen am 06.09.2018

[TN194021] Guide to Office 2013 Security

Microsoft, https://technet.microsoft.com/en-us/library/dn194021.aspx, zuletzt abgerufen am 06.09.2018

[TN797428] File format reference for Word 2013, PowerPoint 2013, and Excel 2013

Microsoft TechNet, https://technet.microsoft.com/de-de/library/dd797428.aspx, zuletzt abgerufen am 06.09.2018

[TN857087] Plan Protected View Settings for Office 2013

Microsoft TechNet, https://technet.microsoft.com/en-us/library/ee857087.aspx, zuletzt abgerufen am 06.09.2018

[XMLDSIG] XML Signature Syntax and Processing

W3C Recommendation, Version 1.1, April 2013, https://www.w3.org/TR/xmldsig-core/, zuletzt abgerufen am 06.09.2018

APP.2: Verzeichnisdienste

Umsetzungshinweise zum Baustein APP.2.2 Active Directory

1 Beschreibung

1.1 Einleitung

Das Active Directory ist der zentrale Datenspeicher für sämtliche Verwaltungsdaten einer Domäne auf Basis der Serverbetriebssysteme Windows Server seit Version Windows 2000 Server. Abstrakt gesehen, bildet das Active Directory eine hierarchisch und baumartig organisierte objektbasierte Datenbank. Es ist an den Verzeichnisdienst-Standard X.500 angelehnt, von dem es die interne Struktur und den internen Aufbau entliehen hat. Es ist jedoch kein X.500 kompatibler Verzeichnisdienst. Active Directory wird häufig als "AD" oder "ADS" (*Active Directory Services)* abgekürzt.

1.2 Lebenszyklus

Für den erfolgreichen Aufbau und Betrieb eines sicheren Active Directory sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Installation bis zum Betrieb. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Planung und Konzeption

Als Einstieg empfiehlt es sich bei nicht bereits ausreichender Fachkenntnis, zunächst die Maßnahme APP.2.2.A4 Schulung zur Active Directory-Verwaltung zu betrachten, die einen Überblick über die Aufbau und Begrifflichkeiten eines Active Directory bietet.

Vor der eigentlichen Einrichtung des Active Directory ist im Vorfeld die Organisationsstruktur der Institution zu ermitteln, um aus dieser eine möglichst optimale Konfiguration für das Active Directory ableiten zu können. Die Maßnahme APP.2.2.A1 Planung des Active Directory erläutert die Vorgehensweise in der Planungsphase und das Domänenkonzept des Active Directory.

APP.2.2.A2 Planung der Active Directory-Administration beschäftigt sich mit der Basisstruktur zur Verwaltung einer Domäne und vermittelt die Aufgaben und Anwendungen der einzelnen administrativen Rollen. Des Weiteren wird hier der organisatorische Aufbau und die Rechteanpassung von administrativen Benutzerkonten eines Active Directory erläutert.

Die Maßnahme APP.2.2.A3 Planung der Gruppenrichtlinien unter Windows befasst sich mit den Gruppenrichtlinien für Windows Betriebssysteme, die auch mittels Active Directory verwaltet werden können.

Beschaffung

Bezüglich der Beschaffung sind keine gesonderten Anforderungen zu erfüllen, die über den Baustein APP.2.1 Allgemeiner Verzeichnisdienst hinausgehen. Es ist lediglich zu beachten, dass bestimmte Sicherheitsfunktionen nur durch neuere Versionen von AD und damit durch Einsatz neuerer Versionen von Windows Server ermöglichst werden, was Beschaffungsentscheidungen beeinflussen kann (siehe APP.2.2.A1 Planung des Active Directory).

Umsetzung

Um einen einheitlichen Sicherheitsstandard zu erhalten, ist die Maßnahme APP.2.2.A7 Umsetzung sicherer Verwaltungsmethoden für Active Directory zu beachten. Des Weiteren sind die für die Administration des Verzeichnisdienstes zuständigen Personen auf Basis APP.2.2.A4 Schulung zur Active Directory-Verwaltung mit den ihnen zugeteilten Aufgabenbereichen vertraut zu machen.

Aufgrund ihrer für die gesamte Netzumgebung zentralen Bedeutung sind die Domänencontroller einer Institution ausreichend zu härten (siehe APP.2.2.A5 Härtung des Active Directory). Dies umfasst insbesondere auch die Einrichtung des sicheren Kanals zwischen DCs, Servern und Clients (APP.2.2.A8 Konfiguration des sicheren Kanals unter Windows) und die weiteren Anforderungen aus APP.2.2.A9 Schutz der Authentisierung beim Einsatz von Active Directory.

Um den Integritätsschutz einer produktiv eingesetzten Active Directory-Umgebung durch die Sicherung der DNS -Komponenten gewährleisten zu können, ist die Maßnahme APP.2.2.A10 Sicherer Einsatz von DNS für Active Directory zu berücksichtigen.

Betrieb

Neben dem zugrundeliegenden Betriebssystem ist auch das Active Directory selbst sorgfältig zu administrieren (siehe APP.2.2.A6 Aufrechterhaltung der Betriebssicherheit von Active Directory), um sicherzustellen, dass die relevanten Systeme des Informationsverbundes auf einem aktuellen Sicherheitsstand gehalten werden.

Um rechtzeitig bei aufkommenden Problemen reagieren zu können, sollte die entsprechende Maßnahme APP.2.2.A11 Überwachung der Active Directory-Infrastruktur berücksichtigt werden. Diese befasst sich nicht nur mit den Rückmeldungen bei der Überschreitung definierter Schwellenwerte, sondern auch mit der Protokollierung durchgeführter Systemänderungen.

Aussonderung

Bezüglich der Aussonderung sind keine gesonderten Anforderungen zu beachten, die über den Baustein APP.2.1 Allgemeiner Verzeichnisdienst hinausgehen.

Notfallvorsorge

Aspekte der Notfallplanung für Active Directory werden in der Maßnahme APP.2.2.A12 Datensicherung für Domänencontroller thematisiert.

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Active Directory" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

APP.2.2.M1 Planung des Active Directory [Fachverantwortliche]

Eine grundlegende Voraussetzung für den sicheren Einsatz des Active Directory ist eine angemessene Planung im Vorfeld. Die Planung für ein Active Directory kann dabei in mehreren Schritten erfolgen. Es sollte zunächst ein Grobkonzept für die Struktur der Domäne erstellt und darauf aufbauend die einzelnen Teilaspekte konkretisiert werden. Die Planung betrifft dabei nicht nur Aspekte, die klassischerweise mit dem Begriff Sicherheit verknüpft werden, sondern auch normale betriebliche Aspekte, die Anforderungen im Bereich der Sicherheit nach sich ziehen können. Hinweise zum Aufbau und zur prinzipiellen Struktur eines Active Directory bietet die Maßnahme APP.2.2.M4 Schulung zur Active Directory-Verwaltung.

Im Rahmen der Active Directory Planung sind folgende Aspekte zu berücksichtigen:

- Welche Version des AD ("Domain Functional Level) benötigt wird, um die benötigten Sicherheitsfunktionen einrichten zu können.
- Welche Active Directory-Struktur im Sinne der Aufteilung in Domänen und welche Anordnung der Domänen in Bäume (Trees) und Wälder (Forests) soll gewählt werden?
- Welche Benutzer und Rechner sollen in welchen Domänen zusammengefasst werden?

Für jede Domäne muss entschieden werden,

- welche OU-Objekte existieren sollen, wie diese hierarchisch angeordnet werden und welche Objekte diese jeweils aufnehmen sollen,
- welche Sicherheitsgruppen benötigt werden und wie diese in OUs zusammengefasst werden,
- welches administrative Modell umgesetzt wird (zentrale/dezentrale Verwaltung),
- ob und an wen administrative Aufgaben delegiert werden sollen,
- welche Sicherheitseinstellungen für verschiedene Typen von Rechnern und Benutzergruppen gelten sollen,
- welche Einstellungen bei den Gruppenrichtlinien benötigt werden und nach welchem Konzept die Gruppenrichtlinien verteilt werden (siehe Planung der Gruppenrichtlinien).
- welche Vertrauensstellungen von Windows-Server automatisch generiert werden und welche zusätzlichen Vertrauensstellungen (z. B. zu NT-Domänen oder externen Kerberos-Realms) eingerichtet werden müssen,
- auf welche Active Directory-Informationen über die verschiedenen Active Directory-Schnittstellen (z. B. ADSI , LDAP) von wem zugegriffen werden dürfen und
- welche Active Directory-Objekte in den so genannten Global Catalog übernommen werden sollen, auf den in einem Forest global zugegriffen werden kann.

Generell muss die geplante Active Directory-Struktur geeignet, d. h. auch für fachkundige Dritte mit kurzer Einarbeitungszeit verständlich, dokumentiert werden. Dies trägt maßgeblich zur Stabilität, konsistenten Administration und damit zur Systemsicherheit bei. Es empfiehlt sich insbesondere festzuhalten, welche Schemaänderungen durchgeführt werden. Dabei sollten auch die Gründe für die Änderung dokumentiert sein.

Sicherheitsfunktionen von AD nach Betriebssystem bzw. Domain Functional Level

Jede neue Generation des Betriebssystems Windows Server bringt zusätzliche Sicherheitsfunktionen und -erweiterungen auch in Bezug auf AD mit. Außerdem werden in der Regel die Standardeinstellungen immer sicherer gesetzt. Einige davon sind verwendbar, sobald das neue System installiert ist, andere erst, wenn das Domänen-/Wald-Functional-Level angehoben wurde.

Es sollte immer ein möglichst hohes Domain Functional Level betrieben werden. Mindestens sollte dieses so hoch sein, dass alle Sicherheitsfunktionen angeboten werden können, die zur Gewährleistung des notwendigen Schutzbedarfs benötigt werden. Die Entscheidung für ein Domain Functional muss begründet getroffen und dokumentiert werden und sollte regelmäßig überprüft werden.

Die wichtigsten neuen Sicherheitsfunktionen bzw. Erweiterungen von solchen mit den letzten Windows-Server-Versionen bis 2012 R2 waren folgende:

Windows Server 2008 R2 Domain Functional Level:

- Unterstützung für Kerberos AES-VerschlüsselungDadurch kann die Unterstützung von RC4 HMAC aus Kerberos entfernt werden. Außerdem unterstützen Windows 7 und Windows Server 2008 R2 kein DES bei Kerberos mehr.
- Verwaltete Dienstkonten (Managed Service Accounts)AD verwaltet die Passwörter dieser Dienstkonten selbst
- Authentication Mechanism Assurance
  Nutzer erhalten zusätzliche Gruppenmitgliedschaften erst nach Authentifikation via Smartcard

Windows Server 2012 Domain Functional Level:

- Verwaltete Dienstkontengruppen (Group Managed Service Accounts)AD verwaltet die Passwörter dieser Dienstkontengruppen selbst
- Compound Authentication und Kerberos FAST (Kerberos Armoring)
  - Kombiniert Nutzer- und Geräteauthentifizierung
  - Schützt Kerberos AS- und TGT-Anfragen.

Windows Server 2012 R2 Domain Functional Level:

- Authentifizierungsrichtlinien und Silos
  Schützt privilegierte Konten durch Beschränkung, wo sie sich anmelden können
- Sicherheitsgruppe Geschützte Benutzer (Protected Users)
  - Primärer DC (PDC) muss Windows 2012 R2 sein, um die Gruppe zu erhalten
  - Protected Users Host Protection (mit Windows 8.1 und 2012 R2) verhindert folgendes auf Systemen:
    - Authentifikation per NTLM, Digest Authentication oder CredSSP
    - Caching von Credentials
    - DES und RC4 bei Kerberos Pre-Authentifikation
    - Delegation von Konten
  - Protected Users Domain Enforcement verhindert folgendes bei Nutzern:
    - NTLM-Authentifikation.
    - DES und RC4 bei Kerberos Pre-Authentifikation
    - Das Delegiert-Werden
    - Eine Erneuerung von Kerberos TGTs über die anfängliche vier-Stunden-Frist hinaus (danach muss neu authentifiziert werden)

Dokumentation

Für jedes Active Directory-Objekt sollte dokumentiert sein:

- Name und Position im Active Directory-Baum (z. B. "Standort Berlin", Vater-Objekt: OU "Filialen-Deutschland")
- welchem Zweck das Objekt dient (z. B. Gruppe der Benutzer mit RAS-Zugang auf RAS-Server 1)
- welche administrativen Zugriffsrechte für das Objekt und dessen Attribute vergeben werden sollen (z. B. vollständig verwaltet von "Admin1")
- wie die Vererbung von Active Directory-Rechten konfiguriert werden soll, z. B. Blockieren der Rechtevererbung (siehe auch Planung der Active Directory-Administration, Schulung zur Active Directory-Verwaltung)
- welche Gruppenrichtlinienobjekte auf dieses Objekt wirken (siehe Planung der Gruppenrichtlinien)

Der Planung der Active Directory-Administration und des benutzten administrativen Modells kommt eine wichtige Aufgabe zu. Empfehlungen dazu finden sich zusammengefasst in Maßnahme Planung der Active Directory-Administration.

Die sicherheitsrelevanten Kernaspekte der Active Directory-Planung sind zusammengefasst:

- Domänen begrenzen die administrative Macht von Administratoren. Administratoren können daher nur innerhalb einer Domäne verwaltend tätig werden, sodass ihre Verwaltungsbefugnis standardmäßig nicht über die Domänengrenze reicht. Dies gilt insbesondere im Verbund mit mehreren Domänen (Baum, Wald), so dass die oft geäußerten Bedenken, dass durch das standardmäßig transitive Vertrauensmodell auch administrative Berechtigungen über Domänengrenzen hinweg möglich sind, für normale Administratorenkonten ausgeräumt werden können (siehe jedoch Organisations-Admins unten).
- Domänenübergreifende Zugriffe setzen voraus, dass in der Ziel-Domäne explizit Zugriffsberechtigungen für den Zugreifenden aus einer anderen Domäne eingerichtet werden. Standardmäßig sind daher keine domänenübergreifenden Zugriffe möglich.
- Dies bedeutet, dass in einem Baum oder Wald ein Administrator einer Domäne "A" nur dann administrativ auf eine beliebige andere Domäne "B" zugreifen kann, falls der Domänenadministrator von "B" dem Administrator der Domäne "A" explizit Berechtigungen dazu einräumt (siehe jedoch Organisations-Admins).
- Die Mitglieder der Gruppe Organisations-Admins genießen einen Sonderstatus, da sie im gesamten Forest Administratorrechte auf dem Active Directory besitzen. Insbesondere werden gesetzte Zugriffsrechte auf Active Directory-Objekte bei Zugriffen von Organisations-Admins ignoriert. Die Mitgliedschaft in der Gruppe der Organisations-Admins muss daher restriktiv vergeben und strikt kontrolliert werden. Es ist zu beachten, dass ein Organisations-Admin benötigt wird, um beispielsweise eine Subdomäne anzulegen.
- Administrative Delegation wird durch die Vergabe von Zugriffsrechten auf Active Directory-Objekte und deren Attribute erreicht. Die Verteilung der Zugriffsrechte muss gemäß dem administrativen Modell erfolgen. Durch die Mechanismen für Zugriffsrechte im Active Directory (Vererbung, Kontrolle der Vererbung, Wirkungsbereich von Zugriffseinstellungen) können sehr komplexe Berechtigungsstrukturen aufgebaut werden. Diese können sehr schnell unübersichtlich und nicht mehr administrierbar werden, so dass sich durch Fehlkonfigurationen im Active Directory Sicherheitslücken ergeben können. Eine möglichst einfache Berechtigungsstruktur ist daher vorzuziehen.
  Um Delegation sicher zu planen und einzusetzen wird empfohlen, zunächst die tatsächlichen Anforderungen in Form real benötigter minimaler Rechte zu ermitteln, zu dokumentieren (z. B. zunächst sprachlich-textuell) und diese anschließend in technische Zugriffsrechte zu übersetzen.
- Schemaänderungen sind kritische Operationen und dürfen nur von autorisierten Administratoren nach sorgfältiger Planung durchgeführt werden.

Abschließend sei darauf hingewiesen, dass Fehler in der Active Directory-Planung und den zugrunde liegenden Konzepten nach erfolgter Installation nur mit beträchtlichem Aufwand zu berichtigen sind. Nachträgliche Veränderungen in der Active Directory-Struktur, wie z. B. die Anordnung von Domänen in Bäume und Forests, ziehen unter Umständen das komplette Neuaufsetzen von Domänen nach sich.

Active Directory Federation Services (ADFS)

Active Directory Federation Services (ADFS oder auch AD FS abgekürzt) ist eine weitere Softwarekomponente von Microsoft und Teil der ADS, mittels derer sogenannte "Federation" oder "Federated Identities" (föderierte Identitäten) abgebildet werden können. Dabei handelt es sich um Funktionen, die einen Single-Sign-On-Zugriff auf Systeme auch über Institutionsgrenzen hinweg ermöglichen. Seit Windows Server 2012 ist die Funktion als Rolle im System verfügbar und benötigt keine zusätzliche Installation mehr. Seit Windows Server 2012 ist eine Verwaltung per PowerShell möglich, seit 2012 R2 auch eine Integration mit OAuth 2.0.

In ADFS wird eine Vertrauensbeziehung zwischen zwei (oder mehr) Organisationen eingerichtet. Ein Federation-Server auf der einen Seite kann dann einen Nutzer mit Standardmitteln, z. B. am AD, identifizieren und stattet ihn daraufhin mit einem Token aus, das gewisse "Claims" (Zusicherungen) enthält. Diese kann der Nutzer vorzeigen, um Berechtigungen in der anderen Organisation zu erlangen.

ADFS gewinnt deutlich an Bedeutung, da es eine natürliche Eignung für die Integration mit Cloud-Diensten mitbringt. So kann es z. B. im Zusammenhang mit dem Microsoft-Dienst "Azure AD" genutzt werden. Eine Interaktion ist auch mit anderen WS-*- oder SAML 2.0-kompatiblen Federation-Diensten möglich.

Der Einsatz von Federation im allgemeinen und ADFS im besonderen ist zu begründen, gründlich zu planen und zu dokumentieren. Dies betrifft insbesondere die notwendigen Vertrauensbeziehungen. Diese sollten minimal gewählt und regelmäßig evaluiert werden. Die Risiken eines Missbrauchs von Rechten, die durch Authentisierung oder Autorisierung in einer anderen Organisation gewährt wurden, sind systematisch zu beschreiben, zu bewerten und geeignet zu behandeln.

Kommen Clouddienste zum Einsatz, so müssen zusätzlich die geeigneten Bausteine angewandt werden (insbesondere OPS.2.2 Cloud-Nutzung und OPS.3.2 Cloud Management).

APP.2.2.M2 Planung der Active Directory-Administration [Fachverantwortliche]

Das Active Directory besteht aus verschiedenen Objekten, die baumartig organisiert sind. Jedes Objekt besteht aus bestimmten Attributen, die die Objektinformationen speichern. Durch Objekte geschieht die Verwaltung eines Windows-Systems, die durch einen berechtigten Administrator erfolgen muss. Für alle Active Directory-Objekte können Berechtigungen vergeben werden, die den Zugriff auf die Objekte steuern. Damit kann festgelegt werden, welche Objekte von welchen Benutzern in einer bestimmten Art und Weise verändert werden können wie beispielsweise das Anlegen von Benutzern oder das Zurücksetzen von Benutzerpasswörtern.

Bei einer Standardinstallation besitzen nur Administratoren das Recht, Veränderungen an Objekten vorzunehmen und damit eine Domäne zu verwalten. Benutzer besitzen in der Regel maximal Leserecht.

Generell gilt unter Windows Server, dass an der Domänengrenze auch die administrative Macht der Administratoren der Domäne endet. Lediglich die Mitglieder der Gruppe Organisations-Admins besitzen in jeder Domäne eines Forests Vollzugriff auf alle AD-Objekte, und zwar unabhängig von den für diese Objekte eingestellten Zugriffsrechten. Standardmäßig sind dies die Mitglieder der Administratorengruppe der Forest-Root-Domain (FRD).

In großen Domänen empfiehlt sich die Delegation administrativer Aufgaben, sodass die administrative Last auf mehrere Administratoren verteilt ist oder auch, unter Umständen zusätzlich, eine Rollentrennung umgesetzt werden kann. Die Delegation administrativer Aufgaben erfolgt im Active Directory durch die Vergabe entsprechender Zugriffsrechte auf Active Directory-Objekte für die jeweiligen Adminstratorengruppen. Dabei erlaubt die Active Directory-Rechtestruktur eine feingranulare Vergabe von Rechten. Auf diese Weise kann z. B. einem Administrator erlaubt werden, Benutzerkonten anzulegen und Benutzerpasswörter zurückzusetzen, jedoch nicht Benutzerkonten zu löschen oder in andere Organizational Units (OU, Organisationseinheiten) zu verschieben. Um die Vergabe gleichförmiger Rechte innerhalb eines kompletten Teilbaums zu vereinfachen, besteht zusätzlich die Möglichkeit, Rechte eines Objektes an Objekte im Unterbaum zu vererben. Da die Übernahme von vererbten Rechten durch bestimmte Objekte im Unterbaum unter Umständen nicht gewünscht ist, lässt sich die Übernahme für Objekte auch blockieren, so dass sich hier durchaus komplexe Szenarien für die Verteilung von Berechtigungen ergeben können (siehe auch APP.2.2.A4 Schulung zur Active Directory-Verwaltung).

Aus Sicherheitssicht ergeben sich folgende Aspekte, die bei der Planung der Active Directory-Administration zu berücksichtigen sind:

- Wird Delegation eingesetzt, so sollten nur die unbedingt notwendigen Rechte vergeben werden, die zur Ausübung der delegierten administrativen Tätigkeiten erforderlich sind.
- Das Delegationsmodell und die daraus resultierenden Rechtezuordnungen müssen dokumentiert werden.
- Die administrativen Tätigkeiten sollten so delegiert werden, dass sich möglichst keine Überschneidungen ergeben. Ansonsten können durch zwei Administratoren sich widersprechende Veränderungen durchgeführt werden. Dies führt dann zu Replikationskonflikten, die von Windows-Server automatisch aufgelöst werden, sodass sich eine der Änderungen auf jeden Fall durchsetzt. Es gibt jedoch für diesen Fall keine Warnungen. Es empfiehlt sich daher, das Administrationsmodell so zu entwerfen, dass möglichst überschneidungsfreie Zuständigkeiten existieren. Auf diese Weise kann die Gefahr von Replikationskonflikten verringert werden. Sind Replikationskonflikte zu erwarten oder bereits aufgetreten, so sollte in regelmäßigen Abständen oder nach wichtigen Änderungen eine manuelle Überprüfung erfolgen, ob sich immer die korrekten Werte durchgesetzt haben. Ob das Führen einer Evidenzdatenbank mit den Active-Directory-Soll-Daten unter Umständen organisatorisch sinnvoll ist, muss im Einzelfall entschieden werden.
- Wird die Verwaltung des Active Directory delegiert, so wird dies durch die Vergabe von entsprechenden Zugriffsrechten innerhalb des Active Directory erreicht. Dabei wird in der Regel der Vererbungsmechanismus eingesetzt, um Berechtigungen auf Objekte in Teilbäumen zu verwalten. Komplexe Szenarien mit Delegation und damit Rechtevererbung sollten jedoch unbedingt vermieden werden, da sonst leicht Sicherheitslücken entstehen können. Beispielsweise kann der Fall eintreten, dass ein Benutzer zu wenig oder zu viele Rechte hat.
- Es muss ein Konzept für die Mitgliedschaft in den verschiedenen administrativen Gruppen entworfen werden. Dabei sind vor allem die Bedingungen und Verfahren zu definieren, die festlegen, ob, wann und wie lange ein Benutzer oder eine Benutzergruppe in eine administrative Gruppe aufgenommen wird. Es muss insbesondere dafür Sorge getragen werden, die Mitgliedschaft in der Gruppe der Organisations-Admins restriktiv zu handhaben und zu kontrollieren. Falls es der organisatorische Ablauf zulässt, kann erwogen werden, alle Mitglieder in dieser Gruppe nach Aufbau der Domänenstruktur zu entfernen und nur bei Bedarf und unter Einhaltung des Vier-Augen-Prinzips entsprechende Mitglieder hinzuzufügen. Es muss jedoch berücksichtigt werden, dass ein Mitglied der Gruppe der Organisations-Admins immer dann benötigt wird, wenn eine neue Domäne im Forest angelegt werden soll.
- Die Administratoren sind über die Active Directory-Struktur und die organisatorischen Abläufe im Rahmen ihrer administrativen Tätigkeit zu informieren und entsprechend zu schulen, um zu verhindern, dass nicht-konforme Änderungen zu Sicherheitslücken führen. Beispielsweise kann es erforderlich sein, beim Anlegen eines neuen Benutzers diesen in entsprechende Sicherheitsgruppen aufzunehmen oder sogar zusätzlich eine neue Sicherheitsgruppe mit einem speziellen Namen anzulegen. Wird dies vergessen, so erhalten Benutzer unter Umständen fehlerhafte Berechtigungen.
- Für große Domänen sollte darüber nachgedacht werden, deren Verwaltung mit geeigneten Werkzeugen zu unterstützen. Es gibt verschiedene kommerzielle und auch frei verfügbare Werkzeuge, die die Active Directory-Verwaltung erleichtern. Es sollte überlegt werden, diese einzusetzen. Werden solche Werkzeuge verwendet, so muss sichergestellt werden, dass die Active Directory-Verwaltung ausschließlich über diese Werkzeuge erfolgt.

Rollenbasiertes Berechtigungskonzept

Es sollte ein rollenbasiertes Berechtigungskonzept implementiert werden, das eine granulare Kontrolle über die einzelnen Berechtigungen eines jeden Accounts gewährt.

Sämtliche Berechtigungen sollten rollenbasiert vergeben werden. In der Praxis bedeutet dies, dass Sicherheitsgruppen erstellt werden, an die Berechtigungen geknüpft sind. Anschließend werden Gruppen erstellt, die Rollen repräsentieren und mit den notwendigen zuvor erstellen Sicherheitsgruppen verknüpft werden. Schließlich werden Benutzerkonten der Gruppen zugewiesen, die Ihrer Rolle entsprechen. Über ein Enterprise Identity Management-Lösung kann zudem insbesondere in großen Institutionen sichergestellt werden, dass die Rechte aller Anwender definierten Vorgaben entsprechen.

Trennung der Verwaltung von Diensten und Daten eines Active Directory

Die administrativen Tätigkeiten für Windows-Server-Betriebssysteme können grundsätzlich in die zwei Rollen "Diensteverwaltung" und "Datenverwaltung" mit unterschiedlichen Verantwortungsbereichen unterteilt werden.

Unter der "Diensteverwaltung" wird die Betreuung des Active-Directory-Dienstes selbst verstanden. Diensteadministratoren verwalten die Domänencontroller, z. B. Einspielen von Updates auf Betriebssystemebene, und die Konfiguration des Active Directory, beispielsweise verzeichnisweite Einstellungen, wie Vertrauensstellungen oder Replikationsarchitektur.

Die Verwaltung der Daten im Active Directory bzw. auf den Mitgliedsrechnern der Active-Directory-Gesamtstruktur sollte von den Datenadministratoren durchgeführt werden. Dabei sollten die Datenadministratoren keine Veränderungen am Active-Directory-Dienst selbst, z. B. Änderungen an der Verzeichnisdienst-Replikation, durchführen dürfen. Mittels Zugriffskontrolllisten (Access Control Lists, ACLs) sollten die Berechtigungen soweit möglich auf einzelne Teilbereiche eingeschränkt werden.

Da Dienste-Administratoren für die Diensteverwaltung weitreichende Berechtigungen benötigen, sollten sie grundsätzlich auch administrative Tätigkeiten in Bezug auf die Datenverwaltung durchführen können. Umgekehrt sollten die Datenadministratoren jedoch nicht in der Lage sein, die Konfiguration des Active Directory zu ändern.

Um Missbrauch der administrativen Konten vorzubeugen, müssen die Benutzerkonten der oben genannten Rollen entsprechend abgesichert werden. Die hierzu erforderlichen Konfigurationen am Active Directory selbst sind in der Maßnahme APP.2.2.A7 Umsetzung sicherer Verwaltungsmethoden für Active Directory aufgeführt.

APP.2.2.M3 Planung der Gruppenrichtlinien unter Windows

Seit Windows 2000 steht zur Konfiguration ein leistungsfähiger Mechanismus der so genannten Gruppenrichtlinien zur Verfügung. Gruppenrichtlinien dienen im Active Directory dazu, einen Satz von Konfigurationseinstellungen, zu denen insbesondere auch Sicherheitseinstellungen gehören, auf eine Gruppe von Objekten anzuwenden. Durch ein so genanntes Gruppenrichtlinienobjekt (englisch Group Policy Object, GPO) wird ein vorgegebener Satz von Konfigurationsparametern zusammengefasst. Für jeden Parameter kann ein konkreter Wert angegeben werden, der unter Umständen nur aus einem beschränkten Wertebereich stammt. Generell kann der Wert auch auf "nicht definiert" gesetzt werden, sodass dann automatisch die Windows-Standardeinstellungen für diese Parameter gelten.

Die Parameter innerhalb eines Gruppenrichtlinienobjektes sind baumartig thematisch zusammengefasst. Dabei ergibt sich eine generelle Zweiteilung auf oberster Ebene in Einstellungen für Rechner sowie für Benutzer. Aus Sicherheitssicht sind insbesondere die Einstellungen interessant, die sich unterhalb der folgenden Pfade finden:

- Rechnereinstellungen\WindowsEinstellungen\Sicherheitseinstellungen
- Rechnereinstellungen\Administrative Einstellungen\Windows Komponenten\Windows Installer
- Rechnereinstellungen\Administrative Vorlagen\System\Gruppenrichtlinien
- Benutzereinstellungen\Administrative Vorlagen\Windows Komponenten\Microsoft Management Konsole
- Benutzereinstellungen\Administrative Einstellungen\Windows Komponenten\Windows Installer

Die aktuellen Windows-Server-Systeme berechnen generell für jeden an einer Domäne angemeldeten Rechner und für jeden angemeldeten Benutzer die jeweils gültigen Einstellungen für jeden Gruppenrichtlinienparameter. Diese Berechnung ist nötig, da die Vorgaben für die Parametereinstellungen durch unterschiedliche Gruppenrichtlinienobjekte definiert sein können, die sich gegenseitig überlagern können. Folgende Gruppenrichtlinienobjekte können definiert werden:

- Jeder Rechner besitzt ein lokal definiertes Gruppenrichtlinienobjekt. Dies erlaubt die Definition von Parametereinstellungen lokal auf dem Rechner, z. B. wenn keine Netzverbindung besteht.
- Gruppenrichtlinienobjekte können über Windows-Server-Standorte (Sites) definiert werden. Damit können Einstellungen standortspezifisch adaptiert werden.
- Innerhalb der Active Directory-Struktur können Gruppenrichtlinienobjekte für das Domänenobjekt definiert werden, sodass damit Parametereinstellungen für Rechner und Benutzer innerhalb der gesamten Domäne gesteuert werden können.
- Auf jedem OU-Objekt können Gruppenrichtlinien definiert werden, deren Einstellungen dann auf alle Rechner und Benutzer unterhalb dieses OU-Objektes wirken.

Für die Berechnung der jeweils für einen konkreten Rechner oder Benutzer geltenden Parametereinstellungen wird das folgende Berechnungs- bzw. Überdeckungsschema (Lokal <- Standort <- Domäne <- Organisationseinheit, LSDO) angewandt: Zunächst werden die lokalen Einstellungen berücksichtigt (L, Lokal). Dann werden diese Einstellungen durch die Einstellungen des Gruppenrichtlinienobjektes, das auf dem zugehörigen Standort definiert ist, überdeckt (S, Standort). Danach erfolgt die Überdeckung durch die auf dem relevanten Domänenobjekt definierten Gruppenrichtlinienobjekte (D, Domäne). Schließlich werden die Gruppenrichtlinienobjekte der OU-Objekte in der Reihenfolge angewandt, wie sie auf dem Weg vom Domänenobjekt zu dem OU-Objekt, das den jeweiligen Rechner oder Benutzer enthält, definiert sind (O, Organisationseinheit).

Die Überdeckung kann durch die Optionen blockieren bzw. erzwingen beeinflusst werden. Stehen die Einstellungen blockieren und erzwingen im Konflikt, so wird die Einstellung erzwingen durchgesetzt. Zusätzlich ist es auf OU-Ebene möglich, mehrere Gruppenrichtlinienobjekte für ein OU-Objekt zu definieren. Dabei erfolgt die Überdeckung gemäß der angegebenen Reihenfolge. Es ist dabei außerdem möglich, jedes einzelne Gruppenrichtlinienobjekt für ein OU-Objekt zu aktivieren oder zu deaktivieren.

Gruppenrichtlinienobjekte können im Active Directory nur auf OU-Objekten definiert werden, nicht jedoch auf einzelnen Rechnern oder Benutzerobjekten. Das lokal definierte Gruppenrichtlinienobjekt wird nicht im Active Directory gespeichert. Soll ein Gruppenrichtlinienobjekt, das auf einem OU-Objekt definiert ist, das Rechnerobjekte zusammenfasst, nicht auf alle enthaltenen Rechnerobjekte wirken, so besteht die Möglichkeit, durch die Vergabe von Zugriffsrechten auf das Gruppenrichtlinienobjekt die Anwendung auf ein konkretes Rechnerobjekt zu unterbinden. Hierzu ist diesem Rechnerobjekt das Zugriffsrecht Anwenden auf das Gruppenrichtlinienobjekt zu entziehen.

Die bisher benutzte Darstellung der Definition von Gruppenrichtlinienobjekten auf OU-Objekten war jedoch vereinfacht: Gruppenrichtlinienobjekte werden separat im Active Directory gespeichert und bilden einen Pool von Objekten. Jedes definierte Gruppenrichtlinienobjekt kann nun einem oder auch mehreren OU-Objekten assoziiert werden. Man spricht dann von einem Link. Durch das Kennzeichnen eines Links als aktiviert oder deaktiviert wird das jeweilige Gruppenrichtlinienobjekt bei der Berechnung für das OU-Objekt herangezogen oder nicht (siehe oben). Für jedes Gruppenrichtlinienobjekt kann über den Eigenschaftsdialog festgestellt werden, mit welchen OU-Objekten ein Link besteht, d. h. auf welche Objekte sie potentiell wirken.

Aus Sicherheitssicht sind bei der Planung und im Umgang mit Gruppenrichtlinienobjekten folgende Aspekte zu berücksichtigen:

- Das Gruppenrichtlinienkonzept muss so einfach wie möglich gehalten werden. Komplexe Strukturen aus Mehrfachüberdeckungen sind zu vermeiden. Insbesondere sollte auf die Möglichkeit der Vergabe von Zugriffsrechten auf Gruppenrichtlinienobjekte nur in Ausnahmefällen zurückgegriffen werden. Generell muss das Gruppenrichtlinienkonzept so dokumentiert sein, dass Ausnahmeregelungen einfach zu erkennen sind.
- Das Gruppenrichtlinienkonzept und die OU-Objektstruktur beeinflussen sich gegenseitig wesentlich, da Gruppenrichtlinienobjekte im Active Directory nur auf OU-Objekte angewandt werden können und nicht auf Rechner- oder Benutzerobjekte. Beim Aufbau der OU-Gruppierungen ist daher darauf zu achten, dass nur Objekte, die mit gleichen GPO-Einstellungen versehen werden sollen, in einem OU-Objekt oder untergeordneten OU-Objekten zusammengefasst werden.
- Durch die Rechteberechnung ist es möglich, die Verwaltung der Parametereinstellungen auf unterschiedliche "Orte" (Lokal, Standort, Domänen-Objekt, OU-Objekte) zu verteilen. Es muss daher für jeden Parameter entschieden werden, wo er definiert wird. Es ist dabei zu beachten, dass einige Parameter nur dann wirksam werden, wenn sie an bestimmten "Orten" definiert werden. So konnten z. B. die Passworteinstellungen ursprünglich nur auf Domänen-Objekten definiert werden. Mit Windows Server 2008 wurden feingranulare Passwortrichtlinien eingeführt, die es ermöglichen, verschiedene Passwortricht- und Sperrrichtlinien für unterschiedliche Nutzergruppen innerhalb einer Domäne zu definieren
- Gruppenrichtlinienobjekte müssen vor unberechtigter Veränderung geschützt werden. Dazu müssen einerseits entsprechende Berechtigungen im Active Directory vergeben werden (siehe auch Planung der Active Directory-Administration , Schulung zur Active Directory-Verwaltung) und andererseits kann der Gebrauch von entsprechenden Verwaltungswerkzeugen, wie z. B. MMC-Gruppenrichtlinien-Snap-In oder Registrierungseditoren, für Benutzer unterbunden werden.
- Insbesondere für die sicherheitsrelevanten Parameter innerhalb eines Gruppenrichtlinienobjektes sind die Einstellungen festzulegen. Neben den oben angegebenen Einstellungen können je nach Anwendungsszenario auch weitere Parameter sicherheitsrelevant sein. Dazu zählen z. B. Internet-Explorer-Einstellungen.

Die Einstellungen der verschiedenen Gruppenrichtlinienobjekte müssen sich dabei generell an den Sicherheitsrichtlinien des Unternehmens bzw. der Behörde orientieren und diese umsetzen.

Sicherheitseinstellungen für Gruppenrichtlinien

Im Folgenden werden Vorgaben für die Sicherheitseinstellungen aufgezeigt, die als Ausgangsbasis für die Sicherheitseinstellungen innerhalb einer Gruppenrichtlinie dienen können. Die angegebenen Werte müssen auf jeden Fall an die lokalen Bedingungen angepasst werden. Im Rahmen des Gruppenrichtlinienkonzeptes sind die einzelnen Werte zudem auf unterschiedliche Gruppenrichtlinienobjekte zu verteilen und jeweils an den Verwendungszweck anzupassen (z. B. Group Policy Objects für Server, Group Policy Objects für Arbeitsplatzrechner). Dadurch können für einzelne Einträge auch jeweils unterschiedliche Werte zustande kommen.

Kennwortrichtlinie

- Kennwortchronik erzwingen: 6 Gespeicherte Kennwörter
- Kennwörter müssen den Komplexitätsanforderungen entsprechen: Aktiviert
- Kennwörtern für alle Domänenbenutzer mit umkehrbarer Verschlüsselung speichern: Deaktiviert
- Maximales Kennwortalter: 90 Tage
- Minimale Kennwortlänge: 6 Zeichen
- Minimales Kennwortalter: 1 Tag

Kontosperrungsrichtlinien

- Kontensperrungsschwelle: 3 Ungültige Anmeldeversuche
- Kontosperrdauer: 0 (Hinweis: Konto ist gesperrt, bis Administrator Sperrung aufhebt)
- Kontosperrungszähler zurücksetzen nach: 30 Minuten

Kerberos-Richtlinie

- Benutzeranmeldeeinschränkungen erzwingen: Aktiviert
- Max. Gültigkeitsdauer des Benutzertickets: 8 Stunden
- Max. Gültigkeitsdauer des Diensttickets: 60 Minuten
- Max. Toleranz für die Synchronisation des Computertakts: 5 Minuten
- Max. Zeitraum, in dem ein Benutzerticket erneuert werden kann: 1 Tag

Überwachungsrichtlinie

- Active Directory-Zugriff überwachen: Erfolgreich, Fehlgeschlagen
- Anmeldeereignisse überwachen: Erfolgreich, Fehlgeschlagen
- Anmeldeversuche überwachen: Erfolgreich, Fehlgeschlagen
  Kontenverwaltung überwachen: Erfolgreich, Fehlgeschlagen
- Objektzugriffsversuche überwachen: Fehlgeschlagen
- Prozessverfolgung überwachen: Keine Überwachung
- Rechteverwendung überwachen: Fehlgeschlagen
- Richtlinienänderungen überwachen: Erfolgreich, Fehlgeschlagen
- Systemereignisse überwachen: Erfolgreich, Fehlgeschlagen

Zuweisen von Benutzerrechten

- Als Dienst anmelden: Definiert, aber leer
- Ändern der Systemzeit: Administratoren
- Anheben der Zeitplanungspriorität: Administratoren
- Anheben von Quoten: Administratoren
- Anmelden als Stapelverarbeitungsauftrag: Definiert, aber leer
- Anmeldung als Batchauftrag verweigern: Nicht definiert
- Anmeldung als Dienst verweigern: Nicht definiert
- Auf diesen Computer vom Netzwerk aus zugreifen: Jeder, Administratoren, Authentisierte Benutzer, Sicherungs-Operatoren
- Auslassen der durchsuchenden Überprüfung: Jeder
- Debuggen von Programmen: Nicht definiert
- Einsetzen als Teil des Betriebssystems: Definiert, aber leer
- Entfernen des Computers von der Dockingstation: Administratoren
- Ermöglichen, dass Computer- und Benutzerkonten für Delegierungszwecke vertraut wird: Administratoren
- Ersetzen eines Tokens auf Prozessebene: Definiert, aber leer
- Erstellen einer Auslagerungsdatei: Administratoren
- Erstellen eines Profils der Systemleistung Administratoren
- Erstellen eines Profils für einen Einzelprozess: Administratoren
- Erstellen eines Tokenobjekts: Definiert, aber leer
- Erstellen von dauerhaft freigegebenen Objekten: Definiert, aber leer
- Erzwingen des Herunterfahrens von einem Remotesystem aus: Administratoren
- Generieren von Sicherheitsüberwachungen: Definiert, aber leer
- Herunterfahren des Systems: Administratoren
- Hinzufügen von Arbeitsstationen zur Domäne: Definiert, aber leer
- Laden und Entfernen von Gerätetreibern: Administratoren
- Lokal anmelden: Administratoren, Sicherungs-Operatoren
- Lokale Anmeldung verweigern: Nicht definiert
- Sichern von Dateien und Verzeichnissen: Sicherungs-Operatoren
- Sperren von Seiten im Speicher: Definiert aber leer
- Synchronisieren von Verzeichnisdienstdaten: Definiert, aber leer
- Übernehmen des Besitzes von Dateien und Objekten: Administratoren
- Verändern der Firmwareumgebungsvariablen: Administratoren
- Verwalten von Überwachungs- und Sicherheitsprotokollen: Administratoren
- Wiederherstellen von Dateien und Verzeichnissen: Administratoren
- Zugriff vom Netzwerk auf diesen Computer verweigern: Nicht definiert

Sicherheitsoptionen

- Administrator umbenennen: Nicht definiert
- Anwender vor Ablauf des Kennworts zum Ändern des Kennworts auffordern: 7 Tage
- Anwendern das Installieren von Druckertreibern nicht erlauben: Aktiviert
- Anzahl zwischenzuspeichernder vorheriger Anmeldungen (für den Fall, dass der Domänencontroller nicht verfügbar ist): 0 Anmeldungen
- Auslagerungsdatei des virtuellen Arbeitsspeichers beim Herunterfahren des Systems löschen: Aktiviert
- Auswerfen von NTFS-Wechselmedien zulassen: Administratoren
- Benutzer automatisch abmelden, wenn die Anmeldezeit überschritten wird (lokal): Aktiviert
- Benutzer nach Ablauf der Anmeldezeit automatisch abmelden: Aktiviert
- Clientkommunikation digital signieren (immer): Deaktiviert
- Clientkommunikation digital signieren (wenn möglich): Aktiviert
- Die Verwendung des Sicherungs- und Wiederherstellungsrechts überprüfen: Deaktiviert
- Gastkonto umbenennen: Nicht definiert
- Herunterfahren des Systems ohne Anmeldung zulassen: Deaktiviert
- LAN Manager-Authentisierungsebene: Nur NTLMv2-Antworten senden\LM verweigern
- Leerlaufzeitspanne bis zur Trennung der Sitzung: 15 Minuten
- Letzten Benutzernamen nicht im Anmeldedialog anzeigen: Aktiviert
- Nachricht für Benutzer, die sich anmelden wollen: Nicht definiert
- Nachrichtentitel für Benutzer, die sich anmelden wollen: Nicht definiert
- Serverkommunikation digital signieren (immer): Deaktiviert
- Serverkommunikation digital signieren (wenn möglich): Aktiviert
- Serveroperatoren das Einrichten von geplanten Tasks erlauben (Nur für Domänencontroller): Nicht definiert
- Sicherer Kanal: Daten des sicheren Kanals digital signieren (wenn möglich): Aktiviert
- Sicherer Kanal: Daten des sicheren Kanals digital verschlüsseln (wenn möglich): Aktiviert
- Sicherer Kanal: Daten des sicheren Kanals digital verschlüsseln oder signieren (immer): Aktiviert(Hinweis: Es sei denn, veraltete Systeme sind damit nicht kompatibel.)
- Sicherer Kanal: Starker Sitzungsschlüssel erforderlich: Aktiviert(Hinweis: Es sei denn, veraltete Systeme sind damit nicht kompatibel.)
- Standardberechtigungen globaler Systemobjekte (z. B. symbolischer Verknüpfungen) verstärken: Aktiviert
- STRG+ALT+ENTF-Anforderung zur Anmeldung deaktivieren: Deaktiviert
  (Hinweis: D. h. STRG+ALT+ENTF ist erforderlich)
- System sofort herunterfahren, wenn Sicherheitsüberprüfungen nicht protokolliert werden können: Deaktiviert
- Systemwartung des Computerkontokennworts nicht gestatten: Deaktiviert
- Unverschlüsseltes Kennwort senden, um Verbindung mit SMB-Servern von Drittanbietern herzustellen: Deaktiviert
- Verhalten bei der Installation von nicht signierten Dateien (außer Treibern): Warnen, aber Installation zulassen
- Verhalten bei der Installation von nicht signierten Treibern: Warnen, aber Installation zulassen
- Verhalten beim Entfernen von Smartcards: Computer sperren
- Weitere Einschränkungen für anonyme Verbindungen: Kein Zugriff ohne explizite anonyme Berechtigung
- Wiederherstellungskonsole: Automatische administrative Anmeldungen zulassen: Deaktiviert
- Wiederherstellungskonsole: Kopieren von Disketten und Zugriff auf alle Laufwerke und alle Ordner zulassen: Deaktiviert
- Zugriff auf CD-ROM-Laufwerke auf lokal angemeldete Benutzer beschränken: Aktiviert
- Zugriff auf Diskettenlaufwerke auf lokal angemeldete Benutzer beschränken: Aktiviert
- Zugriff auf globale Systemobjekte prüfen: Deaktiviert

Ereignisprotokoll

- Anwendungsprotokoll aufbewahren für: Nicht definiert
- Aufbewahrungsmethode des Anwendungsprotokolls: Ereignisse bei Bedarf überschreiben
- Aufbewahrungsmethode des Sicherheitsprotokolls: Ereignisse bei Bedarf überschreiben (Hinweis: Im Hochsicherheitsbereich ist folgende Einstellung zu wählen: Ereignisse nicht überschreiben (Protokoll manuell aufräumen).)
- Aufbewahrungsmethode des Systemprotokolls: Ereignisse bei Bedarf überschreiben
- Gastkontozugriff auf Anwendungsprotokoll einschränken: Aktiviert
- Gastkontozugriff auf Sicherheitsprotokoll einschränken: Aktiviert
- Gastkontozugriff auf Systemprotokoll einschränken: Aktiviert
- Maximale Größe des Anwendungsprotokolls: 30080 Kilobytes
- Maximale Größe des Sicherheitsprotokolls: 100992 Kilobytes
- Maximale Größe des Systemprotokolls: 30080 Kilobytes
- Sicherheitsprotokoll aufbewahren für: Nicht definiert
- System bei Erreichen der max. Sicherheitsprotokollgröße herunterfahren: Deaktiviert (Hinweis: Für Hochsicherheitssysteme aktivieren)
- Systemprotokoll aufbewahren für: Nicht definiert

Security Compliance Manager (SCM)

Gruppenrichtlinien gehören zu den wichtigsten Werkzeugen in Windows-Umgebungen, um eine angemessene Absicherung der Systeme erzielen zu können. Das manuelle Setzen von hunderten von Einstellungen auf sichere, dem Verwendungszweck in der Institution angemessene Werte kann jedoch einen sehr hohen Aufwand darstellen.

Ein Werkzeug, das die Verwaltung von Gruppenrichtlinienobjekten unter Windows Client- und Serversysteme erleichtert, ist der Security Compliance Manager (SCM) von Microsoft. Dieser soll dabei unterstützen, von Microsoft und Drittanbietern empfohlene Sicherheitsrichtlinien institutionsweit durchzusetzen. Er gehört zur Gruppe der von Microsoft frei zum Download angebotenen "Solution Accelerators", die Aufgaben rund um die Planung und das Deployment von Systemumgebungen und Anwendungen unterstützen.

Der SCM stellt bereits nach der Installation eine Vielzahl von aktuellen Baselines für Windows-Betriebssysteme und -Anwendungen bereit, die entsprechend den Sicherheits- und Compliance-Anforderungen einer Institution angepasst und erweitert werden können. Bei einer Baseline handelt es sich um eine Sammlung relevanter Sicherheits- und Konfigurationseinstellungen (engl. Configuration Items), die letztendlich zur Gesamtsicherheit des jeweiligen Systems beitragen sollen.

Die Auswahl an Baselines beschränkt sich nicht auf einzelne Produkte und Versionen, sondern ist zudem nach Anwendungsrollen und Sicherheitsanforderungen unterteilt. So gibt es eigene Vorlagen für File- und Web-Server, Hyper-V, Domänen-Controller oder die Remote Desktop Services sowie die verschiedenen Versionen des Windows-Client-Betriebssystems und von Anwendungssoftware wie Internet Explorer, Microsoft Office, SQL Server oder Exchange Server.

In Version 4 des SCM werden neben Windows 8/8.1 und Windows Server 2012 (R2) mittlerweile auch Windows 10 und Windows Server 2016 unterstützt.

Die wichtigsten Funktionen des Security Compliance Managers sind im Folgenden dargestellt:

- Absicherung von Microsoft-Produkten (Windows Server, Windows Client, Office, Exchange Server, SQL Server, Internet Explorer)
- Zentrale Speicherung und Verwaltung von Baselines
- Möglichkeit der Nutzung von Baselines auf Stand-Alone- und Domänensystemen
- Vergleich und Zusammenführung (Merge) von Baselines
- Verschiedene Import- und Exportmöglichkeit
- Ausführliche integrierte Hilfe und Beschreibung der einzelnen Einstellmöglichkeiten

Beispielsweise werden für Windows Server 2012 R2 folgende Baselines mitgeliefert:

- Domain Controller Security Compliance (Version 1.0: 620 Einstellungen)
- Domain Security Compliance (Version 1.0: 9 Einstellungen)
- Member Server Security Compliance (Version 1.0: 421 Einstellungen)

Für Windows Server 2016 sieht dies folgendermaßen aus:

- Domain Controller Security Compliance (Version 1.0: 1013 Einstellungen)
- Domain Security Compliance (Version 1.0: 9 Einstellungen)
- Member Server Security Compliance (Version 1.0: 1011 Einstellungen)

Die Einstellungen dürfen nicht einfach übernommen werden, sondern müssen jeweils überprüft werden auf Kompatibilität mit den Sicherheitsanforderungen und speziellen Gegebenheiten der Institution. Dies gilt auch für Einstellungen, die auf "undefiniert" gesetzt sind. Vor einem Ausrollen auf produktive Systems sollten die Einstellungen getestet werden.

Feingranulare Passwortrichtlinien

Mit Windows Server 2008 wurden feingranulare Passwortrichtlinien eingeführt, die es ermöglichen, verschiedene Passwortricht- und Sperrrichtlinien für unterschiedliche Nutzergruppen innerhalb einer Domäne zu definieren.

In einer feingranularen Passwortrichtlinie können mit Ausnahme der domänenglobalen Kerberos-Einstellungen alle Passworteinstellungen inkl. der Sperrparameter gesetzt werden. Alle diese Parameter müssen beim Einsatz einer feingranularen Passwortrichtlinie definiert werden. Standardmäßig können nur Mitglieder der Gruppe Domänenadministratoren feingranulare Passwortrichtlinien einrichten. Jedoch lässt sich dieses Recht auch an andere Nutzer delegieren.

Feingranulare Passwortrichtlinien sollten eingesetzt werden, um innerhalb einer Institution überall angemessene Kennwortstärken durchzusetzen.

Shadow Groups

Feingranulare Passwortrichtlinien und einige weitere Parameter können nicht direkt auf OUs angewandt werden. Um eine feingranulare Passwortrichtlinie auf alle Nutzer einer bestimmten OU anzuwenden, können sogenannte Shadow Groups verwendet werden. Eine Shadow Group ist eine globale Sicherheitsgruppe, die logisch einer OU zugewiesen wird. Die Nutzer werden der Shadow Group zugewiesen, und die Passwortrichtlinie auf die Shadow Group angewandt. Zu beachten ist, dass beim Bewegen eines Nutzers in eine andere OU die Mitgliedschaft in den Shadow Groups anzupassen ist.

Keine Verwaltung von Passwörtern per GPO

Grundsätzlich lassen sich lokale Konten per GPO verwalten. Dies gilt etwa für das Anlegen lokaler (auch administrativer) Accounts, das Setzen von Passwörter, die Erstellung von Diensten mit Dienstkonten etc. Das Problem dabei ist, dass die Credentials in diesem Fall in XML-Dateien auf dem SYSVOL-Share auf allen Domänencontrollern der Domäne gespeichert sind und relativ einfach ausgelesen bzw. reversed werden können.

GPOs sollten nicht für das Setzen von Passwörtern verwendet werden. Liegen bereits Passwörter in GPOs vor, so sollten die Richtlinien entfernt und die entsprechenden Dateien gelöscht werden. Gleiches gilt für Skripte (z. B. VBS oder PowerShell), die Passwörter enthalten. Microsoft bietet ein PowerShell-Skript an, das SYSVOL nach Passwörtern in GPO XML-Dateien durchsucht.

APP.2.2.M4 Schulung zur Active Directory-Verwaltung

Das Active Directory ist die zentrale Datenbank der Serverbetriebssysteme ab Windows Server 2000, in der Benutzerdaten, Gruppenzugehörigkeiten und andere Verwaltungsdaten abgelegt werden. Clients können im Active Directory seit der Version Windows 2000 verwaltet werden.

Für die Administration eines Windows-Netzes werden detaillierte Kenntnisse des Active Directory und seiner grundlegenden Konzepte benötigt. Ansonsten kann es leicht zu Fehlkonfigurationen kommen, die erhebliche sicherheitstechnische Auswirkungen haben können. Eine Schulung der Administratoren auf diesem Gebiet und insbesondere zu Active Directory Sicherheitsthemen ist daher unerlässlich.

Schulungsinhalte

Je nach Größe und Komplexität des Netzes wird ein Active Directory nicht von einem einzelnen Administrator, sondern von einer ganzen Reihe von Administratoren mit speziellen Aufgaben und Tätigkeitsbereichen durchgeführt. Insoweit besteht auch nicht für alle Administratoren eines Active Directories der gleiche Schulungsbedarf. Zur Gewährleistung eines sicheren Betriebes muss jedoch jeder Administrator über ein hinreichendes Grundwissen verfügen, um seine eigenen Tätigkeiten in einen Gesamtkontext einordnen zu können.

Schulungsinhalte sollten in jedem Fall die folgenden Stichpunkte umfassen und diese erläutern. Wie tief ein Administrator sich mit den einzelnen Punkten beschäftigen muss, hängt von seinem späteren Tätigkeitsfeld ab.

Grundlagen

- Überblick über die Sicherheitsmechanismen von Windows Server
- Neuerungen in Sicherheitsmechanismen von aktuellen Windows-Client-Betriebssystemen (mit Berücksichtigung der von neuen Betriebssystemversionen oder aktuellen Service Packs hervorgerufenen Änderungen)
- Sicherheitsverwaltung (MMC, Security Editor, GPMC)
- Active Directory und DNS
- Vertrauensbeziehungen zwischen Domänen
- Notwendiger physikalischer Schutz aller Domänencontroller als Träger der Kerberos Daten

Active Directory

- Allgemeines: Planung, Einrichtung, Administration
- Schema-Verwaltung
- Replikation
- Backup
- Rechtevergabe
- Authentisierung
- Gruppenrichtlinien

PKI (Public Key Infrastruktur)

- Funktionsweise einer PKI
- Zertifikate und Zertifikatstypen
- Planung einer PKI
- Einrichten einer PKI
- Verwalten einer PKI
- Benutzerinteraktion mit der PKI

IPsec

- Funktionsweise von IPsec
- Konfiguration von IPsec
- Prüfung der erfolgreichen Einrichtung sicherer Verbindungen, Tools

DFS (Distributed File Service)

- Funktionsweise des DFS
- Administration des DFS
- Planung der DFS-Struktur
- Schutz der über DFS zugreifbaren Daten

Die einzelnen Active Directory Themen sollten dabei wie folgt detaillierter dargestellt werden:

Schema-Verwaltung

Im Normalfall ist eine installationsspezifische Veränderung des Active Directory-Schemas durch einen Administrator nicht notwendig. Die Schulung kann sich insofern auf die Problematik und Auswirkungen von Schema-Veränderungen beschränken.

Sollen individuelle Anpassungen des Schemas vorgenommen werden, sind weitergehende Schulungen zu Interna des Active Directory notwendig.

Replikation des Active Directory

- Verwendete Mechanismen zur Replikation des Active Directory (RPC und SMTP)
- Voreingestellte Parameter zur Replikation von Active Directory Inhalten
- Problematik der dezentralen Administration des AD im Zusammenhang mit Replikationskonflikten

Backup

- Problematik des Erstellens eines "Backups des Active Directory"
- Wiedereinspielen von Backups eines Domänencontrollers
- Zu ergreifenden Maßnahmen bei Ausfall von Domänencontrollern, die FSMO-Rollen innehaben

Rechtevergabe im Active Directory

- Vergabe von Zugriffsrechten auf AD-Objekte auf Attributsebene
- Vererbung von Zugriffsrechten und Blockade der Vererbung
- Mögliche Zugriffsrechte
- Delegation von administrativen Aufgaben auf der Ebene einzelner OUs

Authentisierung

- Kerberos
- PKI
- Smartcards

Gruppenrichtlinien

- Lokale Gruppenrichtlinien und im Active Directory gespeicherte Gruppenrichtlinien
- Konfigurationsmöglichkeiten mit Hilfe von Gruppenrichtlinien
- Wann werden Gruppenrichtlinien angewandt? Wie lässt sich dies konfigurieren?
- Gruppenrichtlinienobjekte (GPOs) als Objekte im Active Directory
- Gruppenrichtlinienobjekte können an Standorte / Domänen / OUs gebunden werden
- Reihenfolge, in der Gruppenrichtlinien abgearbeitet werden
- Möglichkeiten, die Anwendung von Gruppenrichtlinien zu kontrollieren
    - Vergabe von Zugriffsrechten auf Gruppenrichtlinien
    - No Override Eigenschaft der Bindung eines Gruppenrichtlinienobjektes an ein AD-Objekt
    - Block Policy Inheritance Eigenschaft von AD-Objekten
- Möglichkeiten zur selektiven Anwendung der Gruppenrichtlinien:
    - Sicherheitsfilter
    - WMI Filters und deren Ungeeignetheit (Performance-Gründe)
- Security Compliance Manager (SCM)
    - Bedienung
    - Enthaltene Baselines
    - Anpassung von Baselines
    - Anwendung lokal und per AD / SCCM

Einführung in Active Directory

Die folgenden Informationen stellen das Minimum dessen dar, was jedem Administrator als Einführung in AD und dessen Sicherheit bekannt und vertraut sein sollte. Dies kann weder eine gründliche Schulung noch die notwendige Arbeitserfahrung ersetzen, die auf anderem Wege zu erreichen und nachzuweisen ist.

In einer Domäne werden Rechner und Benutzer zusammengefasst und können durch den Domänenadministrator verwaltet werden. Eine Domänengrenze bildet grundsätzlich eine administrative Grenze, wenn auch keine Sicherheitsgrenze (siehe unten sowie Maßnahme APP.2.2.A5 Härtung des Active Directory) und begrenzt auch den Wirkungsbereich von Berechtigungen. Zusätzlich zu diesem Konzept bieten Windows Server an, Domänen baumartig miteinander in Beziehung zu setzen, sodass Eltern-Kind-Beziehungen zwischen Domänen bestehen können. Eine Kind-Domäne wird dabei auch als Sub-Domäne bezeichnet, da sich der Name der Kind-Domäne aus dem Namen der übergeordneten Domäne ableitet, indem diesem Namen der Name der Domäne durch einen Punkt getrennt angehängt wird.

Beispiel:

Name der Eltern-Domäne: unternehmen.de Name der Sub-/Kind-Domäne: verwaltung.unternehmen.de

Der so aufgespannte Namensraum ist mit dem zugehörigen DNS Namensraum identisch und kann auch nicht verschieden von diesem gebildet werden. Domänen, die einen gemeinsamen Namensstamm besitzen, bilden einen Baum (englisch Tree).

Domänen, die in mehreren Bäumen angesiedelt sind, also unterschiedliche Namensräume aufspannen, können dennoch gemeinsam verwaltet werden.

Derart zusammengeschlossene Domänenbäume bilden einen Wald (englisch Forest). Insbesondere bildet eine einzige alleinstehende Domäne auch einen Baum und gleichzeitig auch einen Wald.

In einem Wald gibt es immer eine ausgezeichnete Domäne, die eine gewisse Sonderstellung besitzt. Es ist die als erstes erzeugte Domäne, die auch als Forest-Root-Domäne (FRD, Wurzel-Domäne des Waldes) bezeichnet wird. Die Sonderstellung besteht darin, dass Administratoren der Forest-Root-Domäne im gesamten Forest weitreichende Berechtigungen besitzen. Für die Mitglieder der Gruppe Organisations-Admins stellen die Domänengrenzen keine administrativen Grenzen dar, da sie in allen Domänen Zugriffsrechte besitzen. Beim Aufbau eines Windows Domänenverbundes ist zu bedenken, dass die zuerst erzeugte Domäne immer die Forest-Root-Domäne ist. Insbesondere kann die "Rolle" der Forest-Root-Domäne nachträglich nicht auf eine andere Domäne "übertragen" werden, sodass die Domänenstruktur vollständig in der gewünschten Form neu erzeugt werden muss.

Das Active Directory besteht aus verschiedenen Objekten, den Active Directory Objekten (ADOs). Jedes Objekt besitzt einen ausgezeichneten Typ wie z. B. Benutzerobjekt oder Rechnerobjekt und ist gemäß dieses Typs aus verschiedenen Attributen zusammengesetzt. Die verschiedenen Objektattribute können verschiedene Werte aufnehmen wie z. B. Telefonnummer oder IP-Adresse. Das Active Directory kennt verschiedene vordefinierte Objekttypen:

- Domänen-Objekt: Dieses Objekt ist die Wurzel aller Active Directory-Objekte einer Domäne und enthält Informationen über die Domäne wie z. B. den Namen. Unterhalb eines Domänen-Objektes können andere Objekte angeordnet sein.
- Gruppierungs-Objekte: Diese Objekte dienen dazu, andere Objekte zu gruppieren. Standardmäßig steht das Objekt Organisations-Einheit (Organizational Unit, OU) zur Verfügung. Unterhalb eines OU-Objektes können weitere OU-Objekte enthalten sein sowie Rechner-, Benutzer- und Benutzer-Gruppen-Objekte.
- Rechner-Objekt: Durch dieses Objekt werden Windows Client-Rechner repräsentiert. Unterhalb eines Rechner-Objektes können keine weiteren Objekte mehr angeordnet sein. Das Active Directory ist nur auf die Verwaltung von Windows Rechnern ausgelegt, sodass Rechner-Objekte ausschließlich Windows Rechner repräsentieren können, die mit dem Active Directory zusammenarbeiten. Dies sind standardmäßig Rechner mit den Betriebssystemen ab Windows NT.
- Benutzer-Objekt: Durch dieses Objekt werden Domänenbenutzer repräsentiert. Unterhalb eines Benutzer-Objektes können keine weiteren Objekte mehr angeordnet sein.
- Benutzer-Gruppen-Objekte: Durch diese so genannten Sicherheitgruppen werden Windows-Gruppen repräsentiert. Es gibt verschiedene Gruppentypen, die sich im Geltungsbereich (domänen-, forestweit) und in den möglichen Gruppenmitgliedern (Domänen-, Forest-Objekte) unterscheiden. Es wird unterschieden zwischen lokalen, domänenlokalen, globalen und universalen Gruppen. Sicherheitsgruppen werden dazu benutzt, Berechtigungen zu vergeben. In Windows Server ist für größere Institutionen mit einer hohen Anzahl von Gruppen zu rechnen (durchaus mehrere zehntausend), sodass u. U. über eine werkzeuggestützte Verwaltung nachgedacht werden muss. Diese kann sowohl über selbst geschriebene Skripte als auch über Produkte von Drittherstellern erfolgen. Ob und welche Werkzeuge hier sinnvoll sind, muss jedoch im Einzelfall entschieden werden.

Der generelle Active Directory-Aufbau lässt sich wie folgt darstellen:

- Das Domänen-Objekt ist die Wurzel des Active Directory-Baumes einer Domäne.
- Unter dem Domänen-Objekt werden OU-Objekte erzeugt, um Rechner-, Benutzer- und Benutzer-Gruppen-Objekte strukturiert zusammenzufassen. Da OU-Objekte geschachtelt werden können, ergibt sich eine institutionsspezifische Baumstruktur.

Nach einer Standardinstallation existiert eine einfache und flache Active Directory-Struktur, die von einem Windows Server angelegt wird und dann entsprechend der Active Directory-Planung verändert werden muss. Da das Active Directory primär der Verwaltung eines Windowssystems dient, sollte beim Aufbau der Active Directory-Struktur darauf geachtet werden, dass die Struktur vornehmlich auf administrative Gegebenheiten abgestimmt wird. Wenn stattdessen die organisatorische Struktur einer Institution bis ins Kleinste nachgebildet wird, kann dies zu Problemen in der Administration, mindestens jedoch zu hohem administrativen Aufwand führen.

Die möglichen Anordnungen von Active Directory-Objekten, d. h. die Festlegung, welches Objekt welche anderen Objekte enthalten darf, welche Attribute existieren und aus welchen Attributen Objekte zusammengesetzt werden, wird durch das so genannte Active Directory-Schema definiert. Das von Microsoft vorgegebene Active Directory-Schema kann auch verändert werden. Dies stellt jedoch einen gravierenden Eingriff in das Active Directory dar, der nur nach sorgfältiger Planung durchgeführt werden darf. Eine Schemaänderung wirkt sich in allen gemeinsam verwalteten Domänen, d. h. im Wald, aus. Da die Schemaänderung eine kritische Operation ist, kann diese nur an genau einem Rechner, dem sogenannten Schema-Master durch Mitglieder der Gruppe Schema-Admins durchgeführt werden. Schemaänderungen können zudem unter Umständen nicht mehr rückgängig gemacht werden. Die Mitgliedschaft in dieser Gruppe ist daher unbedingt restriktiv zu vergeben und streng zu kontrollieren.

Die Mitglieder der Gruppe "Organisations-Admins", zu der in der Voreinstellung der Administrator der Forest Root Domäne gehört, haben besondere Befugnisse in allen Domänen des Netzes. Sie können z. B. neue Domänen in den Forest aufnehmen und haben Administratorrechte auf allen Domänencontrollern des Active Directory.

Innerhalb einer einzelnen Domäne erfolgt die Administration durch Mitglieder der jeweiligen domänenspezifischen Gruppe "Domänen-Admins". Diese Gruppe verfügt innerhalb einer Domäne über unbeschränkte administrative Berechtigungen. Es ist jedoch möglich, einzelne administrative Aufgaben auch für andere Benutzerkonten zu ermöglichen und so administrative Aufgaben zu delegieren (siehe auch APP.2.2.A2 Planung der Active Directory-Administration).

Eine Delegation administrativer Aufgaben innerhalb einer Domäne kann auch so erfolgen, dass lediglich die Administration eines Teils der Benutzerkonten und Computer einer Domäne delegiert wird. Dies ist innerhalb der Grenzen der OUs möglich, die zur Gruppierung von Benutzer- bzw. Computerkonten innerhalb der Domäne dienen.

Eine Vielzahl von Windows-Client-Konfigurationsparametern ist in den Gruppenrichtlinien zusammengefasst. Neben den lokalen Gruppenrichtlinien auf jedem einzelnen Windows Client-Rechner gibt es auch Gruppenrichtlinien, die im Active Directory gespeichert sind. Dies gestattet es, Rechner oder Benutzerkonten zentral zu konfigurieren. Wirkungsbereich einer solchen, im AD gespeicherten Gruppenrichtlinie können unter anderem ganze Domänen oder OUs sein. Hier dienen OUs zur Gruppierung gleichartig konfigurierter Rechner oder Benutzerkonten. Da sich OUs schachteln lassen und mit einer einzelnen OU mehrere Gruppenrichtlinien verbunden sein können, wirken auf einen einzelnen Rechner unter Umständen viele verschiedene Gruppenrichtlinien ein (siehe auch APP.2.2.A3 Planung der Gruppenrichtlinien unter Windows und die entsprechenden Client-Bausteine).

Zur Speicherung der Daten wird eine relationale, transaktionsorientierte Datenbank verwendet. Diese Datenbank wird auf speziellen Servern, den "Domänencontrollern", verteilt. Der Domänencontroller nutzt dabei das Active Directory, um eine zentrale Authentisierung und Autorisierung von Benutzern und Computern in einer Domäne zur Verfügung zu stellen. Folgende Protokolle werden dazu verwendet:

- LDAP (Lightweight Directory Access Protocol) zur Abfrage von Objekten und Attributen des Active Directory
- Kerberos zur Authentisierung von Benutzern und Computern
- CIFS (Common Internet File System) zum Transfer von Dateien im Rechnernetz
- DNS (Domain Name System) zur Namensauflösung der Computersysteme im Netz

Mit einigen Ausnahmen enthält jeder Domänencontroller dabei nur die Daten seiner eigenen Domäne. Diese Ausnahmen sind:

- Jeder Domänencontroller enthält die Schema- und Konfigurationsdaten des gesamten Forests.
- Mindestens ein Domänencontroller jeder Domäne enthält zusätzlich noch den "Global Catalog".

Das Active Directory wird auf Domänencontrollern gehalten und innerhalb einer Domäne zwischen diesen durch Replikation synchronisiert. Das Active Directory einer Domäne enthält nur domänenbezogene Informationen. Um in einem Forest schnell auf Informationen aus dem gesamten Forest zugreifen zu können, wird der so genannte Global Catalog (GC) aufgebaut. Er besteht aus Teilinformationen von Active Directory-Objekten und wird im gesamten Forest repliziert, sodass über den Global Catalog in einer Domäne auch direkt auf Informationen aus anderen Domänen zugegriffen werden kann.

Neben der beschriebenen baumartigen und hierarchischen Struktur baut Windows Server automatisch eine zusätzliche und orthogonale Struktur auf. Räumlich nahe Rechner (dies bestimmt Windows Server über Netzlaufzeiten) werden zu so genannten Standorten (englisch Sites) zusammengefasst. Über Sites wird unter anderem auch die Replikationsstruktur von Domänen Controllern gesteuert. Je Site muss mindestens ein Rechner existieren, der eine Kopie des Global Catalogs hält. Der Global Catalog muss im Rahmen des Anmeldeprozesses eines Benutzers angefragt werden, sodass bei der Anmeldung immer ein Global Catalog-Server zugreifbar sein muss. Die von Windows Server automatisch aufgebaute Standortstruktur sollte an die institutionsinternen Gegebenheiten wie z. B. Standorte in verschiedenen Städten oder Ländern individuell angepasst werden. Da dies Einfluss auf die Active Directory-Replikationsbeziehungen hat, ist dazu ein Konzept zu erstellen.

Die Daten des Active Directory werden mittels Multi-Master-Replikation zwischen den Domänencontrollern einer Institution repliziert. Auf jedem Domänencontroller existiert somit ein Replikat des Active Directory, das geändert und als Grundlage für zukünftige Replizierungen dienen kann. Bei der Verwendung mehrerer Domänencontroller in einer Institution werden so redundante Kopien des Active Directory erzeugt und die Wahrscheinlichkeit eines Totalausfalls minimiert.

Der Abgleich der Daten zwischen den einzelnen Domänencontrollern kann über zwei verschiedene Replikationsmechanismen erfolgen (RPC oder asynchrones SMTP). Welcher Mechanismus verwendet wird, lässt sich ebenso konfigurieren wie die Zeitabstände, in denen die Replikation erfolgt.

Durch das Konzept der verteilten Datenbanken kann eine gewisse Ausfallsicherheit des Active Directory erreicht werden, indem eine genügende Anzahl geeignet verteilter DCs betrieben wird. Problematisch sind dabei jedoch die Inhaber der FSMO-Rollen.

FSMO bzw. Operations Master

Operations Master bzw. FSMO (Flexible/Floating Single Master Operations), wie es offiziell bis 2005 hieß (der Name ist trotzdem weiterhin in Gebrauch), ist ein Feature von AD. Der FSMO ist eine bestimmte Menge von Aufgaben eines Domaincontrollers, die nicht wie normale DC-Aufgaben verteilt auf mehreren DCs bearbeitet werden können, die über Kopien der AD-Datenbank verfügen und sich über Multi-Master-Replikation synchronisieren. FSMO-Aufgaben hingegen lassen sich nur in einer einzigen Datenbank ausführen, die Master-Datenbank genannt wird.

Es gibt verschiedene FSMO-Rollen, darunter auf Domänenebene

- PDC (Primärer Domänencontroller)-Emulator: unter anderem für die Zeitsynchronisation verantwortlich
- RID-(Relative ID-)Master: zur konsistenten ID-Vergabe
- Infrastruktur-Master: für die Konsistenz domänenübergreifender Links

und auf Waldebene

- Schema-Master: um Schemaänderungen zu replizieren (etwa beim Upgrade von DCs oder dem Deployment von Exchange Server oder Skype for Business (vormals Lync) Server
- Domain-Naming-Master: zur Verteilung von Änderungen an Namensräumen

Aufgrund der hohen Wichtigkeit von DCs, die FSMO-Rollen innehaben, sind diese besonders zu schützen.

APP.2.2.M5 Härtung des Active Directory

Da die Absicherung der Infrastrukturkomponenten, welche die Funktionen des AD abbilden, wesentlich für die Sicherheit der gesamten Institution sind, ist eine gründliche Härtung sämtlicher Komponenten notwendig.

Built-In-Accounts als Notfallkonten

Built-In-Accounts sollten mit komplexen Passwörtern (mindestens 20 Zeichen) versehen werden und ausschließlich als Notfallkonten dienen. Dafür werden die Passwörter an sicherer Stelle hinterlegt und ein Prozess definiert, von wem sie im Notfall wie genutzt werden sollen.

Protected Users-Gruppe

Für privilegierte Accounts empfiehlt sich die Verwendung der Protected Users-Gruppe (siehe Baustein APP.2.2 Windows Server 2012). Konten dieser Gruppe ist die Authentisierung nur via Kerberos gestattet. Effektiv verhindert dies Pass-The-Hash-Attacken. Diese Maßnahme setzt ein Domain Function Level 2012 voraus. Alle Anwendungen müssen mit Kerberos kompatibel sein.

(Group) Managed Service Accounts

Nach Möglichkeit sollten (Group) Managed Service Accounts verwendet werden, wenn Anwendungen auf Servern besondere Berichtigungen benötigen (siehe Baustein APP.2.2 Windows Server 2012).

Ist das nicht möglich, so sollten, um das Brute-Force-Brechen des Passworts eines Dienstkontos zu verhindern, alle Dienstkonten mit mindestens 20 Stellen Passwortlänge abgesichert sein. Ab Domain Functional Level Windows Server 2008 kann und sollte dies per Passwort-Richtlinie erzwungen werden.

Konfiguration von Windows Server als Domänencontroller

Domänencontroller stellen in einem Netz auf Basis der Windows Server-Betriebssysteme die zur Verwaltung einer Windows Server-Domäne nötigen Dienste zur Verfügung, unter denen ADS die wichtigste Rolle einnimmt. In der Regel wird von einem Domänencontroller auch der Namensdienst DNS (Domain Name Service) angeboten, ohne den das Active Directory nicht betrieben werden kann. Im DNS werden von Windows Referenzen auf wichtige Windows Server-Ressourcen gehalten, deren Integrität für das korrekte Funktionieren einer Windows Server-Domäne essentiell sind. Da ein Domänencontroller als Anmeldeserver fungiert, führt er den dazu notwendigen Kerberos-Dienst aus. Die Kerberos-Komponenten auf dem Domänencontroller bewahren zudem die im Rahmen des Authentisierungsprotokolls genutzten geheimen Schlüssel auf.

Da jedem Domänencontroller daher eine wichtige Rolle zukommt und durch ihn schützenswerte Daten gespeichert werden, sind für die Konfiguration folgende Punkte zu beachten. Daneben gelten auch für einen Domänencontroller die im entsprechenden passenden Baustein für das Betriebssystem (z. B. SYS.1.2.2 Windows Server 2012) beschriebenen Aspekte.

- Die Sicherheit eines Domänencontrollers leitet sich hauptsächlich aus zwei wesentlichen Bereichen ab: der Sicherheit der Betriebssystemkonfiguration und der Sicherheit des Active Directory, das auf eigene Sicherheitsmechanismen zurückgreift (siehe auch APP.2.2.A4 Schulung zur Active Directory-Verwaltung). Die Sicherheitseinstellungen des Betriebssystems erfolgen im Wesentlichen durch Gruppenrichtlinien. Die Sicherheitseinstellungen des Active Directory erfordern entsprechende Planung und Umsetzung (siehe APP.2.2.A1 Planung des Active Directory, APP.2.2.A3 Planung der Gruppenrichtlinien unter Windows).
- An einem Domänencontroller dürfen sich nur berechtigte Administratoren lokal anmelden. Ein Benutzerbetrieb auf einem Domänencontroller darf nicht erlaubt werden. Nach einer Standardinstallation ist es normalen Benutzern daher nicht gestattet, sich lokal an einem Domänencontroller anzumelden.
- Ein Domänencontroller sollte neben den zwingend notwendigen Standard-Domänencontrollerdiensten wie z. B. Active Directory, Kerberos und DNS keine weiteren Infrastrukturdienste (z. B. DFS, DHCP) anbieten. Insbesondere vom Betrieb eines DHCP-Servers auf einem Domänencontroller muss aus Sicherheitsgründen abgeraten werden. Beide Dienste laufen unter den gleichen Berechtigungen ab. Dadurch können vereinfacht dargestellt die Zugriffsrechte auf DNS-Daten nicht mehr durchgesetzt werden, wenn der DHCP-Dienst Veränderungen an DNS-Daten durchführt.
- Ein Domänencontroller sollte keine (Applikations-)Serverdienste anbieten, da bei Fehlern in den Serverprogrammen eine Kompromittierung des Domänencontrollers und damit der gesamten Windows Server-Domäne möglich ist.

- Die Konfiguration des Kanals, der zur Kommunikation von Verwaltungsdaten zwischen Rechnern einer Windows-Server Domäne genutzt wird, sollte so sicher wie möglich sein (siehe dazu APP.2.2.A8 Konfiguration des sicheren Kanals unter Windows).
- Kann ein Domänencontroller in den so genannten Active Directory-Restore-Modus gebootet werden, so ist es möglich, Veränderungen am AD durchzuführen, indem z. B. alte Zustände (teilweise oder vollständig) von Backup-Medien geladen werden. Diese Veränderungen lassen sich so einspielen, dass sie nach dem regulären Booten durch die Active Directory-Replikation an alle anderen Domänencontrollern einer Domäne propagiert werden. Es ist daher sicherzustellen, dass der Active-Directory-Restore-Modus durch ein geeignetes Passwort geschützt ist und Arbeiten in diesem Modus nur unter Einhaltung des Vier-Augen-Prinzips erfolgen. Der Active Directory-Restore-Modus ist kommandozeilenbasiert, und Tippfehler können gravierende Folgen haben, z. B. Löschen oder Überschreiben des falschen Active Directory-Zweiges. Daher bietet das Vier-Augen-Prinzip hier neben der Tätigkeitskontrolle auch eine Sicherheit durch die Kontrolle aller Eingaben durch zwei Personen.
- Die Domänencontroller der Forest-Root-Domäne (FRD) sind aufgrund der Sonderstellung der FRD besonders schutzbedürftig.

Sicherer Betrieb von Domänencontrollern

Um Konfigurationsfehler zu vermeiden und einen einheitlichen Sicherheitsstand zu erhalten, sollte ausgehend von einer Referenzinstallation eine abbildbasierte Einrichtung der Domänencontroller vorgenommen werden. Ferner sollten auch die Sicherheitseinstellungen in der Basiseinrichtung der Domänencontroller einheitlich vorgenommen werden. Dies sollte durch die Implementierung eines vorhersagbaren und leicht zu wiederholenden Bereitstellungsvorgangs erreicht werden. Dies beinhaltet:

- Regelmäßiges Einspielen aktueller Hotfixes und Service Packs
  In regelmäßigen Abständen sollten aktuelle Hotfixes und Service Packs eingespielt werden. Die Auswirkungen sollten jedoch vorher an einem Abbild des Referenz-Domänencontrollers ausführlich getestet werden.
- Vergabe von ausreichend starken Passwörtern
  Für die Benutzerkonten im Active Directory sind ausreichend starke Passwörter zu vergeben. Hinweise auf ausreichend starke Passwörter finden sich in der institutionsweiten Regelung des Passwortgebrauchs . Neben der Erstellung komplexer Passwörter ist sicherzustellen, dass die Weitergabe der Passwörter an die betroffenen Personen über vertrauensvolle Wege erfolgt. Auch sollten die Benutzerkonten insbesondere bei der Ersteinrichtung mit individuellen Passwörtern ausgestattet werden.
- Sicherstellen der Integrität der Installation
  Werden die Domänencontroller an einem anderen Zielstandort bereitgestellt, sollten für deren Transport Signaturen verwendet werden, um auf diese Weise die Integrität der Installationen sicherzustellen

Berechtigung ausführbarer Dateien

Um nach der Heraufstufung der Domänencontroller die Stammordner der Datenträger vor Speicherplatzangriffen zu schützen, sollten die Berechtigungen für die Gruppe "Jeder" auf "Lesen und Ausführen" eingrenzt werden. Der "Vollzugriff" ist lediglich für die Administratoren zu erteilen.

Systemstart von anderen Betriebssystemen verhindern

Ein Systemstart von anderen Betriebssystemen auf den Domänencontrollern kann die Zugangsrestriktionen von NTFS aushebeln und einen Zugriff auf kritische Daten ermöglichen. Neben der bereits erwähnten räumlichen Absicherung der Server sind daher ebenfalls organisatorische Vorkehrungen zu treffen.

Der Remote-Netzstart und somit auch die Möglichkeit zur Remote-Netzinstallation z. B. durch Remote Installation Services (RIS) oder Bootstrap Protocol (BOOTP) sollte deaktiviert und die Verwendung eines BIOS-Kennwortes beim Systemstart vorgesehen werden.

Neustart-Schutz mit Festplattenverschlüsselung (BitLocker)

Noch sicherer ist eine Festplattenverschlüsselung, welche die Eingabe eines Passworts oder Nutzung eines Datenträgers beim Systemstart des DC erfordert. Die Maßnahme ist im entsprechenden Windows Server-Baustein beschrieben (z. B. SYS.1.2.2 Windows Server 2012).

Sichere Richtlinieneinstellungen für Domänen und Domänencontroller

Ein Windows Server mit Active Directory enthält Standard-Sicherheitsrichtlinieneinstellungen für die Domäne und für die Domänencontroller. Es werden jedoch Änderungen der Standard-Richtlinieneinstellungen zur Erhöhung der Sicherheit von Domäne und Domänencontrollern durch die folgenden Punkte empfohlen:

- Sichere Kennwortrichtlinien-Einstellungen
  Der Zugriff auf Domänencontroller muss mit starken Mechanismen abgesichert sein. Näheres zu den dafür notwendigen Einstellungen der Kennwortrichtlinien findet sich in den Microsoft-Server-spezifischen Bausteinen.
- Konto-Sperrungsrichtlinien
  Die Protokollierung der Anmeldeversuche (siehe hierzu auch APP.2.2.M11 Überwachung der Active Directory Infrastruktur) sollte so eingerichtet werden, dass Angriffe erkannt werden können. Beispielsweise könnte eine große Zahl nicht erfolgreicher Kennworteingaben während eines Anmeldeversuchs auf einen Brute-Force-Angriff hindeuten. Die eigentliche Kontosperrung ist über die Optionen Kontosperrdauer, Kontosperrungsschwelle und die Zurücksetzung des Kontosperrungszählers entsprechend der Beschreibung in Maßnahme APP.2.2.M3 Planung der Gruppenrichtlinien unter Windows zu definieren.
- Kerberos-Richtlinien-Einstellungen
  Der durch Kerberos zur Verfügung stehende Authentisierungsdienst teilt dem jeweiligen Client die erforderlichen Autorisierungsdaten für Ressourcenzugriffe zu. Hierbei wird der Zugriff auf Netzressourcen anhand von Sitzungstickets gewährt. Dazu stellt der Domänencontroller im Vorfeld ein sogenanntes Ticket-Granting-Ticket (TGT) an den Client aus. Erfolgt ein Zugriffsversuch seitens der Clients auf eine Ressource, so übermittelt der Client das TGT zur Prüfung an den Domänencontroller. Der Domänencontroller wiederum generiert dem Client nach erfolgreicher Prüfung ein Sitzungsticket, mit dem ein zeitlich begrenzter Zugriff auf die Ressource ermöglicht wird. Durch eine Anpassung der Kerberos-Richtlinieneinstellung können für Domänen-Benutzerkonten Aspekte der Kerberos-Tickets wie die Gültigkeitsdauer angepasst werden (siehe Maßnahme APP.2.2.A3 Planung der Gruppenrichtlinien unter Windows).

In Bezug auf sichere Richtlinieneinstellungen für Domänencontroller werden des Weiteren nachfolgende Maßnahmen empfohlen:

- Benutzerrechte sollten restriktiv vergeben werden, sodass die Benutzer in der Domäne oder auf dem Domänencontroller lediglich die von ihnen verantworteten betrieblichen oder administrativen Aufgaben erledigen können. Die Zugriffsmöglichkeiten von Benutzern sollte dabei so eingeschränkt werden, dass sie die Sicherheit der Domänencontroller nicht gefährden (siehe auch Maßnahme APP.2.2.A1 Planung des Active Directory).
- Durch die Einrichtung von Richtlinieneinstellungen für die Domänencontroller-Überwachung wird der Nachweis der Verantwortung für sensible Verzeichnisoperationen, z. B. Verwaltungs- oder Konfigurationsänderungen, ermöglicht. Es sollte eine Überwachung von Anmeldeversuchen, Kontoverwaltung, Active Directory-Zugriff, Objektzugriffsversuchen, Richtlinienänderungen, Rechteverwendung, Prozessverfolgung und Systemereignisse eingerichtet werden (siehe Maßnahme APP.2.2.A11 Überwachung der Active Directory Infrastruktur).
- Wichtige Active Directory-Objekte wie z. B. die Verzeichnispartitionen sind mit geeigneten Richtlinieneinstellungen zu überwachen. Dazu muss die Überwachung der Verzeichnispartitionen (logische Bereiche der Active Directory-Datenbank) aktiviert werden. Die hiervon betroffenen Verzeichnispartitionen lauten "Schema", "Konfiguration" und "Domäne" (dito).

Die obigen Empfehlungen zur Einrichtung von Richtlinieneinstellungen führen dazu, dass die voreingestellte maximale Größe des Sicherheitsprotokolls angehoben werden muss, damit eine größere Anzahl überwachter Ereignisse aufgenommen werden kann. Die Protokolle müssen zeitnah ausgewertet werden. Außerdem muss es ein klar definiertes Vorgehen für die regelmäßige und rechtzeitige Archivierung sowie eine Sicherung der Sicherheits- und Systemereignisprotokolle geben, damit keine Ereignisse verloren gehen oder überschrieben werden.

Ist darüber hinaus die Zusammenarbeit zwischen Domänen in verschiedenen Gesamtstrukturen zu unterstützen, z. B. zur gemeinsamen Nutzung von Anwendungen oder zur begrenzten Zusammenarbeit zwischen verschiedenen Gesamtstrukturen in einer Institution, sollten externe Vertrauensstellungen eingerichtet werden. Durch externe Vertrauensstellungen entsteht jedoch ein potenzielles Sicherheitsrisiko, da Sicherheitsgrenzen überschritten werden. Daher sollten die Domänencontroller in der vertrauenden Domäne Autorisierungsdaten der Benutzer filtern und Sicherheitskennungen (Security IDs, SIDs) entfernen, die sich nicht auf die Domäne des Benutzerkontos beziehen. Eine ausführliche Beschreibung hinsichtlich der Erschleichung umfassender Berechtigungen durch gefälschte SIDs und die Gegenmaßnahmen durch SID-Filterung ist in den Microsoft-Knowledge-Base-Artikeln 289243 und 289246 aufgeführt.

Die Richtlinieneinstellungen der Sicherheitsoptionen für Domänencontroller beeinflussen die sicherheitsrelevanten Konfigurationseinstellungen der Windows Server Betriebssysteme und sollten daher gewissenhaft eingestellt werden. Dies gilt nicht nur für die Active Directory-relevante Konfiguration, sondern auch für andere Komponenten des Windows Server-Betriebssysteme (z. B. Sicherheitskonfigurationseinstellungen für Netz, Dateisystem und Benutzeranmeldung).

Viren-Schutz für Domänencontroller

Für einen ausreichenden Schutz gegen Computer-Viren und andere Schadprogramme muss in einer Institution ein umfassendes Viren-Schutzkonzept umgesetzt werden. Die entsprechende Vorgehensweise wird im Baustein OPS.1.1.5 Schutz vor Schadprogrammen beschrieben. In dem Viren-Schutzkonzept sollten grundsätzlich auch die Domänencontroller einer Institution berücksichtigt werden.

Damit die Nutzung eines Viren-Schutzprogramms auf einem Domänencontroller keine negativen Auswirkungen auf den laufenden Betrieb hat, sind jedoch für Domänencontroller einige Besonderheiten zu beachten.

Die Hinweise in dieser Maßnahme sind als allgemeine Hinweise zu verstehen. Unter Umständen müssen zusätzlich die speziellen Anweisungen des Herstellers des jeweils eingesetzten Viren-Schutzprogramms berücksichtigt werden.

Bei der Auswahl der Viren-Schutz-Software muss darauf geachtet werden, dass der Einsatz auf einem Domänencontroller explizit unterstützt wird. Entscheidend ist dabei, dass die Viren-Schutz-Software die vom Betriebssystem-Hersteller vorgesehenen Programmierschnittstellen (Application Programming Interface, API) verwendet.

Bei der Verwendung falscher Programmierschnittstellen werden unter Umständen die Metadaten der untersuchten Dateien durch den Zugriff der Viren-Schutz-Software verändert. In diesem Fall ist es möglich, dass der File Replication Service (FRS) des Betriebssystems eine Replizierung der vermeintlich geänderten Datei innerhalb der Institution veranlasst. Solche unnötigen Replizierungen können zu einer verminderten Systemleistung führen und sollten daher vermieden werden. Weitere Details bezüglich kompatibler Viren-Schutzprogramme sind im Microsoft-Knowledge-Base-Artikel mit der Artikel-ID 815263 zu finden.

Die korrekte Funktionsweise der Viren-Schutz-Software sollte vor dem endgültigen Einsatz in einer Produktivumgebung in einer Testumgebung ausgiebig auf korrekte Funktionalität getestet werden. Die Testumgebung sollte dabei den Gegebenheiten der Produktivumgebung möglichst nachempfunden werden, um Auswirkungen auf die Gesamtleistung des Domänencontrollers festzustellen.

Um die Einführung von Schadsoftware zu vermeiden, sollte auf Domänencontrollern ausschließlich die Active Directory-Funktionalität des Betriebssystems verwendet und möglichst keine weiteren Dienste angeboten werden. Insbesondere darf ein Domänencontroller nicht als herkömmlicher Arbeitsplatz genutzt werden. So sollten lokal auf einem Domänencontroller angemeldete Benutzer nicht in der Lage sein, im Internet zu surfen, E-Mails zu empfangen oder auf externe Datenträger wie z. B. USB-Speicher oder optische Medien zuzugreifen.

Ebenso sollte der Domänencontroller nicht als Dateifreigabe-Server genutzt werden. Werden auf dem Domänencontroller Dateien per Dateifreigaben im Netz verfügbar gemacht, so werden diese Dateien vom Viren-Schutzprogramm bei jedem Zugriff auf Schadsoftware untersucht, was zu Performance-Einbußen auf dem Domänencontroller führen kann. Dateifreigaben auf dem Domänencontroller sollten daher deaktiviert werden.

Grundsätzlich sollte das Viren-Schutzprogramm alle Dateizugriffe transparent im Hintergrund überwachen. Allerdings existieren in Windows Server-Betriebssystemen einige Dateien, z. B. Verzeichnisdienst-Datenbank, Protokolldateien, Datenbank des Dateireplikationsdienstes, die bei einem Zugriff durch ein Viren-Schutzprogramm die Funktionen des Domänencontrollers beeinträchtigen können. Um unnötige Dateisperrungen durch das Viren-Schutzprogramm zu verhindern und den einwandfreien Betrieb des Domänencontrollers sicherzustellen, sollten daher die folgenden Punkte beachtet werden.

Zugriff auf die Active Directory-Datenbank und Protokolldateien durch die Extensible Storage Engine (ESE)

Die Verzeichnisdienst-Datenbank und Protokolldateien werden vom Active Directory mittels ESE für den exklusiven Dateizugriff geöffnet. Daher kann die ESE nur auf die Dateien zugreifen, die nicht durch die Viren-Schutz-Software blockiert werden. Gleichzeitig kann die Viren-Schutz-Software nur auf die Dateien zugreifen, die nicht durch die ESE blockiert werden.

Sowohl die Datenbankdateien als auch die Protokolldateien verwenden Active Directory-interne Prüfsummen, die durch den Dateizugriff eines Viren-Schutzprogramms ungültig werden und zu inkonsistenten Datenbanken führen können. Eine inkonsistente Datenbank kann zu einem Ausfall des Active Directory führen.

Daher sind folgende Dateien aus der regelmäßigen Virenüberprüfung auszuschließen:

- Active Directory-Hauptdatenbank
- Active Directory-Transaktionsprotokolldateien
- Active Directory-Arbeitsordner

Zugriff auf die Datenbank und Protokolldateien des Dateireplikationsdienstes (FRS) durch ESE

Wie bereits beschrieben können durch den unsachgemäßen Einsatz von Viren-Schutzprogrammen bei Datenbank- oder Protokolldateizugriffen konkurrierende Zugriffe des Replikationsdienstes auftreten. Ebenso kann eine Änderung der internen Prüfsummen dieser Dateien zu einem Ausfall des Active Directory führen. Daher sollten folgende Dateien aus der regelmäßigen Virenüberprüfung ausgeschlossen werden:

- Dateien im Arbeitsordner des Dateireplikationsdienstes
- Datenbankprotokolldateien des Dateireplikationsdienstes
- Staging-Ordner (Cache für neue und geänderte Dateien, die repliziert werden sollen) und Stammreplikat (Kopie des Distributed-File-System-Stamms und dessen untergeordnete Verknüpfungen) des Dateireplikationsdienstes
- Vorinstallationsordner des Dateireplikationsdienstes

Wird der Dateireplikationsdienst verwendet, um Windows-Freigaben zu replizieren, deren Verknüpfungsziel auf Windows Server-Betriebssystemen liegt, so sind diese Dateien der SYSVOL-Ordner ebenfalls auszuschließen.

Dateireplikation durch den Dateireplikationsdienst (File Replication Service, FRS)

Der Dateireplikationsdienst wird von den Windows Server-Betriebssystemen für die Replizierung von Anmeldeskripten und Systemrichtlinien des SYSVOL-Ordners zwischen Domänencontrollern verwendet. Werden die Metadaten (Sicherheitsinformationen oder Zeitstempel) einer Datei durch ein Viren-Schutzprogramm verändert, so wird die entsprechende Datei durch FRS zwischen den Domänencontrollern erneut repliziert. Dieses Verhalten führt zu einer erhöhten Replizierung der SYSVOL-Dateien und damit zu

- einem erhöhten Bandbreitenverbrauch im Netz,
- einem erhöhten Ressourcenverbrauch auf den Domänencontrollern und
- einer hohen Anzahl von Dateien im Staging-Ordner.

Um eine übermäßige Replikation zu verhindern, sollten folgende Punkte beachtet werden:

- Es ist ein Viren-Schutzprogramm auszuwählen, das die Metadaten der SYSVOL-Dateien nicht ändert.
- Sollte eine entsprechende Auswahl nicht möglich sein, so ist das SYSVOL-Verzeichnis inklusive aller Unterverzeichnisse aus der automatischen Überprüfung durch das Viren-Schutzprogramm zu entfernen. Dabei erhöht sich allerdings das Risiko für einen Virenbefall, da anders als bei den oben genannten Dateien in diesem Falle ausführbare Dateien, z. B. Anmeldeskripte, von der Viren-Schutz-Software nicht mehr erfasst werden. Daher sollten für den Fall, dass die SYSVOL-Verzeichnisse nicht durch das Viren-Schutzprogramm abgesichert werden können, ausschließlich signierte Anmeldeskripte auf den Domänencontrollern und Arbeitsstationen der Administratoren verwendet werden.

Update-Funktion des Microsoft Betriebssystems

Im Rahmen der Update-Funktion des Windows-Server-Betriebssystems ("Microsoft Update", "Windows Update" oder "Automatisches Update") kann das exklusive Zugriffsrecht für Dateien eines Viren-Schutzprogramms zu Problemen führen.

Um diese Probleme zu vermeiden, sollten folgende Dateien aus der regelmäßigen Virenüberprüfung ausgeschlossen werden:

- Datenbankdateien mit Bezug auf die Update-Funktionalität wie z. B. im Ordner %windir%\SoftwareDistribution\Datastore die Datei "Datastore.edb"
- die im Ordner %windir%\SoftwareDistribution\Datastore\Logs abgelegten Transaktionsprotokolldateien

Weitere Details zu den auszuschließenden Dateien finden sich online im Dokument "Empfehlungen zum Virenscan auf Unternehmenscomputern, auf denen unterstützte Windows-Versionen ausgeführt werden".

RDP

Beim Schließen einer RDP-Sitzung sollte der Benutzer automatisch abgemeldet werden. Dies kann per GPO realisiert werden.

Individuell geprüft werden muss die Verwendung des Restricted Admin Mode. Bei Aktivierung können keine Zugangsdaten bei der Anmeldung via RDP übertragen werden. Dadurch sind auf dem Host-System keine Hashes vorhanden. Allerdings erlaubt diese Einstellung die Durchführung von Pass-the-Hash-Angriffen auf den RDP-Dienst.

APP.2.2.M6 Aufrechterhaltung der Betriebssicherheit von Active Directory

Die in der Produktivumgebung eingesetzten Domänencontroller sind durch die Administratoren auf dem vorangegangen Sicherheitsniveau zu halten und bei erhöhten Anforderungen entsprechend anzupassen. Für Änderungen an den Systemen, die sich unter anderem durch die regelmäßigen Wartungsarbeiten ergeben, sind im Vorfeld schriftlich niedergelegte Richtlinien zu entwickeln.

Beschränkung der Vertrauensbeziehungen

Die Vertrauensbeziehungen zwischen Domänen und vor allem von und zu anderen Wäldern bzw. zwischen verschiedenen Wäldern (z. B. Tiers) der Institution sollten regelmäßig evaluiert werden daraufhin, ob sie weiterhin benötigt und gerechtfertigt sind, ob sie den korrekten Typ haben (d. h. vor allek, ob eine zweiseitige Vertrauensbeziehung wirklich notwendig ist) und ob die Sicherheitskontrollen zu ihrer Gewährleistung ausreichend sind.

Die Frage "Was geschieht, wenn diese Vertrauensbeziehung gelöscht wird?" sollte für jede Vertrauensbeziehung gestellt werden. Wenn die Antwort unbekannt oder nicht klar ist., ist dies ein Hinweis darauf, dass die Vertrauensbeziehung unter Beachtung üblicher Testprozeduren und Fallbackplanung deaktiviert und bei Ausbleiben von Problemen gelöscht werden sollte.

Sicherheit der Dienste-Administratorkonten

Die Verantwortung zur Steuerung der Konfiguration und Funktionsweise des Verzeichnisdienstes ist nur zuverlässigen, vertrauenswürdigen Personen zu übertragen. Dieser Personenkreis muss mit den gültigen Sicherheitsrichtlinien der Institution vertraut sein und Bereitschaft demonstrieren, diese konsequent durchzusetzen.

Die Zugriffsrechte der Dienste-Administratoren sollten auf das für ihre Arbeiten notwendige Minimum reduziert und ausschließlich für Aufgaben genutzt werden, die erhöhte Rechte voraussetzen. Um die berechtigte Notwendigkeit für Personen mit Dienste-Administratorrechten sicherzustellen, ist diese in regelmäßigen Abständen zu überprüfen und bei Bedarf entsprechend anzupassen. Auch ist die Mitgliederanzahl der Administratorenkonten auf einem notwendigen Minimum zu halten. Die Benutzung ausreichend starker Passwörter für die Konten der Administratorengruppen ist zwingend erforderlich. Es sollte überlegt werden, Verfahren zur starken Authentisierung zu verwenden wie z. B. die zusätzliche Nutzung von Chipkarten zur Anmeldung am Betriebssystem.

Beschränkung der Gruppe Domänenadministratoren (DA)

Idealerweise sollte die Gruppe DA (Domänenadministratoren) sogar leer sein, um sicherzustellen, dass jede Gruppe nur genau die Rechte erhält, die sie für ihre Arbeit benötigt.

Die Administratoren des AD selbst etwa benötigen lediglich Mitgliedschaft in der Gruppe der Administratoren der entsprechenden Domäne, um volle Verwaltungsrechte auf dem AD sowie auf den DC zu erhalten. Nur wer tatsächlich mit der Verwaltung der ADS beauftragt ist, sollte DA sein.

Zusätzlich sollte für den Notfall ein Domänenadministratorkonto (z. B. der Default-DA mit einem starken Passwort) eingerichtet und sicher sowie gleichzeitig gut erreichbar hinterlegt werden für den Fall, dass keiner der DAs verfügbar ist.

Entfernung inaktiver Konten aus dem AD

Nicht mehr verwendete Konten sollten im AD deaktiviert oder gelöscht werden, damit sie nicht von Angreifern missbraucht werden können. Ist der Account deaktiviert, so fällt eine versuchte Verwendung auf und sollte geloggt und ausgewertet werden, denn ein legitimer Gebrauch sollte nun nicht mehr vorkommen.

Am sichersten funktioniert dies, wenn Konten bei Ende ihrer Verwendung in einem Prozess automatisch aus dem AD ausgetragen werden. Dies kann technisch oder organisatorisch sichergestellt werden.

Gewährleistung der Aktualität von Basisinformationen

Unter dem Begriff "Basisinformationen" werden die wichtigsten Konfigurationsparameter des Active Directory zusammengefasst. Die Basisinformationen sollten mindestens folgende Punkte beinhalten:

- Überwachungsrichtlinien
- Gruppenrichtlinienobjekte und deren Zuweisung
- bestehende Vertrauensstellungen
- Organisationseinheit der Domänencontroller und Dienst-Admins
- Inhaber der Betriebsmasterfunktionen
- Replikationstopologie
- Datenbankeigenschaften
- verwendete Service Packs und Hotfixes für Domänencontroller und Administratorarbeitsstationen und deren aktueller Systemstatus
- aktuell vorhandene Sicherungsmedien
- Überprüfung der Sicherungsmedien
- Überprüfung der aktuell benötigten Dienste-Administratorenberechtigungen

Mit Hilfe dokumentierter Basisinformationen ist eine Nachverfolgung und Überprüfung der am Active Directory durchgeführten Änderungen möglich. Die Basisinformationen sollten für alle Domänencontroller in einer Basisdatenbank zusammengefasst werden. Diese Basisdatenbank bietet zusätzlich einen Überblick der aktuell eingesetzten Komponenten. Die Zuständigkeiten für die Pflege der Basisinformationen muss geklärt werden.

APP.2.2.M7 Umsetzung sicherer Verwaltungsmethoden für Active Directory [Fachverantwortliche]

Trennung von Standard- und privilegierten Identitäten

Administratorkonten sollten nicht für die gewöhnliche tägliche Arbeit verwendet werden. Gleiches sollte gelten für Administrationssysteme, wenn hier die Möglichkeit für dedizierte Systeme besteht. Insbesondere sollte mit Administratorkonten und Administrationssystemen nicht auf das Internet zugegriffen werden.

Jeder Anwender sollte daher über ein Standard-Benutzerkonto für den allgemeinen Gebrauch verfügen. Administrative Tätigkeiten sollten mit einem gesonderten Konto erfolgen. Das Administrationskonto darf nicht für allgemeine Tätigkeiten verwendet werden.

Benannte Accounts

Jeder Account, der verwendet wird, sollte sich eindeutig einem Mitarbeiter zuordnen lassen. Das erhöht nicht nur die Verantwortlichkeit der Mitarbeiter, sondern erleichtert auch die Rückverfolgung im Fall eines Angriffs.

Beschränkung der Anmeldemöglichkeiten von Administratoren

Die Anzahl der Systeme, an denen sich Administratoren der ADS anmelden, sollte möglichst weit eingeschränkt werden. Wenn AD-Administratoren sich lediglich an den Systemen anmelden, die sie tatsächlich zu verwalten haben sowie indirekt an bestimmten wenigen Administrations-Workstations, können die Orte, an denen wertvolle Credentials abgegriffen werden, stark einschränkt werden. Server-Administratorkonten dürfen daher nicht auf Workstations verwendet werden, Domain-Administratorkonten nicht auf Workstations oder Servern. Es sollte möglichst technisch ausgeschlossen sein, dass ein privilegierter Account zur Anmeldung an einem System einer anderen Schicht genutzt wird.

Ab einem Domain Functional Level 2012 lässt sich mittels GPOs sicherstellen, dass eine interaktive Anmeldung von einer Schicht auf eine andere nicht möglich ist. Somit darf sich ein Domänen-Administrator nicht an einem System der Produktions-IT oder der Büro-IT anmelden. Ein Server-Administrator darf sich nicht an einem Domänencontroller oder einem Gerät in der Büro-IT anmelden.

Dienste- und Datenadministration

Zur Administration einer Domäne werden Verantwortlichkeiten und Aufgabenfelder in weitere Untergruppen verteilt. Da die Benutzerkonten in den Verwaltungsgruppen "Dienste-Administratoren" (verantwortlich für die Ausführung der Aufgaben, die zur Bereitstellung des Verzeichnisdienstes erforderlich sind) und "Datenadministratoren" (verantwortlich für das Verwalten der Inhalte, die in Active Directory gespeichert oder durch Active Directory geschützt werden) besonders weitreichende Zugriffsrechte haben, sind für deren Schutz entsprechende Vorkehrungen zu treffen:

Dienste-Administratorkonten

In jeder Domäne der Gesamtstruktur wird das Standardkonto "Administrator" bei der Installation angelegt. Als Standardkonto ist dieses Benutzerkonto im besonderen Maße Angriffen ausgesetzt. Da das Administrator-Konto nicht deaktiviert oder gelöscht werden kann, sollte es als Schutzmaßnahme umbenannt werden. Bei der Umbenennung ist darauf zu achten, dass auch die Beschreibung des Administrator-Kontos abgeändert wird. Nachdem das Konto umbenannt wurde, sollte anschließend ein unprivilegiertes Konto mit Namen "Administrator" eingerichtet werden, das im täglichen Betrieb nicht verwendet werden darf. Bei der Auswertung der Protokoll-Dateien kann so erkannt werden, ob es erfolgreiche oder nicht erfolgreiche Anmeldungen an dieses unprivilegierte Benutzerkonto gab. Dies würde auf einen Angriffsversuch hindeuten.

Die Anzahl der Dienste- und Datenadministratoren ist auf ein Minimum zu beschränken. Routinemäßige Administrations- und Verwaltungsaufgaben, z. B. Verwaltung der Domänen-Benutzer, die nicht die Konfiguration des Active Directory selbst betreffen, sollten nicht von Dienste-Administratoren durchgeführt werden, sondern an Datenadministratoren delegiert werden.

Die Administratorkonten sollten möglichst sparsam eingesetzt werden. Unnötige Anmeldung an der Domäne mit administrativen Rechten sollten vermieden werden. Daher sollten die Administratoren einer Institution für alltägliche, nichtadministrative Aufgaben, z. B. Informationsbeschaffung im Internet, unprivilegierte Benutzerkonten verwenden.

Die Verwaltung von Dienste-Administratorkonten darf ausschließlich von Mitgliedern der Dienste-Administratorgruppe durchgeführt werden. Insbesondere Benutzer mit weniger Privilegien, z. B. Datenadministratoren, dürfen keine Änderungen an Dienste-Administratorkonten vornehmen, da sich die weniger privilegierten Nutzer ansonsten erweiterte Rechte einräumen könnten.

Daher sollte zur Verwaltung der Dienste-Administratorkonten eine eigene Organisationseinheit, z. B. Dienst-Admins, in der Benutzerverwaltung des Active Directory angelegt werden. Die Berechtigungen für diese Unterstruktur müssen dabei wie folgt gewählt werden:

- Vererbung der Berechtigungen von übergeordneten Objekten deaktivieren
- Zugriffsberechtigungen auf die einzurichtende Organisationseinheit (inklusive untergeordnete Objekte)
    - Administratoren: Vollzugriff
    - Organisations-Admins: Vollzugriff
    - Domänen-Admins: Vollzugriff

Die Dienste-Administratorgruppen (Domänen-Admins, Organisations-Admins und Schema-Admins) werden anschließend in die neue Unterstruktur verschoben. Darüber hinaus sind die administrativen Benutzerkonten der Domänenadmins in die Organisationseinheit "Benutzer und Gruppen" und die Konten der Arbeitsstationen in die Organisationsstruktur "Administrator-Arbeitsstationen" der neuen Unterstruktur zu verschieben. Dabei ist zu beachten, dass Domänencontroller-Konten nicht verschoben werden dürfen.

Zusätzlich sollten sowohl die Protokollierung von Änderungen, Löschungen und Einrichtung von Dienste-Administratorkonten und Arbeitsstationen sowie Änderungen an den Richtlinien überwacht werden.

Da einige der vordefinierten Dienste-Administratorkonten nicht in die neu erstellte Unterstruktur verschoben werden können, müssen diese Konten gesondert geschützt werden.

Lokale Administrationskonten

Lokale Administrationskonten sollten über sichere, einzigartige Passwörter verfügen. Mit LAPS (Local Administrator Password Solution) stellt Microsoft ein kostenloses Tool bereit, mit dem solche einfach per AD automatisch generiert und verwaltete werden können, siehe Baustein SYS.1.2.2 Windows Server 2012.

AdminSDHolder

Im Active Directory werden die geschützten Dienste-Administratorkonten regelmäßig überprüft. Dabei werden die Sicherheitseinstellungen der geschützten Konten mit den Sicherheitsbeschreibungen des AdminSDHolder-Objekts (frei übersetzt "Bewahrer des Security Descriptors für Admin-Konten", im Systemcontainer "CN=AdminSDHolder, CN=System, DC=Domänen-name") überschrieben. Der entsprechende Prozess, mit dessen Hilfe das Überschreiben angestoßen wird, startet nach fest vorgegebenen Intervallen (standardmäßig jede Stunde).

Dieser Mechanismus galt auf Windows Server 2000-Systemen für die Benutzergruppen "Administratoren", "Domänen-Admins", "Organisations-Admins" und "Schema-Admins". In der Betriebssystemversion Windows Server 2003 wurde der Mechanismus auf die Gruppen "Serveroperatoren", "Kontenoperatoren", "Sicherungsoperatoren", "Druckoperatoren" und "Zertifikat-Herausgeber" erweitert.

Folgende Berechtigungen sollten für das AdminSDHolder-Objekt zugelassen werden:

- Jeder
  - Kennwort ändern
- Administratoren
  - Inhalt auflisten
  - Alle Eigenschaften lesen
  - Alle Eigenschaften schreiben
  - Löschen
  - Berechtigungen lesen
  - Berechtigungen ändern
  - Besitzer ändern
  - Alle bestätigten Schreibvorgänge
  - Alle erweiterten Rechte
  - Alle untergeordneten Objekte erstellen
  - Alle untergeordneten Objekte löschen
- Authentifizierte Benutzer
  - Inhalt auflisten
  - Alle Eigenschaften lesen
  - Berechtigungen lesen
- Domänen-Admins
  - Inhalt auflisten
  - Alle Eigenschaften lesen
  - Alle Eigenschaften schreiben
  - Berechtigungen lesen
  - Berechtigungen ändern
  - Besitzer ändern
  - Alle bestätigten Schreibvorgänge
  - Alle erweiterten Rechte
  - Alle untergeordneten Objekte erstellen
  - Alle untergeordneten Objekte löschen
- Organisations-Admins
  - Inhalt auflisten
  - Alle Eigenschaften lesen
  - Alle Eigenschaften schreiben
  - Berechtigungen lesen
  - Berechtigungen ändern
  - Besitzer ändern
  - Alle bestätigten Schreibvorgänge
  - Alle erweiterten Rechte
  - Alle untergeordneten Objekte erstellen
  - Alle untergeordneten Objekte löschen
- SYSTEM
  - Vollzugriff

Personen

Die Personen der Dienste-Administratorengruppen müssen sowohl vertrauenswürdig sein als auch über ausreichend sichere Kenntnisse hinsichtlich der Active Directory-Administration verfügen. Damit eine geradlinige Umsetzung der Sicherheitsrichtlinien der Institution gewährleistet werden kann, müssen die Dienste-Administratoren mit den entsprechenden Richtlinien vertraut sein.

Die Mitgliederliste der Dienste-Administratorgruppen darf ausschließlich aus Benutzern der eigenen Active Directory-Gesamtstruktur bestehen. Wird Dienste-Administratoren aus entfernten Domänen vertraut, so vertraut die Institution automatisch auch den Sicherheitsmaßnahmen der entfernten Institution. Da diese Sicherheitsmaßnahmen in der Regel nicht beeinflusst werden können, ist für institutionsfremde Benutzer ein Benutzerkonto in der eigenen Gesamtstruktur einzurichten. Hierdurch können die Zugriffe auf die eigene Domäne besser reglementiert werden und es wird verhindert, dass Benutzer auf die Domäne zugreifen, deren Rechte aufgrund der automatischen Vertrauensregelung nicht bekannt sind.

Aufgrund der weitreichenden Berechtigungen sind Dienste-Administratorkonten bevorzugte Angriffsziele. Daher wird bei erhöhten Sicherheitsanforderungen empfohlen, die Zugehörigkeitsinformationen aller Dienste-Administratorgruppen für nicht privilegierte Benutzer zu unterbinden.

Dabei ist jedoch zu beachten, dass einige Serverapplikationen den lesenden Zugriff auf die Mitgliederliste der Dienste-Administratoren für einen störungsfreien Betrieb brauchen. Daher ist im ersten Schritt zu ermitteln, ob derartige Serveranwendungen in der Institution verwendet werden.

Die Benutzerkonten, unter denen die identifizierten Serverprozesse gestartet werden, sind in einer eigenen Gruppe, z. B. Serveranwendungen, zusammenzufassen. Anschließend werden folgende Berechtigungen in der ACL des AdminSDHolder Objekts für diese Gruppe vergeben:

- Inhalt auflisten
- Alle Eigenschaften lesen
- Berechtigungen lesen

Der Zugriff kann somit auf die authentisierten Benutzer eingegrenzt werden, die über einen lesenden Zugriff auf die Mitgliederliste verfügen müssen.

Da das Verbergen der Gruppenzugehörigkeit für Dienste-Administratorgruppen Auswirkungen auf den Betrieb haben kann, wird dringend empfohlen, die oben beschriebenen Änderungen am AdminSDHolder-Objekt im Vorfeld auf mögliche Auswirkungen zu überprüfen.

Die Mitglieder der Active Directory-Gruppe "Sicherungsoperatoren" sind als Dienstadministratoren anzusehen, da sie Systemdateien des Domänencontrollers wiederherstellen können. Die Anzahl der Mitglieder dieser Benutzergruppen sollte möglichst klein gehalten werden. Daher sind Administratoren, die für die Sicherung und Wiederherstellung von Anwendungsservern innerhalb des Active Directory verantwortlich sind, nicht in die Active Directory-Gruppe "Sicherungsoperatoren" einzutragen. Vielmehr sind die entsprechenden Benutzerkonten in den lokalen Gruppen "Sicherungsoperatoren" der Anwendungsserver einzutragen.

Die Active Directory-Gruppe "Kontenoperatoren" sollte nicht für die Datenverwaltung (z. B. Kontenverwaltung) verwendet werden, da Mitglieder die Möglichkeit haben, die eigenen Rechte auszuweiten. Aus Sicherheitsgründen sollten sich daher in der Gruppe "Kontenoperatoren" keine Mitglieder befinden.

Ähnliches gilt für die Active Directory-Gruppe "Schema-Admins". Da Änderungen am Schema des Active Directory normalerweise sehr selten sind, sollten vertrauenswürdige Administratoren nur solange zur Gruppe "Schema-Admins" hinzugefügt werden, wie die Berechtigungen auch tatsächlich benötigt werden. Sobald die Änderungen am Schema erfolgt sind, sollten die Mitglieder wieder aus der Gruppe entfernt werden.

Die Benutzerkonten der Gruppen "Organisations-Admins" und "Domänen-Admins" in der Stammdomäne der Active-Directory-Gesamtstruktur einer Institution sind aufgrund der weitreichenden Berechtigungen besonders zu schützen. Daher sollten jedem dieser Konten zwei Administratoren zugewiesen und das Passwort in zwei Hälften geteilt werden. Jedem der beiden Administratoren darf jeweils nur eine Hälfte des Passworts bekannt sein, damit innerhalb des Benutzerkontos nur unter Beachtung des Vier-Augen-Prinzips gearbeitet werden kann. So kann die unbemerkte Nutzung von Dienste-Administratorkonten der Stammdomäne in der Gesamtstruktur des Active Directory vermieden werden.

Alternative Methoden zur Durchsetzung des Vier-Augen-Prinzips wie z. B. die Verwendung von Chipkarten, wobei PIN und Chipkarte voneinander getrennt werden, sind ebenfalls denkbar.

Neben der Absicherung der Dienste- und Datenadministratorkonten sind außerdem die Arbeitsplätze der Administratoren wie folgt abzusichern:

- Die Benutzerkonten der Administratoren sollten so eingerichtet werden, dass die Konten nur von bestimmten Arbeitsplätzen aus verwendet werden können. Kompromittierte Administratorkonten können so nur noch von bestimmten Arbeitsstationen aus verwendet werden.
- Nach 5 Minuten Inaktivität durch den Benutzer ist die automatische Sperrung zu aktivieren. Dabei ist darauf zu achten, dass zur Aufhebung der Konsolensperrung keine zwischengespeicherten Daten verwendet werden dürfen, sondern zwingend eine erneute Authentisierung am Domänencontroller erfolgen muss. Dazu muss der Wert des Registrierungsschlüssels ForceUnlockLogon im Verzeichnis HKLM\Software\Microsoft\ Windows NT\CurrentVersion\Winlogon\ auf den Wert "1" gesetzt werden.
- Auf den Arbeitsstationen der Administratoren sollten Viren-Schutzprogramme eingesetzt werden.
- Anwendungen sollten nicht im Kontext der Administratoren ausgeführt werden. Beim Hinzufügen einer neuen Arbeitstation zur Domäne ist daher darauf zu achten, dass die Domänen-Admins nicht automatisch zu der lokalen Gruppe der Administratoren der Arbeitsstation hinzugefügt werden.
- Prozesse sollten nicht mit den Berechtigungen der Domänen-Admins ausgeführt werden. Stattdessen sollte der Sicherheitskontext der lokalen Administratorgruppe der jeweiligen Arbeitsstation verwendet werden.
- Der Datenverkehr zwischen den Arbeitsstationen der Administratoren und den Domänencontrollern ist entsprechend abzusichern. Hierzu sollten die LDAP-Paketsignaturen aktiviert werden. Dafür ist der Registrierungsschlüssel LDAPClientIntegrity in dem Windows-Registry-Pfad HKLM \System\CurrentControlSet\Services\LDAP\ auf den Wert "2" zu setzen.

Für die Remoteadministration von Domänencontrollern sollten ausschließlich Protokolle verwendet werden, die eine Verschlüsselung des Datenverkehrs ermöglichen.

Datenadministratorkonten

Grundsätzlich hängen die Strukturen und Berechtigungen der Datenadministratorenkonten stark von der Struktur der jeweiligen Institution ab. Für die im Folgenden aufgeführten Aspekte ist daher zu verifizieren, ob sie sich mit den Anforderungen der Institution verbinden lassen.

Die Delegierung der Datenverwaltung erfolgt über Gruppen, denen die entsprechenden Benutzerrechte zugewiesen werden. Auf die Mitglieder dieser Gruppen werden die Gruppenrichtlinieneinstellungen angewendet. Nach diesen Schritten genügt es, für die Delegierung Benutzerkonten zu den erstellten Gruppen hinzuzufügen. Das gewährleistet größtmögliche Sicherheit und ermöglicht es den Administratoren, ihre übertragenen Aufgaben weiterhin zu erfüllen.

Der Zugriff auf die Gruppenrichtlinien ist auf vertrauenswürdige Personen einzuschränken. Benutzer, deren Konten die Erstellung und Änderung von Gruppenrichtlinieneinstellungen zulassen, können anderen Benutzerkonten über diese Richtlinien höhere Berechtigungen einräumen und müssen folglich vertrauenswürdig sein.

Datenadministratoren werden als Ersteller eines Objektes gleichzeitig auch dessen Besitzer. Im Zugriffssteuerungsmodell von Windows Server verfügt der Besitzer eines Objektes über Vollzugriff auf dieses Objekt. Dazu gehört auch die Möglichkeit, die ACL des Objektes zu ändern. Der Besitzer eines Objektes verfügt außerdem über Vollzugriff auf alle untergeordneten Objekte. Er hat des Weiteren die Möglichkeit, die ACL-Vererbung von übergeordneten Objekten zu sperren und den Zugriff von Dienste-Administratoren auf dieses Objekt zu blockieren.

Es ist sicherzustellen, dass die Gruppen "Administratoren" bzw. "Domänenadministratoren" in den einzelnen Domänen Besitzer des Domänenstammobjektes für die jeweilige Domänenpartition sind. Die Besitzer dieser Partitionsstammobjekte können über vererbliche Access Control Entries (ACEs) die Sicherheitseinstellungen aller anderen Objekte in dieser Partition ändern.

Es ist sicherzustellen, dass bei der Planung von Kontenverwaltungsaufgaben die Gruppenzugehörigkeit in einem delegierten Bereich von einem einzigen Datenadministrator geändert wird oder aber die Aufgabe unter Abstimmung weniger Datenadministratoren erfolgt. Falls im Rahmen der Replikation ein Konflikt zwischen zwei gleichzeitigen Änderungen der Gruppenzugehörigkeit durch verschiedene Domänencontroller festgestellt wird, hat die aktuellste Änderung an einem Konto Vorrang. Bis zur Serverrepliktation ist die auf dem jeweiligen Server eingerichtete Änderung gültig.

Der Einsatz von domänenlokalen Gruppen für die Steuerung der Leseberechtigung für Objektattribute, die in den globalen Katalog repliziert werden, sollte vermieden werden, da hierbei fälschlicherweise der Objektzugriff verweigert oder gewährt werden könnte. Um dennoch Zugriffe auf die Daten des globalen Katalogs zu steuern, sollten stattdessen globale oder universelle Gruppen verwendet werden.

Papierkorb

Bis Windows Server 2008 mussten versehentlich gelöscht AD-Objekte oder solche, die absichtlich gelöscht, aber trotzdem später wieder benötigt wurden, aufwändig und fehleranfällig aus Backups wiederhergestellt werden. In Windows Server 2008 R2 wurde ein Papierkorb (Trash Bin) eingeführt, der jedoch nur von der Kommandozeile aus bedient werden konnte. Erst seit Windows Server 2012 existiert ein einfach zu verwendender Papierkorb, der sowohl von der Kommandozeile per PowerShell als auch per GUI bedient werden kann.

Der Papierkorb ist standardmäßig deaktiviert. Er sollte aktiviert werden, um den Verlust von AD-Objekten zu verhindern. Einmal aktiviert, lässt sich der Papierkorb nicht mehr ausschalten. Da er Domain Functional Level Windows Server 2008 R2 verlangt, müssen alle Domänencontroller im Wald mindestens dieses Level besitzen. Mit einmal aktiviertem Papierkorb lässt sich das Functional Level daher auch nicht mehr auf ein älteres zurückrollen, sodass bei erstmaliger Aktivierung eine gründliche Planung notwendig ist. Wie alle Änderungen am AD sollte auch diese zunächst in einer Testumgebung getestet werden.

Die Aktivierung wird als Organisations-Admin oder Schema-Admin im ADAC (AD Administration Center) in der Forest Root Domain (FRD) durchgeführt. Danach sollte die Anzeige des ADAC neu geladen werden, um die Aktivierung zu prüfen. Diese muss sich nun noch durch den Wald replizieren, bis gelöschte Objekte wiederhergestellt werden können.

Enterprise Identity Management

Über eine separat zu beschaffende Enterprise Identity Management-Lösung kann insbesondere in großen Institutionen sichergestellt werden, dass die Rechte aller Anwender definierten Vorgaben entsprechen.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Active Directory".

APP.2.2.M8 Konfiguration des sicheren Kanals unter Windows

Zwischen Rechnern einer Windows-Domäne müssen administrative Daten ausgetauscht werden. So tauschen beispielsweise Domänencontroller einer Domäne Verwaltungsdaten aus. Generell werden dabei sensitive Daten transportiert, die abgesichert übertragen werden müssen. Schon unter Windows NT stand dafür der so genannte Sichere Kanal (englisch Secure Channel) zur Verfügung. Auch unter Windows ab Version 2000 wird dieser Mechanismus genutzt und muss entsprechend den Sicherheitsanforderungen und den lokalen Gegebenheiten konfiguriert werden. Hierbei werden als Sicherheitsmechanismen die Authentisierung der beiden Kommunikationspartner, Verschlüsselung zur Wahrung der Vertraulichkeit und Signaturen zur Absicherung der Integrität eingesetzt.

Die Konfiguration des sicheren Kanals erfolgt über Gruppenrichtlinien. Bei deren Konfiguration ist Folgendes zu berücksichtigen:

- Die gegenseitige Authentisierung ist immer gewährleistet, Verschlüsselung und Signatur können jedoch unabhängig voneinander gefordert werden. Unterstützt der Kommunikationspartner die geforderte Absicherung nicht, wird diese nicht eingesetzt. Die Kommunikation erfolgt dann ungesichert.
- Verschlüsselung oder Signatur können als notwendige Voraussetzung für die Kommunikationsaufnahme spezifiziert werden. Unterstützt der Kommunikationspartner die Absicherung nicht, wird keine Kommunikation aufgebaut. Dies kann zum Beispiel zur Folge haben, dass sich Clients nicht an einer Domäne anmelden können. Diese Option sollte nur aktiviert werden, wenn alle IT-Systeme einer Domäne und alle IT-Systeme aller vertrauten Domänen das Verschlüsseln und Signieren unterstützen. Dies ist ab Windows Server 2000 der Fall und sollte daher heutzutage als gegeben vorausgesetzt werden können.

Bei Windows Server (sowie Clients seit Windows XP) lauten die Einstellungen:

- Domänenmitglied: Daten des sicheren Kanals digital signieren (wenn möglich)
- Domänenmitglied: Daten des sicheren Kanals digital verschlüsseln (wenn möglich)
- Domänenmitglied: Daten des sicheren Kanals digital verschlüsseln oder signieren (immer)
- Domänenmitglied: Starker Sitzungsschlüssel erforderlich (Verschlüsselung mit 128 Bit, immer wenn Windows 2000 oder höher)
- Domänenmitglied: Änderungen von Computerkennwörtern deaktivieren
- Domänenmitglied: Maximalalter von Computerkennwörtern (Standard: 30 Tage, sollte im Normalfall nicht auf größere Werte geändert werden)

Diese Parameter finden sich unter Computerkonfiguration | Windows-Einstellungen | Sicherheitseinstellungen | Lokale Richtlinien | Sicherheitsoptionen. Alle Optionen sollten entsprechend aktiviert werden.

APP.2.2.M9 Schutz der Authentisierung beim Einsatz von Active Directory

Das Active Directory fungiert innerhalb des Netzes als zentrale Komponente. Um eine vertrauenswürdige Kommunikation zwischen den betroffenen Teilnehmern innerhalb des Netzes gewährleisten zu können, ist die Sicherheit und Zuverlässigkeit hinsichtlich der Authentisierung und Autorisierung beim Zugriff auf Netzressourcen erforderlich. Um einen möglichst hohen Schutz der Active Directory-Authentisierung zu erhalten, sollte die LAN-Manager-Authentisierung deaktiviert und der Server-Message-Block-Datenverkehr (SMB-Datenverkehr) zwischen Domänencontrollern sowie zwischen Domänencontroller und Computern der Domäne signiert werden. Ferner sollte der prä-Windows-2000-kompatible Zugriff deaktiviert, sowie die anonymen Zugriffe auf die Domänencontroller eingeschränkt werden.

Authentisierung

Ein hohes Maß an Sicherheit kann nur erreicht werden, wenn alle Domänencontroller, Mitgliedsserver und Arbeitsstationen mindestens das Authentisierungsprotokoll NTLMv2 (NT LAN Manager Version 2) unterstützen. NTLMv2 steht standardmäßig ab Windows NT 4.0 SP4 zur Verfügung. Ältere Authentisierungsprotokolle aus früheren Windows-Versionen bieten eine geringere Sicherheit. So werden beispielsweise bei dem LAN-Manager-Authentisierungsprotokoll (LM) die Kontokennwörter in einem unsicheren LM-Hashformat gespeichert. Die Kennwörter für das Windows-NT-Authentisierungsprotokoll NT LAN Manager (NTLM) und NT LAN Manager Version 2 (NTLMv2) werden im NTLM-Hashformat abgelegt. Der NTLM-Hash ist kryptografisch stärker als das LM-Hashformat.

Unsichere Legacy-Authentisierung per LM und NTLMv1 sollte dringend per GPO verboten werden. Falls wegen des Einsatzes von Legacy-Systemen noch nicht möglich, so muss die Umstellung auf NTLMv2 oder (da auch in NTLMv2 Schwachstellen in Bezug auf Replay-Angriffe bestehen) noch besser reines Kerberos mindestens geplant und ein Termin festgelegt werden.

Windows Server ab 2008 R2 kann unsichere Authentisierung im Netz per NTLM oder schlechter identifizieren und melden und so helfen, die Umstellung zu planen.

SMB-Signatur

Das SMB-Protokoll bildet die Grundlage für die Microsoft Datei- und Druckfreigabe sowie für viele andere Netzoperationen wie z. B. die Remoteverwaltung von Windows. Um beispielsweise Man-in-the-Middle-Angriffe zu verhindern, bei denen SMB-Pakete während der Übertragung geändert werden, unterstützt das SMB-Protokoll die digitale Signatur von SMB-Paketen.

Dafür sollten folgende vier Einstellungen unter Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options aktiviert werden:

- Microsoft Network Client: Digitally Sign Communications (Always)
- Microsoft Network Server: Digitally Sign Communications (Always)
- Microsoft Network Client: Digitally Sign Communications (If Server Agrees)
- Microsoft Network Server: Digitally Sign Communications (If Client Agrees)

APP.2.2.M10 Sicherer Einsatz von DNS für Active Directory

Eine Active Directory-Installation besteht üblicherweise aus mehreren Servern mit unterschiedlichen Verzeichnispartitionen. Damit der Zugriff sowohl für die Clients als auch der Zugriff zwischen den Servern z. B. bei der Replikation erleichtert wird, verwendet Active Directory DNS (Domain Name System) für die Suche nach Active Directory-Servern. Somit muss der DNS-Dienst als eine Grundlage des Active Directory angesehen werden.

Um die Integrität und Verfügbarkeit des Active Directory sicherzustellen, ist dafür Sorge zu tragen, dass DNS-Clientabfragen nicht durch unautorisierte Systeme im Netz fehlgeleitet werden können. In Windows-Umgebungen sollte der Schutz der DNS-Daten durch in Active Directory integrierte DNS-Zonen auf den Domänencontrollern erhöht werden. Dabei werden die zonenspezifischen DNS-Daten in dem Container "MicrosoftDNS" des Active Directory gespeichert.

Die Konfigurationsdaten für in Active Directory integrierte DNS-Zonen werden in der Windows-Registry abgelegt. Der Zugriff auf die Konfigurationsdaten sollte auf administrative Konten beschränkt werden.

Im Folgenden wird ausschließlich auf in Active Directory integrierte DNS-Zonen und damit auf die Windows Server-spezifischen Eigenschaften zur Unterstützung des sicheren Betriebs von Active Directory eingegangen. Darüber hinausgehende, allgemeine Maßnahmen zur Absicherung von DNS werden hier nicht beschrieben.

Zum Schutz der DNS-Infrastruktur sollten die DNS-Server geschützt werden sowie auf den DNS-Servern gespeicherte DNS-Daten ausreichend abgesichert werden und die Integrität der DNS-Antworten auf die Client-Anfragen bei der Übertragung gesichert werden. Wie dies umgesetzt werden kann, wird im Folgenden erläutert.

Um die Integrität der auf dem Domänencontroller zwischengespeicherten DNS-Daten zu gewährleisten, muss die Option "Zwischenspeicher vor Beschädigungen sichern" für den DNS-Server-Prozess aktiviert werden. Damit soll sichergestellt werden, dass ausschließlich autorisierte DNS-Einträge im Zwischenspeicher eingefügt werden können.

Der Zugriff auf den DNS-Dienst der Domänencontroller sollte so weit wie möglich eingeschränkt werden. Dies kann z. B. dadurch erreicht werden, dass an den Sicherheitsgateways zwischen zwei Netzsegmenten der DNS-Dienst (UDP-Port 53) eingeschränkt wird. Der DNS-Dienst muss dabei für folgende Komponenten verfügbar sein:

- zwischen den DNS-Clients und dem entsprechenden DNS-Server,
- zwischen DNS-Servern, die Zonentransfers durchführen,
- zwischen DNS-Servern, die Client-Anfragen an die entsprechenden Zonen delegieren, und den für die jeweilige Zone verantwortlichen DNS-Servern,
- zwischen DNS-Servern, die Client-Anfragen weiterleiten und den DNS-Servern der übergeordneten Hierarchieebene.

Des Weiteren sollten die Netzaktivitäten in Bezug auf DNS-Anfragen überwacht werden, da ein ungewöhnlich hohes Aufkommen an DNS-Anfragen auf einen Denial-of-Service-Angriff (DoS-Angriff) gegen einen DNS-Server und damit unter Umständen auch gegen einen Domänencontroller hindeuten kann. In diesem Falle sollte der Angreifer möglichst schnell identifiziert und entsprechende Gegenmaßnahmen eingeleitet werden (siehe auch Maßnahme Erstellung eines Notfallplans im Baustein APP.2.1 Allgemeiner Verzeichnisdienstes).

Mittels IPsec (Internet Protocol Security) kann die Vertraulichkeit, Authentizität und Integrität des IP-Datenverkehrs im Netz sichergestellt werden. Bei einem IPsec-Verbindungsaufbau authentisieren sich Client und Server gegenseitig, so dass die Authentizität der Daten vom DNS-Client überprüft werden kann.

Die Integrität der DNS-Daten bei der Übertragung kann durch IPsec bei der Verwendung von Authentication Header (AH) bzw. durch Encapsulating Security Payload (ESP) sichergestellt werden.

Im Gegensatz zum Authentication Header des IPsec wird bei der Verwendung von ESP der Datenverkehr zusätzlich verschlüsselt. Durch ESP ist ebenfalls die Vertraulichkeit der DNS-Daten sichergestellt. ESP sollte daher bevorzugt werden.

Durch die Verwendung von IPsec erhöht sich das Datenaufkommen. Daher sollte vor dem Einsatz von IPsec sichergestellt werden, dass ausreichend Ressourcen vorhanden sind, damit bei aktivierter Verschlüsselung bzw. Signierung ein ausreichender Datendurchsatz im Netz möglich ist.

Ausreichende Absicherung der gespeicherten DNS-Daten

Für den Schutz der DNS-Daten auf dem Server sollten folgende Punkte berücksichtigt werden:

- Bei Windows Server-Betriebssystemen wird ein DNS-Server mitgeliefert. Wird dieser verwendet, muss er so konfiguriert werden, dass nur Registrierungsanforderungen von autorisierten Clients der Active Directory-Gesamtstruktur verarbeitet werden. Falls er nicht verwendet wird, ist er zu deaktivieren.
- Wird ein DNS-Server eines anderen Herstellers verwendet, so ist darauf zu achten, dass dieser die sichere dynamische Aktualisierung der DNS-Daten unterstützt und entsprechend konfiguriert wurde.
- Der Zugriff von Benutzern auf die DNS-Daten im entsprechenden Active Directory-Container "MicrosoftDNS" sollte über ACLs so eingerichtet werden, dass nur Administratoren, Domänen-Administratoren, Organisations-Administratoren und DNS-Administratoren Vollzugriff auf die Domänendaten besitzen.
- Die Administration der DNS-Server und damit auch der DNS-Daten ist ebenso kritisch wie die Konfiguration des Active Directory. Daher ist bei der Vergabe der Administratorberechtigungen in gleicher Art und Weise vorzugehen wie bei der Vergabe der Berechtigungen für die Dienste-Administratorkonten (siehe APP.2.2.M2 Planung der Active Directory-Administration)
- Die Informationen sekundärer DNS-Zonen werden auf einem Domänencontroller nicht im Active Directory, sondern in einer textbasierten Zonendatei gespeichert. Wenn möglich sollte auf eine verteilte DNS-Struktur zurückgegriffen werden, bei der jeder DNS-Server nur eine Zone verwaltet und entsprechende Client-Anfragen von den anderen Servern an den verantwortlichen DNS-Server weitergeleitet werden. Können sekundäre DNS-Zonen auf diese Weise nicht vermieden werden, z. B. aufgrund des erhöhten Datenvolumens, so muss die Zonen-Datei mittels NTFS-Berechtigungen vor unbefugten Zugriffen geschützt werden. Lediglich die allgemeinen Administratoren, Domänen-Administratoren, Organisations-Administratoren und DNS-Administratoren sollten Vollzugriff auf die sekundären Domänen-Daten erhalten.

Weiterführende Informationen zur Konfiguration von DNS-Servern finden sich online im Dokument "Securing the DNS Server Service" im Microsoft TechNet.

APP.2.2.M11 Überwachung der Active Directory-Infrastruktur

Der Sicherheitsstatus der Active Directory Infrastruktur wird über die Protokollierung der systemeigenen Ereignisse überwacht und bewertet. Die Protokolltiefe ist den jeweiligen Anforderungen anzupassen und sollte regelmäßig neu bewertet werden.

Die Protokolldaten sollten regelmäßig ausgewertet werden. Zur Kontrolle sollten sie des Weiteren zusätzlich mit einem Referenzwert verglichen werden, der sich beispielsweise aus früheren Daten ermitteln lässt.

Active Directory

Die Auswertung der bei der Überwachung erzeugten Protokolldaten kann in Abhängigkeit von deren Umfang manuell oder mit der Hilfe spezieller Überwachungssoftware erfolgen. In großen Active Directory-Strukturen kann normalerweise eine rein manuelle Auswertung der Überwachungsdaten nicht mehr realisiert werden.

Die Ergebnisse der Sicherheitsüberwachung sollten in regelmäßig erstellten Berichten zusammengefasst und ausgewertet werden, damit grundlegende Sicherheitsprobleme frühzeitig erkannt und behoben werden können.

Bei der Protokollierung können auch Sicherheitswarnungen auftreten, auf die sofort reagiert werden muss, so wie es im Notfallplan (siehe auch Baustein Notfallmanagement) der Institution vorgesehen ist.

Es können grundsätzlich zwei Methoden angewandt werden, um Änderungen an sicherheitsrelevanten Konfigurationsparametern des Domänencontrollers bzw. des Active Directory zu erkennen. Zum einen ist dies die Ereignisbenachrichtigung, zum anderen sind das Trendanalysen.

Für die Ereignisbenachrichtigung werden so genannte Schwellen- oder Grenzwerte für Änderungen von Konfigurationsparametern im Active Directory oder am Domänencontroller selbst definiert. Wird ein Konfigurationsparameter abgeändert und somit ein zuvor definierter Grenzwert überschritten, so wird dieses Ereignis vom Betriebssystem protokolliert.

Im Rahmen der Trendanalyse werden festgelegte Parameter über einen längeren Zeitraum in regelmäßigen Abständen erfasst. Werden bei der Auswertung dieser Daten extreme Änderungen bemerkt, so könnte das auf sicherheitsrelevante Vorfälle hindeuten. Wird beispielsweise der freie Festplattenspeicherplatz in regelmäßigen Abständen (z. B. alle 5 Minuten) erfasst und ein dramatischer Anstieg des Verbrauches von Festplattenspeicher bemerkt, so kann das auf einen Denial-of-Service-Angriff (DoS) gegen den Domänencontroller hinweisen.

Änderungen des Domänencontroller-Status

Änderungen an den Domänencontrollern können die Sicherheit des Active Directory beeinflussen. Daher sollten mindestens die Bereiche Verfügbarkeit und Systemressourcen der Domänencontroller überwacht werden:

Die Verfügbarkeit von Domänencontrollern kann auf verschiedene Weise überwacht werden. Denkbar ist beispielsweise der Einsatz spezieller Überwachungssoftware. Alternativ können jedoch auch regelmäßige LDAP-Anfragen an die Domänencontroller geschickt werden. Dabei kann mit dieser Methode nicht nur bestimmt werden, ob der entsprechende Domänencontroller aktiv ist (der Test-Client erhält eine Antwort), sondern zusätzlich können aus der Antwortzeit auch Rückschlüsse auf die Systemauslastung des Domänencontrollers gezogen werden.

Es ist außerdem sicherzustellen, dass Neustarts der Domänencontroller erkannt werden, da ein nicht autorisierter Neustart von Domänencontrollern auf einen Angriff hindeuten kann. Dementsprechend sind die Systemereignisprotokolle aller Domänencontroller in einer Institution auf unautorisierte Systemneustarts zu untersuchen.

Zusätzlich zur direkten Verfügbarkeit von Domänencontrollern sollten auch die Systemressourcen der Domänencontroller überwacht werden. Eine Änderung der Systemressourcen muss nicht zwangsläufig auf einen Angriff hindeuten. Vielmehr kann die Ursache auch technischer Natur sein, z. B. Fehlkonfiguration oder Verwendung veralteter Hardware bei wachsenden Active Directory-Strukturen.

Folgende Systemressourcen sollten auf allen Domänencontrollern in einer Institution überwacht werden:

- Prozentuale Prozessorauslastung (oberer Grenzwert: 80%)
- Freier Speicherplatz auf dem Datenträger mit der Active Directory-Datenbank in Prozent (unterer Grenzwert: 25%)
- Verfügbarer Arbeitsspeicher in Prozent (unterer Grenzwert: 10%)
- Bindungsdauer für LDAP-Verbindungen (Auffällig wäre eine ungewöhnlich starke Zunahme der Bindungsdauer.)
- Anzahl erfolgreicher LDAP-Verbindungen pro Sekunde (Auffällig wäre eine ungewöhnlich starke Zunahme der LDAP-Verbindungen. Der jeweilige Grenzwert hängt hierbei von dem Datenaufkommen von LDAP Verbindungen innerhalb der Institution ab.)

Änderungen im Active Directory

Werden Änderungen auf Domänenebene durchgeführt, so wirken sich diese meist auf alle Domänencontroller, Mitgliedsserver, Benutzer und Arbeitsstationen aus. Folgende Änderungen sind in diesem Zusammenhang denkbar:

- Ändern der domänenweiten Betriebsmasterfunktion
  Änderungen an den domänenweiten Betriebsmasterfunktionen wirken sich auf die gesamte Domäne aus. Zu den domänenweiten Betriebsmasterfunktionen gehört unter anderem der Emulationsmaster des Primären Domänen Controllers (PDC). Dies kann sich im Falle einer Fehlkonfiguration negativ auf das Gesamtkonstrukt der Domäne auswirken und zu weitreichenden Beeinträchtigungen innerhalb des Netzes führen. Eine im Vorfeld sorgfältig durchgeführte Planung hinsichtlich angedachter Änderungen an den Betriebsmasterfunktionen ist daher unabdingbar.
- Ändern der Vertrauensstellungen
  Zwischen unterschiedlichen Domänen einer Institution können Vertrauensbeziehungen eingerichtet werden. Änderungen an Vertrauensbeziehungen müssen unbedingt überwacht werden, damit insbesondere das Hinzufügen von Vertrauensbeziehungen und damit unter Umständen erweiterte Rechte der Domänen-Benutzer schnellstmöglich erkannt werden.
- Ändern des AdminSDHolder
  Das AdminSDHolder-Objekt wird vom primären Domänencontroller (PDC) verwendet, um die Benutzer der Dienste-Administratorgruppen und die Dienste-Administratorengruppe selbst vor nicht autorisierten Veränderungen der Berechtigungen zu schützen. Dazu sollte vom PDC stündlich überprüft werden, ob die benutzerbestimmbaren Zugriffskontrolllisten (D ACLs, Discretionary Access Control Lists) der zuvor genannten Benutzerkonten mit der DACL des AdminSDHolder-Objekt übereinstimmen. Weichen die DACLs voneinander ab, so müssen die DACLs der Benutzerkonten an die Einstellung des AdminSDHolder-Objekts angepasst werden.
- Änderungen an Gruppenrichtlinienobjekte und deren Zuweisung
  Änderungen an den Gruppenrichtlinien wie z. B. Passwortrichtlinien für Domänenbenutzer wirken sich auf die Domäne und damit auch auf alle Domänencontroller der betroffenen Domäne aus und sind daher zu überwachen Darüber hinaus sind auch die Zuweisungen von Gruppenrichtlinienobjekten zu Domänen Containern sowie von Gruppenrichtlinienobjekten zur Organisationseinheit "Domänencontroller" zu überwachen.
- Ändern der Mitgliedschaft vordefinierter Dienste-Administratorgruppen
  Das unautorisierte Hinzufügen oder Entfernen von Benutzern in vordefinierten Dienste-Administratorgruppen wie z. B. Administratoren oder Sicherungs-Operatoren kann auf einen Angriff hindeuten. Daher sind Änderungen an Mitgliedschaften von Diensteadministratorgruppen zu überwachen.
- Überwachung der Mitgliedschaft in der privilegierten Gruppen
  Die Gruppen mit administrativen Rechten in Bezug auf das AD müssen regelmäßig betrachtet werden, insbesondere wenn neue Mitglieder hinzugefügt werden. Noch effektiver ist ein System (technisch oder organisatorisch implementiert), das eine formale Bestätigung einholt, bevor ein Konto einer privilegierten Gruppe hinzugefügt wird. Dieses System kann auch Nutzer aus Gruppen ausschließen, wenn ihre Genehmigung der Mitgliedschaft abläuft
- Ändern der Überwachungsrichtlinien für eine Domäne
  Eine unautorisierte Änderung an den Überwachungsrichtlinien kann die Überwachung stören oder sogar komplett deaktivieren. Damit eine Deaktivierung der Überwachung erkannt werden kann, müssen die Überwachungsrichtlinien selbst auch überwacht werden.

Werden Änderungen durchgeführt, die sich auf die gesamte Active-Directory-Struktur, z. B. alle definierten Domänen, der Institution auswirken, so spricht man von Änderungen an der Gesamtstruktur. Änderungen an der Gesamtstruktur umfassen folgende Ereignisse:

- Änderungen an der Einstufung von Domänencontrollern
  Wird ein Domänencontroller herauf- oder herabgestuft, so wird von Änderungen an der Domänencontroller-Einstufung gesprochen.
- Änderungen am Active Directory-Schema
  Wird die Struktur der Verzeichnisdienstdatenbank verändert, z. B. bei Änderungen von Objektklassen oder Attributen innerhalb des Active Directory, so wird das Active Directory-Schema geändert.
- Änderungen der LDAP-Richtlinien
  Mit Hilfe von LDAP-Richtlinien können LDAP-Anfragen und damit ebenfalls der Zugriff auf die Active Directory-Daten per LDAP eingeschränkt werden.
- Änderungen an der Replikationstopologie zwischen Domänencontrollern
  Unter Änderungen der Replikationstopologie wird das Erstellen, Löschen und Ändern von Active Directory-Standorten, Standortverknüpfungen und Subnetzen verstanden.
- Ändern des dSHeuristic-Attributs
  Das dSHeuristic-Attribut steuert das Verhalten des Active Directory, hierüber kann z. B. die Auflistung von Objekten aktiviert oder deaktiviert werden.
- Änderungen der gesamtstrukturweiten Betriebsmasterfunktionen
  Die gesamtstrukturweiten Betriebsmasterfunktionen werden historisch auch als Flexible oder Floating Single Master Operations (FSMO) bezeichnet. Zu den FSMO zählen die Schemamaster- und die Domänen-Master-Funktion.

Alle zuvor genannten Änderungsereignisse, sowohl auf Ebene einzelner Domänen als auch in Bezug auf die Gesamtstruktur, sollten auf allen Domänencontrollern einer Institution überwacht und ausgewertet werden. Wird bei der Auswertung der Sicherheitsüberwachungsprotokolle eines Domänencontroller eine nicht autorisierte Änderung festgestellt, so sind entsprechende Notfallmaßnahmen einzuleiten, die im Vorfeld geplant sein müssen.

Bei einigen Ereignissen ist aus den Protokolldateien nicht ersichtlich, welche Objekte oder Attribute geändert wurden. Daher ist das Schema des Active Directory zu dokumentieren, damit Änderungen später gegebenenfalls durch manuellen Abgleich identifiziert und behoben werden können.

Kann die vollständige Behebung unautorisierter Änderungen im Active Directory nicht sichergestellt werden, so ist die Wiederherstellung der Gesamtstruktur in Erwägung zu ziehen.

In der Gruppe "Dienst-Admins" ist die Erstellung, Löschung und Änderung von Benutzerkonten in der Dienste-Administratorgruppe zu überwachen. Darüber hinaus sollte ein Hinzufügen oder Löschen von Administratorarbeitsstationen in der Organisationseinheit "Dienst-Admins" überwacht werden.

Wenn der Speicherplatz auf dem Domänencontroller für die Active Directory-Datenbank erschöpft ist, können keine neuen Objekte im Active Directory mehr angelegt werden. Daher sollte der Speicherplatz, der von Active Directory-Objekten verwendet wird, kontinuierlich überwacht werden.

Mit einer derartigen Überwachung kann nicht nur der zur Neige gehende Speicherplatz für die Active Directory-Datenbank verfolgt werden, sondern es können auch Objektüberflutungsangriffe erkannt werden, bei denen der Speicherplatzbedarf in vergleichsweise kurzer Zeit dramatisch ansteigt.

Für ein schnelles Eingreifen bei einem Objektüberflutungsangriff kann auf den Domänencontrollern eine Reservedatei beliebiger Größe angelegt werden. Im Fall eines Speicherplatzangriffs kann die Reservedatei auf den betroffenen Domänencontrollern gelöscht werden, um kurzfristig freien Speicherplatz zu schaffen und so den normalen Betrieb zu sichern.

Im Nachgang müssen die unerwünschten Objekte des Angriffs im Active Directory ermittelt und entfernt werden.

Änderungen an kritischen Dateien

Sowohl auf den Domänencontrollern selbst als auch an den Administrationsarbeitsplätzen sollte eine Überwachung eingerichtet werden, mit der eine Veränderung an kritischen Dateien erkannt werden kann. Dabei sollten mindestens die Dateien überwacht werden, die zur Konfiguration des Betriebssystems und der installierten Anwendungen verwendet werden. Darüber hinaus sollten wichtige ausführbare Dateien, z. B. Administrationswerkzeuge auf den Administratorarbeitsplätzen, ebenfalls auf Änderungen überwacht werden.

Für die Überwachung der Systemkonfiguration muss zunächst eine geeignete Software ausgewählt werden. Anschließend sollte eine vertrauenswürdige Basiskonfiguration der zu überwachenden Betriebssysteme erstellt werden.

Mit Hilfe der Überwachungssoftware wird auf Basis dieser Konfiguration ein Referenzabbild erstellt, das als Grundlage für zukünftige Überprüfungen verwendet wird. In regelmäßigen Abständen ist zu überprüfen, ob sich die aktuelle Konfiguration der Domänencontroller oder Administratoren-Arbeitsplätze im Vergleich zur Referenzkonfiguration geändert hat. Werden Änderungen festgestellt, so ist der ursprüngliche Systemzustand schnellstmöglich wieder herzustellen.

APP.2.2.M12 Datensicherung für Domänen-Controller

Da Domänencontroller üblicherweise zentrale Authentisierungs- und Autorisierungsaufgaben für den Zugriff auf wichtige Ressourcen im Netz ermöglichen, führt ein Ausfall unmittelbar zu schwerwiegenden Beeinträchtigungen im Netz. Daher muss für die Datensicherung der Domänencontroller als zentrale IT-Komponenten eine geeignete Vorgehensweise festgelegt werden. Diese sollte entweder im Datensicherungskonzept der Institution oder in einer eigenständigen Datensicherungsrichtlinie dokumentiert sein. Die grundsätzliche Vorgehensweise wird im Baustein OPS.1.1.6 Datensicherung beschrieben. Darüber hinaus sind zusätzlich Domänencontroller-spezifische Besonderheiten bei der Entwicklung der Datensicherungsrichtlinie für Active Directory zu berücksichtigen. Dieses Regelwerk sollte folgende Aspekte berücksichtigen:

- Auf Domänencontrollern müssen regelmäßig und nachvollziehbar Datensicherungen durchgeführt werden.
- Es sollten für Datensicherungen keine institutionsweiten, allgemeinen Benutzerkonten verwendet werden.
- Datensicherungssysteme sollten nur an Standorten aufgestellt werden, bei denen die Sicherheit der Hardware und Medien gewährleistet ist.
- Es muss regelmäßig getestet werden, ob sich die Domänencontroller unter Verwendung der Sicherungsmedien wiederherstellen lassen.
- Ausgesonderte Datensicherungsmedien müssen vernichtet werden.

Gegenüber herkömmlichen Server-Sicherungen sollten bei Domänencontrollern die im Folgenden genannten Punkte zusätzlich betrachtet werden:

Die Wiederherstellung eines ausgefallenen Domänencontrollers wird selten unter alleiniger Zuhilfenahme von Datensicherungsmedien durchgeführt. Bewährt hat sich hierbei die Hochstufung eines Mitgliedsservers zum Domänencontroller und anschließende Replizierung der Active Directory-Daten von einem anderen Domänencontroller. Diese Methode kann allerdings nur dann verwendet werden, wenn durch den Einsatz mehrerer Domänencontroller nach dem Ausfall eines oder mehrerer Systeme noch mindestens ein gültiges Replikat des Active Directory existiert.

Existierte lediglich ein Domänencontroller oder ist nach dem Ausfall der Domänencontroller kein Active Directory-Replikat mehr verfügbar, so muss die Wiederherstellung über die Datensicherungsmedien erfolgen. Dabei ist zu beachten, dass unter Umständen Probleme wie fehlerhafte Sicherungsmedien, unvollständige Wiederherstellungsverfahren oder fehlende Verfahrenskenntnisse bei den Verantwortlichen auftreten können. Um diesen Problemen entgegenzuwirken ist sicherzustellen, dass die Administratoren mit den Wiederherstellungsverfahren für die Gesamtstruktur vertraut sind.

Auswahl kompatibler Sicherungssoftware

Werden die Metadaten der zu sichernden Dateien vom Datensicherungsprogramm nicht korrekt behandelt, so kann dies ebenso wie bei der Verwendung ungeeigneter Virenschutzprogramme zu einer erhöhten Dateireplizierung durch den File Replication Service (FRS) führen.

Ähnlich wie beim Einsatz von Virenschutz-Programmen (siehe APP.2.2.A5 Härtung des Active Directory) ist daher bei der Auswahl der Datensicherungssoftware zwingend darauf zu achten, dass die einzusetzende Software für die Datensicherung von Domänencontrollern vom Hersteller freigegeben wurde.

Besondere Sicherheitsanforderungen

Das Dienstkonto, mit dem Domänencontroller gesichert werden, muss über Dienste-Administratorrechte und damit über hohe Rechte verfügen. Um dem Missbrauch dieser Rechte vorzubeugen, sollte der Benutzerkreis, der Zugang zu diesen Konten hat, möglichst gering gehalten werden.

Daher empfiehlt es sich, für den Sicherungsagenten auf den Domänencontrollern andere Dienstkonten zu verwenden als auf den übrigen Servern der Institution. Unterschiedliche Benutzerkonten auf Domänencontrollern und anderen Servern schützen darüber hinaus den Domänencontroller zusätzlich, für den Fall, dass ein herkömmlicher Server der Institution kompromittiert wurde.

Des Weiteren sollten die Mitglieder der Gruppe "Sicherungs-Operatoren" auf Benutzer beschränkt werden, die zur Datensicherung der Systemdateien erforderlich sind. Benutzer, die für die Datensicherung von Anwendungsdaten zuständig sind, sollten nicht Mitglied der Gruppe "Sicherungs-Operatoren" des Domänencontrollers sein. Vielmehr sollten diese Benutzer als Mitglieder in der lokalen Gruppe "Sicherungs-Operatoren" des jeweiligen Anwendungsservers eingetragen werden.

Die Domänen-Gruppe "Sicherungs-Operatoren" ist standardmäßig nicht besonders geschützt. Um einen entsprechenden Schutz umzusetzen, ist der Zugriff auf das entsprechende AdminSDHolder-Objekt (Containerobjekt zur Speicherung von Berechtigungen) möglichst eng zu reglementieren (siehe APP.2.2.M7 Umsetzung sicherer Verwaltungsmethoden für Active Directory).

Es müssen in regelmäßigen Abständen Datensicherungen der Domänencontroller durchgeführt werden. Bei der Festlegung eines geeigneten Sicherungsintervalls ist zu berücksichtigen, dass zur Löschung markierte Active Directory-Objekte nicht direkt aus dem Active Directory entfernt, sondern zunächst in einen speziellen Container des Active Directory ("Gelöschte Objekte") verschoben werden. Solche zur Löschung markierten Objekte werden als veraltete oder auch als "Tombstone"-Objekte bezeichnet.

Nach einer einstellbaren Zeitdauer (Standard: 60 Tage) werden die veralteten Objekte dann endgültig gelöscht. Dieses Verfahren hat den Vorteil, dass versehentlich gelöschte Objekte innerhalb der Frist wieder aktiviert werden können. Bei der Löschung wird das Konto bzw. Objekt daher zunächst effektiv deaktiviert, so dass es nicht mehr genutzt werden kann. Stellt sich allerdings heraus, dass es voreilig gelöscht wurde, kann es schnell wiederhergestellt werden.

Um Probleme bei der Replizierung zu vermeiden, sollte darauf geachtet werden, dass die Datensicherungen so wenig wie möglich veraltete Objekte mit überschrittener Lebensdauer beinhalten. Um dies sicherzustellen, sollten die Sicherungsmedien nach circa 75% der Lebensdauer von veralteten Objekten im Rahmen der regelmäßigen Sicherung überschrieben werden. Es sollte also möglichst häufig gesichert werden, allerdings ist dabei zu empfehlen, die Backup-Medien nach 45 Tagen (bei einer Objektlebensdauer von 60 Tagen) wieder mit neuen Backups zu überschreiben, damit eine Wiederherstellung veralteter Objekte ausgeschlossen wird.

Da die Datensicherungsmedien der Domänencontroller alle Informationen der Active Directory-Datenbank beinhalten, sollten für jene die gleichen physikalischen Sicherheitsvorkehrungen getroffen werden wie sie auch für die Domänencontroller gelten. Insbesondere für die Sicherung in Niederlassungen muss überprüft werden, ob eine ausreichende Sicherheit der Sicherungshardware und -medien gewährleistet werden kann. Hierfür gibt es folgende Möglichkeiten:

- Es erfolgt keine Datensicherung der Domänencontroller in den Niederlassungen.
- Die Datensicherung in den Niederlassungen erfolgt mit Hilfe von Remote-Sicherungssystemen (Offline-Medien) in sichere Rechenzentren.
- Die Datensicherung in den Niederlassungen erfolgt mit Hilfe von lokalen Sicherungen auf Datenträgern.

Diese Optionen sind hinsichtlich des administrativen Aufwands, der Verzögerung durch die Wiederherstellung und der Sicherheitsgewährleistung zu prüfen. Der Zustand und die Tauglichkeit der Datensicherungsmedien muss in regelmäßigen Abständen geprüft werden, indem Datenwiederherstellungen durchgeführt werden.

Die vor Ort verwendeten Sicherungsmedien müssen an einer sicheren und überwachten Stelle aufbewahrt werden, um Änderungen oder Diebstähle von Daten zu verhindern. Das Medium selbst ist nur während der Sicherung und Wiederherstellung im entsprechenden Laufwerk einzusetzen. Auch sollten Verfahren erstellt werden, die Unterschriften autorisierter Administratoren vorsehen, wenn Archivsicherungsmedien zurückgeholt werden.

Auswahl der zu sichernden Domänencontroller

Sind Domänencontroller an mehreren Standorten verteilt (z. B. in Zweigniederlassungen), so sollten Datensicherungslösungen angestrebt werden, die eine angemessene Absicherung des Backup-Verfahrens und der hierfür benutzten Medien zulassen. Es ist darauf zu achten, dass standortübergreifend für alle Domänencontroller das Datensicherungskonzept angemessen umgesetzt wird. Existieren an einem Standort z. B. keine sichere Lagerungsmöglichkeiten für die Sicherungsmedien, so sollten die Sicherungsmedien an einen geeigneten Standort ausgelagert werden.

Für Niederlassungen sind Remote-Lösungen denkbar, bei denen die zu sichernden Daten an einem zentralen Standort über das Netz eingesammelt werden. Folgende Punkte sind im Rahmen einer Remote-Datensicherungslösung zu beachten:

- Die Integrität und Vertraulichkeit der Daten sind bei der Übertragung über das Netz durch geeignete Maßnahmen zu schützen, z. B. durch Verschlüsseln der zu sichernden Daten vor oder während der Übertragung.
- Es muss ausreichend Bandbreite zur Verfügung stehen, sodass weder der Betrieb noch die Datensicherung während eines Remote-Backups gestört wird.
- Wird die Datensicherung zunächst lokal in den Standorten durchgeführt und dann von einer zentralen Stelle aus die Backup-Medien eingesammelt, so ist der Zugriff entsprechend abzusichern, z. B. ist der Zugriff auf Dateifreigaben mit den lokal zwischengespeicherten Datensicherungen auf Domänenadministratoren zu beschränken.

Inkrementelle Sicherungen

Zur platzsparenden Datensicherung wird bei Systemdateien häufig auf inkrementelle Datensicherungsverfahren zurückgegriffen. Bei diesen Verfahren werden ausschließlich die Dateien gesichert, die sich seit der letzten Datensicherung geändert haben. Im Falle einer Wiederherstellung bringt dieses Verfahren jedoch auch einen erhöhten Zeitbedarf mit sich. Inkrementelle Datensicherung sollte für Domänencontroller nicht angewendet werden, auch der Hersteller rät davon ab.

Wiederherstellungsmethoden

Wenn trotzdem inkrementelle Datensicherungen angefertigt werden, werden hierbei nur die seit der letzten Komplettsicherung neu erstellten Daten gesichert. Ältere Aktualitätsstände werden nicht berücksichtigt. In Einzelfällen kann allerdings die Anforderung bestehen, ältere Aktualitätsstände wiederherzustellen und entsprechend zu replizieren, z. B. im Zuge einer Roll-Back-Aktion. Die hiervon betroffenen Daten können mit Hilfe des Kommandozeilen-Werkzeugs ntdsutil für eine Replizierung priorisiert werden. Bei der Priorisierung wird festgelegt, welche Daten aus der Sicherung wiederhergestellt bzw. welche Daten beibehalten werden sollen. Aus diesem Grund ist das Priorisieren der Daten sorgfältig durchzuführen, da es hierbei sonst zu Inkonsistenzen in der Gesamtstruktur kommen kann, z. B. dass gesperrte oder ungültige Benutzerkonten wieder verfügbar sind.

Die Datensicherung und Wiederherstellung von Domänencontrollern mittels einer Image-Erstellung wird aufgrund der auftretenden Inkonsistenz beim USN-Rollback (Update Sequence Number Rollback) nicht empfohlen.

Ausreichende Verfügbarkeit von Sicherungen

Damit die Datensicherungen im Notfall auch verfügbar sind, muss am Ende jedes Sicherungsvorganges überprüft werden, ob er fehlerfrei durchgeführt werden konnte.

In allen Domänen sollte regelmäßig eine Überprüfung der Datensicherungen durchgeführt werden, um drei Aspekte sicherzustellen:

- Es muss sichergestellt sein, dass in der betreffenden Woche ausreichend Domänencontroller erfolgreich gesichert wurden.
- Es ist sicherzustellen, dass die erstellten Sicherungsmedien deutlich mit der eindeutigen Bezeichnung des Domänencontrollers und dem Datum der Datensicherung beschriftet und anschließend sicher aufbewahrt werden. Dabei sollte die Beschriftung der Sicherungsmedien die Funktion des Domänencontrollers einschließen, um eine spätere Identifizierung zu erleichtern.
- Im Fall einer erfolglosen Datensicherung ist der Fehler schnellstmöglich zu beheben.

Dabei ist in regelmäßigen Abständen zu testen, ob sich die Datensicherungen auch wieder einspielen lassen. Erfolgreich geprüfte Backup-Medien sollten entsprechend gekennzeichnet werden. Diese Tests sind in einer gesonderten Testumgebung, die von der Produktionsumgebung getrennt ist, durchzuführen.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

APP.2.2.M13 Zwei-Faktor-Authentifizierung (CIA)

Privilegierte Konten im Bereich des AD sollten mittels Zwei-Faktor-Authentifizierung geschützt werden. Für diesen Zweck können Smartcards verwendet werden. Smartcards alleine bieten jedoch keinen Schutz vor Kompromittierung, da Smartcard-Logon-Sessions einen NTLM-Hash haben, der bei ungeeigneter Konfiguration von Angreifern ausgelesen werden und im Rahmen von Pass-the-Hash-Angriffen missbraucht werden können. Die Maßnahme ist daher mit der sicheren Konfiguration und Härtung des AD im Zusammenhang zu sehen.

APP.2.2.M14 Dedizierte privilegierte Administrationssysteme (CIA)

Es ist möglich, die Administration der Active Directory Services lediglich von besonders für diese Aufgabe bereitgestellten (also dedizierten) und besonders für diesen Zweck gehärteten Systemen aus durchzuführen und den administrativen Zugriff von allen anderen Systemen zu unterbinden. Derartige Systeme werden häufig als PAWs (Privileged Access Workstations) oder auch, so etwa bei Microsoft intern, als SAWs (Secure Admin Workstations) bezeichnet.

Empfohlene Maßnahmen zur Absicherung der PAWs umfassen die folgenden Punkte (für Details siehe die jeweiligen Clientbausteine):

- UEFI/TPM/Secure Boot/Measured Boot
- BitLocker
- Standard User Configuration
- AppLocker
- USB Media Restrictions
- Device Guard (Windows 10)
- Credential Guard (Windows 10)
- EMET (abgekündigt)
- Outbound Traffic restrictions (kein Internet)
- Inbound Traffic restrictions (Default Deny)
- Automatische Updates
- Endpoint Protection
- Known Good Media Build Process
- Rapid Build Process
- Logon Restrictions
- Microsoft Security Baselines (SCM)
- Analyse von unsigniertem Code
- OU und GPO ACL Lockdowns
- Lateral Traversal Mitigation(s)
- Nur autorisierte Verwaltungswerkzeuge

APP.2.2.M15 Trennung von Administrations- und Produktionsumgebung (CIA)

Zur Partitionierung der Benutzerdaten kann die Administrationsumgebung in einen separaten Forest ausgelagert werden. Zwischen dem Administrations- und dem Produktionsforest wird ein einseitiger Trust etabliert, so dass die Produktionsumgebung dem Administrationsforest vertraut. Diese Möglichkeit bietet einige Vorteile. So können Konten in der Administrationsumgebung als Standard-Benutzer provisioniert werden, die in der eigenen Umgebung keine besonderen Rechte haben, aber in der Produktionsumgebung hochprivilegiert sind. Weiter können so durch die selektive Authentisierung der Vertrauensstellung weitere Einschränkungen getroffen werden, welche Konten zur Anmeldung an welchen Systemen verwendet werden können.

Bei Microsoft wird das Konzept unter dem Namen "Enhanced Security Administrative Environment" (ESAE) geführt. Dies beschreibt einen Satz von Referenzimplementierungen, die auf der Grundidee der Bildung von "Tiers" (Schichten) für Workstations, Server und AD beruhen. Verschiedene Varianten nutzen unterschiedlich viele Wälder und Zusatztechnologien wie Microsoft Identity Manager (MIM) oder Privileged Access Management (PAM) für feingranulare Kontrolle von Rechten und Protokollierung privilegierter Handlungen.

Jede Institution muss sich ihr eigenes Tiering-Konzept gemäß den eigenen erhöhten Sicherheitsanforderungen erstellen und validieren.

Abstufung von Schutzschichten

Domaincontroller > Server > Workstations

Alle Systeme sollten nach drei Kategorien eingeteilt werden:

- Kritische Systeme (Domaincontroller, CA...), die Kontrolle über andere Systeme haben
- Server (Produktions-IT)
- Workstations (Office-IT)

Kein System einer unteren Schicht darf Kontrolle über ein System der darüber liegenden Schicht(en) haben.

Aufwand und Komplexität

Zu beachten ist, dass Einrichtung und Betrieb mehrerer Wälder eine hohe Komplexität und möglicherweise erhebliche Kosten mit sich bringt, da viele Systeme und Dienste mehrfach vorgehalten werden müssen. Dies betrifft nicht nur die AD-Infrastruktur selbst, sondern bei konsequenter Umsetzung der Idee auch weitere Infrastrukturkomponenten wie WSUS, Antivirus, Backup sowie Clients/Workstations.

3 Weiterführende Informationen

3.1 Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Active Directory" finden sich unter anderem in folgenden Veröffentlichungen:

[ADFS] Active Directory Federation Services

Microsoft TechNet und Faq-o-Matic, und https://msdn.microsoft.com/en-us/library/bb897402.aspxund https://www.faq-o-matic.net/2014/04/02/adfs-grundlagen-und-architektur, zuletzt abgerufen am 05.10.2018

[ADRC] Configuring Active Directory Recycle Bin (Papierkorb)

TechGenix, Februar 2015 http://techgenix.com/configuring-active-directory-recycle-bin/, zuletzt abgerufen am 05.10.2018

[ADRL] AD Reading Library

(Active Directory Security), mit weiterführender Literatur des AD Security Blogs, https://adsecurity.org/page_id=41, zuletzt abgerufen am 24.08.2018

[ESAE] Enhanced Security Administrative Environment

Microsoft TechNet https://docs.microsoft.com/de-de/windows-server/identity/securing-privileged-access/securing-privileged-access, zuletzt abgerufen am 09.08.2018

[MSAV] Empfehlung zum Virenscan auf Unternehmenscomputern, auf denen unterstütze Windows-Versionen ausgeführt werden

Microsoft, https://support.microsoft.com/de-de/help/822158/virus-scanning-recommendation-for-enterprise-computers-that-are-running-currently-supported-versions-of-windows, zuletzt abgerufen am 05.10.2018

[PAM] Privileg Access Management for Active Directory Domain Services

Microsoft, Dezember 2016, https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/privileged-identity-management-for-active-directory-domain-services, zuletzt abgerufen am 05.10.2018

[PAW] Privileged Access Workstations

Microsoft TechNet, April 2016, http://download.microsoft.com/download/9/3/9/9392A4D2-D530-4344-8447-4A7CF1C01AEE/Privileged%20Access%20Workstation_Datasheet.pdf, zuletzt abgerufen am 09.08.2018

[SYSOPS] Enhanced Security Amdinistrative Environment ESAE

4sysops, https://4sysops.com/archives/microsoft-enhanced-security-administrative-environment-esae/, zuletzt abgerufen am 05.10.2018

[TN283324] Einstiegspunkt Active Directory für Windows Server 2012 (R2)

Microsoft TechNet, https://technet.microsoft.com/en-us/library/dn283324.aspx, zuletzt abgerufen am 09.08.2018

[TN378801] Einstiegspunkt Active Directory für Windows Server 2008 R2

Microsoft TechNet, Mai 2009, https://technet.microsoft.com/en-us/library/dd378801.aspx, zuletzt abgerufen am 09.08.2018

[TN731367] Securing the DNS Server Service

Microsoft TechNet, https://technet.microsoft.com/en-us/library/cc731367.aspx, zuletzt abgerufen am 05.10.2018

[TN755321] Security Considerations for Trust

Microsoft TechNet, https://technet.microsoft.com/en-us/library/cc755321.aspx, zuletzt abgerufen am 05.10.2018

Umsetzungshinweise zum Baustein APP.2.3 OpenLDAP

1 Beschreibung

1.1 Einleitung

OpenLDAP ist ein frei verfügbarer Verzeichnisdienst, der in einem Datennetz Informationen über beliebige Objekte, beispielsweise Benutzer oder IT-Systeme, in einer definierten Art zur Verfügung stellt. Die Informationen können einfache Attribute wie die Namen oder Nummern von Objekten oder auch komplexe Formate, wie Fotos oder Zertifikate für elektronische Signaturen umfassen. Typische Einsatzgebiete sind zum Beispiel Adressbücher oder Benutzerverwaltungen.

OpenLDAP stellt eine Referenz-Implementierung für einen Server-Dienst im Rahmen des Lightweight Directory Access Protocols (LDAP) dar. Als Open-Source-Software kann OpenLDAP auf einer Vielzahl von Betriebssystemen installiert werden und gilt als einer der verbreitetsten Verzeichnisdienste. Zur Besonderheit von OpenLDAP gehören die Overlays. Overlays erweitern den Funktionsumfang von OpenLDAP um zahlreiche Funktionen und werden auch für grundlegende Funktionen, wie Protokollierung, Replikation und die Wahrung der Integrität, verwendet.

1.2 Lebenszyklus

Planung und Konzeption

Ist die allgemeine Planung des Verzeichnisdienstes abgeschlossen, müssen Teilkonzepte für den Einsatz von OpenLDAP, unter Berücksichtigung aller geltenden übergeordneten Konzepte und Richtlinien, erstellt werden. Als Einstieg empfiehlt es sich, zunächst die Einführung in OpenLDAP zu betrachten, die einen Überblick über Aufbau und Begrifflichkeiten von OpenLDAP bietet, siehe Kapitel 3.1 Wissenswertes. Die generelle Vorgehensweise und die Planung von OpenLDAP wird in APP.2.3.M1 *Planung und Auswahl von Backends und Overlays für OpenLDAP* erläutert.

Beschaffung

Nach Abschluss der konzeptionellen Planungsarbeiten muss die Integrität und Authentizität der zur Installation verwendenden Pakete (Quelltext- oder Binärpakete) überprüft werden (siehe APP.2.3.M2 *Sichere Installation von OpenLDAP*).

Umsetzung

Bevor OpenLDAP auf einem IT-System installiert wird, muss zunächst dessen Betriebssystem geeignet konfiguriert und abgesichert werden. Außerdem müssen im Rahmen der Planung ermittelte notwendige Programme zur Unterstützung installiert sein. Bei der eigentlichen Installation und der anschließenden Grundkonfiguration sind eine Reihe von Punkten zu beachten, die in APP.2.3.M2 *Sichere Installation von OpenLDAP*, APP.2.3.M3 *Sichere Konfiguration von OpenLDAP*, APP.2.3.M4 *Konfiguration der durch OpenLDAP verwendeten Datenbank*, APP.2.3.M5 *Sichere Vergabe von Zugriffsrechten auf dem OpenLDAP, APP.2.3.M6 Sichere Authentisierung gegenüber OpenLDAP,* APP.2.3.M8 *Einschränkungen von Attributen bei OpenLDAP* sowie APP.2.3.M9 *Partitionierung und Replikation bei OpenLDAP* beschrieben werden.

Die sichere Installation von OpenLDAP ist kein einmaliger Vorgang. Statt dessen sollte die Software, wie in der Maßnahme APP.2.3.M10 *Sichere Aktualisierung von OpenLDAP* beschrieben, auf einem aktuellen Stand gehalten werden.

Die Administratoren müssen für die sichere Installation und den sicheren Betrieb von OpenLDAP geschult werden. Wichtige Aspekte, die eine solche Schulung abdecken sollte, sind in APP.2.3.M7 *Schulung von Administratoren von OpenLDAP* beschrieben.

Betrieb

Im Regelbetrieb sollte eine aktuelle Dokumentation vorhanden sein. Weiterhin ist neben dem zugrunde liegenden Betriebssystem auch OpenLDAP selbst sorgfältig zu administrieren (siehe APP.2.3.M6 *Sicherer Betrieb von OpenLDAP*). Um aufkommende Probleme rechtzeitig erkennen zu können, sollte die entsprechende Maßnahme APP.2.3.M12 *Protokollierung und Überwachung von OpenLDAP* berücksichtigt werden. Zum Schutz der Vertraulichkeit und der Integrität der übermittelten Daten ist außerdem stets eine gesicherte Kommunikation zwischen dem OpenLDAP-Server und den Clients aufrecht zu erhalten (siehe APP.2.3.M6 *Sichere Authentisierung gegenüber OpenLDAP*).

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "OpenLDAP" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

APP.2.3.M1 Planung und Auswahl von Backends und Overlays für OpenLDAP [Leiter IT]

Der Einsatz von OpenLDAP in einer Institution muss sorgfältig vom Leiter-IT und den IT-Betrieb geplant werden. Die konkrete Planung hängt auch von der verwendeten Infrastruktur ab. Wenn OpenLDAP geplant wird, sind mindestens die folgenden Punkte zu berücksichtigen:

- **Einbindung in andere Anwendungen**
  OpenLDAP besitzt zahlreiche Möglichkeiten, zur Unterstützung in Betriebssysteme und andere Anwendungen eingebunden zu werden, zum Beispiel:
  Soll OpenLDAP gemeinsam mit anderen Anwendungen verwendet werden, so müssen die Planung, Konfiguration und Installation von Anwendungen und OpenLDAP unbedingt aufeinander abgestimmt werden. Im Rahmen der IT-Grundschutz-Systematik sind korrespondierende Maßnahmen parallel umzusetzen. Die "OpenLDAP Frequently Asked Questions" (siehe [OLDAPFAQ]) halten Informationen zur Anbindung an andere Anwendungen in einem eigenen Abschnitt unter Faq-O-Matic | OpenLDAP Software FAQ | Integration bereit.
  - als zentraler Verzeichnisdienst in heterogenen Netzen oder zusammen mit Active Directory mittels Samba (siehe Baustein APP.3.4 *Samba*) oder
  - zur Benutzerverwaltung in Unix- und Linux-Systemen über das Pluggable Authentication Module (PAM) und den Name Service Switch (NSS),
  - als Adressbuch und Zertifikatsverzeichnis für E-Mail-Programme wie Microsoft Outlook oder Mozilla Thunderbird (siehe Baustein APP.5.1 *Allgemeine Groupware*).
- **Auflösung von Abhängigkeiten**
  Um alle Funktionen eines Verzeichnisdienstes gemäß des LDAPv3-Standards zu erfüllen, ist OpenLDAP darauf angewiesen, Funktionen weiterer Anwendungen zu nutzen. Dies gilt insbesondere für die zur Datenhaltung verwendete BerkeleyDB, für die OpenLDAP optimiert wurde. Nur mit dieser hierarchischen Datenbank verfügt OpenLDAP über seinen vollen Funktionsumfang. Dabei ist zu beachten, dass es sich bei BerkeleyDB und OpenLDAP um zwei unabhängig voneinander entwickelte Software-Anwendungen handelt. OpenLDAP benötigt eine unterstützte Version der BerkeleyDB.
  Einen Überblick über die unterstützten oder notwendigen Versionen der BerkeleyDB gibt der Anhang "Recommended Versions" des OpenLDAP Administrator's Guide (siehe [OLDAPGUIDE]). Der Anhang gibt auch Auskunft über weitere Softwarepakete, von denen die Funktion von OpenLDAP abhängt. Deren Anforderungen sind zu beachten, besonders die Installation einer Transport Layer Security-Variante wie "OpenSSL" oder "GnuTLS" und die Installation des Simple Authentication and Security Layers "Cyrus-SASL". Die denkbare Alternative "GnuSASL" wird in der Version 2.4 noch nicht von OpenLDAP unterstützt. Ohne diese beiden unterstützenden Anwendungen kann OpenLDAP den LDAPv3-Standard nicht vollständig umsetzen. Soll die Authentisierung mit Kerberos abgesichert werden, ist eine Installation der Dienste "Heimdal Kerberos" oder "MIT Kerberos" nötig. Auf die im Anhang der Administrators Guide aufgeführte Software "TCP Wrappers" zur Absicherung der Kommunikation mit dem Verzeichnisdienst sollte zugunsten eines anderen IP-Filter-Mechanismus verzichtet werden (nähere Informationen zu Paketfiltern finden Sie im Baustein NET.3.2 *Firewall und [OLDAPGUIDE]*).
- **Auswahl der Konfigurationsmethode**
  OpenLDAP unterstützt seit der Version 2.3 zwei verschiedene Konfigurationsmethoden. Die klassische Konfiguration wird statisch in einer Konfigurationsdatei (slapd.conf) vorgenommen, die der Serverprozess "slapd" beim Start einliest. Die aktuellere Konfiguration wird auch als Online-Konfiguration bezeichnet und speichert Konfigurationseinstellungen in einem speziellen Bereich des Verzeichnisbaumes ("slapd-config"). Die Online-Konfiguration bietet mehrere Vorteile:
  - Änderungen der Online-Konfiguration erfolgen durch LDAP-Operationen und sind über eine Netzverbindung möglich, ohne Zugriff auf das Dateisystem des IT-Systems, auf dem OpenLDAP betrieben wird.
  - Die Administration ist mit einfach zu bedienenden grafischen LDAP-Clients durchführbar.
  - Einstellungen in der Online-Konfiguration können zur Laufzeit des Servers geändert werden und werden sofort wirksam, ohne dass ein Neustart des Server-Prozesses "slapd" erforderlich ist.
  - Die Konfiguration kann als Teil des Verzeichnisses auf andere Server repliziert werden, wodurch die Administration von verteilten Verzeichnisdiensten erleichtert wird. Zum Beispiel werden Änderungen von Zugriffsrechten schneller auf allen beteiligten Servern wirksam.
    Andererseits unterstützen nicht alle Backends und Overlays die Online-Konfiguration. Zudem schützt die statische Konfiguration vor unüberlegten Änderungen der Konfiguration und begrenzt die Auswirkungen von Sicherheitsvorfällen.
    Bei der Planung von OpenLDAP ist ein Konfigurationsweg auszuwählen und dann durchgehend beizubehalten. Die Online-Konfiguration ist umso sinnvoller,
  - desto umfangreicher der Verzeichnisdienst ist,
  - desto höher seine Verfügbarkeitsanforderungen sind und
  - desto mehr Server an einem verteilten Aufbau beteiligt sind.

Aus den geplanten Nutzungsmöglichkeiten des Verzeichnisdienstes folgt, welche Backends für die spätere Installation und Konfiguration vorzusehen sind:

- Verwaltet OpenLDAP eine oder mehrere Datenbanken direkt, so ist ein Backend auszuwählen, das für eine entsprechende Datenhaltung geeignet ist. Für die Verwaltung von Daten ist OpenLDAP darauf optimiert, das Datenbankmanagementsystem (DBMS) BerkeleyDB zu verwenden. Für BerkeleyDB stehen zwei verschiedene Backends zur Verfügung: "back-bdb" und die Weiterentwicklung "back-hdb". Das Backend "back-hdb" erzeugt zwar eine höhere Last im IT-System und hat höhere Anforderungen an den für das Zwischenspeichern von Daten benötigten Datenspeicher, besitzt jedoch einen größeren Funktionsumfang und unterstützt das Umbenennen ganzer Teilbäume in der Verzeichnisstruktur (subtree renaming). Die mittelfristige Planung des OpenLDAP-Teams sieht vor, "back-bdb" aufzugeben. Für Neuinstallationen von OpenLDAP wird deshalb empfohlen, "back-hdb" zu verwenden.
  OpenLDAP kann mit dem Backend "back-ldif" Daten auch in Dateien im LDAP Data Interchange Format (LDIF) speichern. Im Format LDIF wird die gesamte Datenbank im Klartextformat in Textdateien abgelegt. Diese Art der Datenhaltung ist ineffizient für größere Datenmengen und für eine große Zahl von Benutzern ungeeignet. Wird die Online-Konfiguration verwendet, so ist dennoch "back-ldif" notwendig, da das Suffix "CN=config" immer im Format LDIF abgelegt wird.

- OpenLDAP kann ganz oder teilweise als Proxy für andere LDAP-Server eingesetzt werden. In diesem Fall wird das Backend "back-ldap" oder die Weiterentwicklung "back-meta" benötigt. Im Gegensatz zu "back-ldap" ist "back-meta" in der Lage, gleichzeitig verschiedene Server anzusprechen. Das Backend hat einen größeren Funktionsumfang als "back-ldap", ist dafür allerdings auch sehr aufwändig zu konfigurieren. Für die meisten Anwendungsfälle ist "back-ldap" ausreichend.
  Das Backend "back-ldap" wird auch immer dann benötigt, wenn der slapd-Server selbst ldap-Operationen auslöst. Dies ist beispielsweise der Fall, wenn der slapd-Server Verweise eigenständig auflöst oder eine Replikation im push-Modus durchgeführt wird.
- Es ist darüber hinaus möglich, dass OpenLDAP auf Daten einer relationalen Datenbank zugreift. Hierfür wird das Backend "back-sql" verwendet. Es wird darauf hingewiesen, dass eine relationale Datenbank ungeeignet ist, um die Daten eines Verzeichnisdienstes vollständig zu speichern. Es kann lediglich sinnvoll sein, OpenLDAP an eine relationale Datenbank anzubinden, um einzelne Zusatzinformationen aus einer solchen Datenquelle auszulesen, wie eine Telefonnummer aus einer Telefonliste in einen Verzeichnisdienst, der alle Benutzer einer Institution verwaltet.
- Gegebenenfalls muss OpenLDAP Daten aus selbst entwickelten Anwendungen beziehen oder wird eingesetzt, um solche Anwendungen zu steuern. Geschieht die Kommunikation nicht über den LDAP-Standard, so ist in Abhängigkeit von der selbst erstellten Schnittstelle eines der Backends "back-perl", "back-shell" oder "back-sock" notwendig.
- Wird entschieden, dass der Betrieb von OpenLDAP überwacht werden soll (Monitoring), so stellt das Backend "back-monitor" die dafür nötigen Funktionen bereit (siehe APP.2.3.M12*Protokollierung und Überwachung von OpenLDAP (Datenschutzbeauftragte)*).

Andere als die hier genannten Backends sollten nicht in der Planung für Produktionsumgebungen berücksichtigt werden. Sie sind entweder veraltet (back-ldbm, back-tcl), nur für Testzwecke gedacht (back-passwd, back-null) oder haben in der OpenLDAP-Version 2.4 noch einen experimentellen Status (back-dnssrv, back-ndb, back-relay).

APP.2.3.M2 Sichere Installation von OpenLDAP

Bei der Installation von OpenLDAP sind verschiedene Aspekte zu berücksichtigen, die direkten Einfluss auf die Sicherheit haben. Diese Maßnahme kann lediglich Hinweise auf besonders zu beachtende Punkte geben. Sie bezieht sich auf die Installation von OpenLDAP aus dem Quelltext. Binärpakete von Betriebssystemherstellern oder Distributoren können davon abweichen, so lösen diese in der Regel die Abhängigkeiten zu anderen Anwendungen selbstständig auf. Die mit OpenLDAP gelieferte Dokumentation, insbesondere die Manpages und die "help"-Ausgabe des Skripts "configure" liefern weitere Informationen.

Absicherung des Servers

Auch der Server, auf dem OpenLDAP betrieben wird, sollte nach IT-Grundschutz abgesichert werden. Die mit OpenLDAP verarbeiteten Verzeichnisdienstinhalte müssen auf einem lokalen Speichermedium unter Kontrolle des Serverbetriebssystems gespeichert werden, denn auf einem verteilten Dateisystem wie NFS (Network File System) stehen einige, für OpenLDAP notwendige Funktionen nicht zur Verfügung. Auf dem Server muss der Port 389 erreichbar sein. Wird "ldaps://" verwendet (siehe *APP.2.3.M6 Sichere Authentisierung gegenüber OpenLDAP*), muss der Port 636 ebenfalls geöffnet werden. Andere Dienste sollten auf dem Server nicht betrieben werden (siehe Baustein SYS.1.1 *Allgemeiner Server*).

Weitere Software-Produkte

Bei der Installation von OpenLDAP ist zu überprüfen, ob alle im Rahmen der Planung (siehe APP.2.3.M1 *Planung und Auswahl von Backends und Overlays für OpenLDAP*) identifizierten weiteren Anwendungen in einer kompatiblen Version installiert sind. Dies gilt insbesondere für die BerkeleyDB. Ist diese bereits installiert, kann die Version am Eintrag DB_VERSION_STRING der Datei "db.h" abgelesen werden. Der Speicherort dieser Datei hängt von der Installation der BerkeleyDB ab, üblich sind auf einem Unix- oder Linux-System /usr/include/db.h, /usr/local/include/db.h und /usr/local/BerkeleyDB/include/db.h. Wird eine Betriebssystem-Distribution verwendet, kann die Version auch im Paketmanager abgefragt werden.

Sind noch weitere Anwendungen zu installieren, kann die Reihenfolge der Installationen wichtig sein, damit für eine Anwendung jeweils alle benötigten Header-Informationen gefunden werden. Eine sinnvolle Installationsreihenfolge ist beispielsweise:

1. OpenSSL oder GnuTLS
2. BerkeleyDB
3. Heimdal Kerberos oder MIT Kerberos
4. Cyrus-SASL
5. OpenLDAP
6. Heimdal Kerberos (sofern schon in Schritt 3 verwendet)
7. Cyrus-SASL

Die zweifache Installation von Heimdal Kerberos (nicht MIT Kerberos) und Cyrus-SASL vor und nach OpenLDAP kann sinnvoll sein, da diese Programme dann wiederum in OpenLDAP Benutzerdaten hinterlegen können.

Übersetzung und Installation von OpenLDAP

Die Version der Software muss vor der Installation sorgfältig ausgewählt und deren Integrität überprüft werden.

Ein Quelltextpaket sollte unter einem unprivilegierten Benutzeraccount entpackt und mit Hilfe des Skripts "configure" konfiguriert werden. Nicht genutzte Backends und Overlays müssen durch Konfigurationsparameter von der Installation ausgeschlossen werden, da sie wie jede installierte Software die Gefahr von Schwachstellen und Fehlkonfigurationen bergen. Zu beachten ist weiter, dass die Parameter bei der Installation bzw. beim configure-Skript Auswirkungen auf die zu verwendende Konfiguration haben. Beispielsweise können Backends und Overlays fest einkompiliert oder als Module dynamisch geladen werden. Wird das dynamische Laden aktiviert, kann OpenLDAP nicht ohne Weiteres mit einer Konfiguration eingesetzt werden, die fest einkompilierte Backends und Overlays erwartet.

Nachdem das Paket konfiguriert wurde, sind mit dem Programmaufruf "make depend" Abhängigkeiten zu den oben vorbereiteten Anwendungen einzufügen, bevor OpenLDAP mit dem Programmaufruf "make" übersetzt wird. Die übersetzte Software sollte wegen der beschriebenen Abhängigkeiten mittels "make test" geprüft werden. Erst der letzte Schritt, die eigentliche Installation des übersetzten Programms mit "make install", muss gegebenenfalls mit höheren Privilegien erfolgen. Hat der unprivilegierte Benutzeraccount Schreibberechtigungen für sämtliche Zielverzeichnisse der Installation, so kann selbst dieser letzte Schritt ohne root-Berechtigungen durchgeführt werden. Dadurch wird die Sicherheit bei der Installation erhöht, da ein gegebenenfalls fehlerhaftes oder manipuliertes Programm auf diese Weise nur eingeschränkte Rechte erhält.

Wird OpenLDAP aus dem Quelltext übersetzt, müssen die gewählten Parameter genau dokumentiert werden. Zudem empfiehlt es sich, ein Protokoll der Ausgaben des Konfigurations- und Übersetzungslaufs (beispielsweise, indem Ausgaben in eine Datei umgeleitet werden) anzufertigen und aufzubewahren. Alle Installationsschritte sollten dokumentiert werden, damit sie sich im Notfall schnell reproduzieren lassen. Dies betrifft neben den Einstellungen beim Übersetzen auch Installationspfade, Berechtigungen, Änderungen an der Konfiguration und ähnliche Informationen.

Der Start des slapd-Servers sollte im Allgemeinen aus den Startup-Skripten des Betriebssystems erfolgen. So ist der slapd-Server nach einem Neustart des Servers sofort verfügbar und es ist sichergestellt, dass beispielsweise keine Parameter beim Starten des Servers vergessen werden.

In Abhängigkeit von der verwendeten Infrastruktur ist zu entscheiden, ob OpenLDAP aus einem Quelltext- oder Binärpaket installiert wird. Wird eine Betriebssystemdistribution eingesetzt, ist darin oft auch OpenLDAP als Binärpaket enthalten. Dies bietet den Vorteil, dass Abhängigkeiten zu anderen Softwarepaketen meist automatisch aufgelöst und zusätzlich benötigte Pakete nachinstalliert werden. In jedem Fall muss eine geeignete aktuelle Version ausgewählt, beschafft und deren Authentizität überprüft werden (siehe auch Baustein OPS.1.1.3 *Patch- und Änderungsmanagement*). Die Auswahl und Herkunft der zu installierenden Software sollte ebenso wie der Prozess der Integritätsprüfung der Software dokumentiert werden.

Grundsätzliches zur Auswahl der Version

Die Entwickler von OpenLDAP stellen den aktuellen Quelltext und Zwischenversionen der Software regelmäßig über eine Versionsverwaltung zur Verfügung. Aus dieser Versionsverwaltung kann jederzeit die aktuellste Version aller Dateien bezogen werden (Head-Branch).

In unregelmäßigen Abständen wird ein erreichter Entwicklungsstand von der weiteren Entwicklung separiert, das heißt, diesem werden bewusst keine neuen Funktionen mehr hinzugefügt (Feature Freeze). Dieser Software-Stand wird bereinigt, getestet und als Release (Veröffentlichung) veröffentlicht. Ein Release erhält eine Versionsnummer in der Form [Software-Generation].[Hauptversion].[Release-Nr.], wie beispielsweise 2.4.23.

OpenLDAP ist als Open Source Software für zahlreiche Betriebssysteme und in zahlreichen Umgebungen nutzbar. Es ist nicht möglich, dass ein Release von den Entwicklern von OpenLDAP in allen möglichen Konstellationen und für alle möglichen Einsatzzwecke getestet wird. Allerdings werten die Entwickler von OpenLDAP die Rückmeldungen von Anwendern und professionellen Distributoren zu einem Release sorgfältig aus. Werden Probleme aufgedeckt, wird in der Regel ein neues Release bereitgestellt. Wird ein Release über einen hinreichend langen Zeitraum von erfahrenen Anwendern und Distributoren verwendet und treten dabei keine Probleme auf, so wird das Release von den OpenLDAP-Entwicklern zum Stable Release (stabile Veröffentlichung) erklärt. Über Releases informieren die OpenLDAP-Entwickler mit der Mailingliste "openldap-announce" (siehe [OLDAPLIST]). Die Liste sollte zur Überwachung der OpenLDAP-Entwicklung abonniert und die erhaltenen Nachrichten archiviert werden.

Installation aus einem Quelltextpaket

Auf der Internetseite von OpenLDAP [OPENLDAP] wird auf mehrere weltweit verteilte Server verwiesen, von denen die aktuelle Release und Stable Release Versionen heruntergeladen werden können. Über einen FTP-Server werden auch ältere Software-Versionen zum Download bereitgestellt. Durch das Versionsverwaltungssystem sind zudem der aktuelle Entwicklungsstand und Zwischenversionen, die keinem Release entsprechen, verfügbar. In Produktionsumgebungen dürfen ausschließlich Releases oder Stable Releases eingesetzt werden. Es wird empfohlen, den aktuellsten Stable Release zu verwenden. Keinesfalls dürfen der aktuelle Entwicklungsstand oder eine andere, nicht für den Betrieb empfohlene Version eingesetzt werden.

Die Entwickler von OpenLDAP verwenden **keine** digitalen Signaturen, um die Quelltextpakete abzusichern. Allerdings werden von der komprimierten Version des Quelltextes eines Releases (Datei mit der Endung "tgz") die Hashwerte mit den Verfahren MD5 und SHA1 berechnet und in der zugehörigen Nachricht zum Release über die Mailingliste openldap-announce mitgeteilt. Vor der Installation eines Paketes sollten möglichst beide Hashwerte erstellt und mit den erwarteten Werten abgeglichen werden. Wird nur ein Hashwert berechnet, ist SHA1 zu bevorzugen, da das Verfahren sicherer ist. Die Software und die Information über den Hashwert dürfen nicht zeitgleich vom gleichen Server heruntergeladen werden. Statt dessen sind die Hashwerte aus der Mailingliste openldap-announce zur Prüfung zu verwenden.

Installation aus Binärpaketen der Distribution

Wird OpenLDAP aus den offiziellen Installationsquellen der verwendeten Distribution installiert, so ergibt sich die einzusetzende Version in der Regel aus dem Angebot des Distributors. Wird ein Paketmanager (zum Beispiel yum oder rpm) eingesetzt, so stellt dieser auch die Authentizität und Integrität der Pakete sicher.

Installation aus Binärpaketen fremder Quellen

Werden Binärpakete aus Installationsquellen bezogen, die nicht Teil der eingesetzten Distribution sind, so muss sichergestellt werden, dass es sich um einen vertrauenswürdigen Anbieter handelt. Bei OpenLDAP gilt dies insbesondere für Windows-Installationspakete, die von Software-Portalen zum Download angeboten werden, aber nicht von den Entwicklern von OpenLDAP erstellt wurden. Die Auswahl der Version sowie die Überprüfung der Authentizität der Binärpakete erfolgen sukzessive, wie im Abschnitt "Installation aus einem Quelltextpaket" oder im Abschnitt "Installation aus Binärpaketen der Distribution" beschrieben.

APP.2.3.M3 Sichere Konfiguration von OpenLDAP

In dieser Maßnahme wird beschrieben, wie der slapd-Server korrekt konfiguriert wird, damit er die ihm zugedachten Aufgaben sicher erfüllt. Um die Sicherheit der Daten eines Verzeichnisdienstes zu gewährleisten, sind auch die verwendeten Client-Anwendungen sicher zu konfigurieren. Dies können, müssen aber nicht, die ldap*-Werkzeuge von OpenLDAP sein. Auf die Vielfalt der verfügbaren Werkzeuge kann in dem IT-Grundschutz-Kompendium nicht eingegangen werden. Umso wichtiger ist es, den slapd-Server sicher zu konfigurieren, um sich nicht auf die Sicherheitseinstellungen der verwendeten Clients verlassen zu müssen.

Verschiedene Konfigurationswege

Bei OpenLDAP bestehen seit der Version 2.3 zwei verschiedene Wege, um den slapd-Server zu konfigurieren. Der klassische Weg ist, alle Einstellungen in die Datei "slapd.conf" einzutragen. Die Datei wird von OpenLDAP auf Unix- und Linux-Systemen unter usr/local/etc/openldap/slapd.conf abgelegt, kann sich aber auch an anderen Orten befinden, beispielsweise wenn distributionsspezifische Installationspakete verwendet werden. In OpenLDAP 2.3 ist zusätzlich das "slapd-config" Format eingeführt worden. Hierbei handelt es sich um eine hierarchische Datenbank, die unterhalb von /usr/local/etc/openldap/slapd.d bzw. an einem distributionsspezifischen Ort in Form von LDIF-Dateien gespeichert wird.

Der wesentliche Vorteil von "slapd-config" gegenüber "slapd.conf" ist die Möglichkeit, die Konfiguration zur Laufzeit zu verändern, während der slapd-Server bei jeder Änderung in der slapd.conf neu gestartet werden muss. Im Zusammenhang mit der Datenbank "slapd-config" wird deshalb auch von der Online-Konfiguration oder seltener von der RunTimeConfiguration (RTC) gesprochen. Die Online-Konfiguration ist mit dem fest eingestellten Suffix "CN=config" Teil des Verzeichnisbaums im slapd-Server. Bei der Planung ist der Konfigurationsweg auszuwählen und dann beizubehalten. Es ist ferner zu beachten, dass die in der Datei "slapd.conf" sichtbaren Einstellungen nicht gültig sind, wenn die Datenbank "slapd-config" verwendet wird.

Benutzerrechte auf Betriebssystemebene

Während Änderungen der "slapd.conf" umgesetzt werden, indem die Datei editiert wird, sind Änderungen der Online-Konfiguration über Änderungsbefehle im Rahmen des Protokolls LDAP zu initiieren. Daraus folgt, dass ein Administrator bei der Konfiguration via "slapd.conf" Zugriff auf das Dateisystem des IT-Systems benötigt, auf dem der slapd-Server betrieben wird. Dem Systembenutzer, in dessen Kontext der slapd-Server läuft, sollten dagegen nur Leserechte auf die Datei gewährt werden. Für die Konfiguration mittels der Datenbank "slapd-config" ist ein Benutzeraccount im Verzeichnisdienst ausreichend, allerdings muss der Systembenutzer, in dessen Kontext der slapd-Server ausgeführt wird, für das Datenbankverzeichnis schreibberechtigt sein. Wurde OpenLDAP mit root-Berechtigungen installiert und eingerichtet, sind anschließend die Berechtigungen auf das Verzeichnis oftmals falsch gesetzt. Dies kann zur falschen Einschätzung führen, dass der Betrieb des slapd-Servers root-Berechtigungen erfordern würde.

Aufbau der Konfiguration

Die Konfigurationseinstellungen werden in OpenLDAP als Direktiven bezeichnet. Es gibt globale Direktiven, Backend-Direktiven und Datenbank-Direktiven. Die globalen Direktiven werden in Abgrenzung zu den Backends und Datenbanken gelegentlich auch als Frontend-Direktiven bezeichnet. Die Direktiven bauen hierarchisch aufeinander auf: Globale bzw. Frontend-Direktiven können von Backend-Direktiven verdrängt werden und diese wiederum von Datenbank-Direktiven. Direktiven haben teilweise Sub-Direktiven, in denen weitere Einstellungen zur jeweiligen Direktive vorgenommen werden. Dies ist insbesondere bei Backends und Overlays der Fall, die durch eine Direktive aufgerufen und durch Sub-Direktiven konfiguriert werden.

Umwandlung von slapd.conf in slapd-config

Zwischen den Direktiven beider Konfigurationswege besteht eine eindeutige Beziehung, wobei dem jeweiligen Attribut in der Datenbank "slapd-config" in der Regel die Buchstaben "olc" vorangestellt sind (für Online Configuration). So entspricht "backend" in der "slapd.conf" dem Ausdruck "olcBackend" in der Datenbank "slapd-config". Jedes slap*-Werkzeug von OpenLDAP ist in der Lage, eine klassische Konfiguration in eine Online-Konfiguration umzuwandeln, indem mit dem Parameter "-f" die Position von "slapd.conf" angegeben wird und mit dem Parameter "-F" das Zielverzeichnis von der Datenbank "slapd-config". Ein Beispiel ist: slaptest -f /usr/local/etc/openldap/slapd.conf -F /usr/local/etc/openldap/slapd.d.

Unabhängig von der gewählten Konfigurationsmethode muss jede neue oder geänderte Konfiguration mit dem Werkzeug slaptest darauf geprüft werden, ob sie syntaktisch korrekt ist. Dies ist zu tun, bevor der slapd-Server mit der neuen Konfiguration gestartet wird. Bei Änderungen am laufenden System im Rahmen der Online-Konfiguration weist der slapd-Server unzulässige Konfigurationsänderungen ab. Wichtig ist, alle Konfigurationseinstellungen zu dokumentieren, damit sie sich im Notfall schnell reproduzieren lassen.

slapd.conf

Die Datei "slapd.conf" entspricht in ihrer Syntax dem in RFC 2849 (siehe [RFC2849]) definierten LDAP Data Interchange Format (LDIF), das die Administratoren kennen sollten. Die Konfigurationsdatei "slapd.conf" beginnt mit globalen Direktiven. Die globalen Direktiven enthalten die Schema-Spezifikationen. Da die Einbindung von Schemas in die slapd.conf sehr umfangreich werden kann, wird empfohlen, für ein Schema eine eigene lokale Datei zu erstellen und diese mit "include" in der Konfigurationsdatei "slapd.conf" aufzurufen. Auf die globalen Direktiven folgen gegebenenfalls Backend-Direktiven, sofern diese verwendet werden. Sie werden mit der Direktive "backend <typ>" eingeleitet, wobei <typ> das Backend angibt, d. h. dessen Typbezeichnung ohne das Suffix "back-". Ein Beispiel ist "backend hdb". Die dann folgenden Direktiven gelten nicht mehr global, sondern nur für alle Datenbanken dieses Typs. Datenbank-Direktiven werden mit der Direktive "database <typ>" eingeleitet, wobei <typ> analog zu den Backends den Datenbanktyp festlegt. Die folgenden Direktiven gelten dann nur für diese Datenbank. Zu beachten ist, dass der Typ einer bestehenden Datenbank nicht einfach geändert werden darf, indem der Datenbank-Aufruf angepasst wird. Dies hat keinen Einfluss auf die bestehenden Datenstrukturen, die für verschiedene Datenbanktypen unterschiedlich sein können.

slapd-config

Im Konfigurations-Teilbaum der Datenbank "slapd-config" werden globale Direktiven als Werte im Bereich "CN=config" oder in der speziellen Dummy-Datenbank "olcDatabase=frontend, CN=config" eingetragen. Schemas sind Kindelemente des Teilbaums "CN=schema, CN=config". Backends und Datenbanken sind wiederum Kindelemente von "CN=config". Die initiale Konfiguration kann erzeugt werden, indem eine bestehende Konfigurationsdatei "slapd.conf" umgewandelt wird oder indem das Suffix "CN=config" mit seinen Elementen im Format LDIF erstellt und mittels "slapadd" in den Verzeichnisdienst importiert wird. Zu beachten ist, dass die "slap-config"-Konfiguration nicht geändert werden darf, indem die LDIF-Dateien im Datenbank-Verzeichnis "slapd.d" angepasst werden. Dabei werden die als operationelle Attribute geführten Zeitstempel nicht aktualisiert. Der slapd-Server bemerkt diese Änderungen deshalb nicht und setzt sie nicht um.

Overlays

Overlays werden in der Konfigurationsdatei "slapd.conf" entweder bei den globalen Direktiven aufgerufen oder in einem Datenbank-Abschnitt. Overlays sollten erst nach allen anderen datenbankspezifischen Direktiven aufgerufen werden, um Fehlkonfigurationen zu vermeiden, bei denen Datenbank-Direktiven als Sub-Direktiven des Overlays interpretiert werden. In der Datenbank "slapd-config" sind Overlays Kindelemente von "CN=config" (für globale Overlays) oder des Datenbank-Elements (für datenbankspezifische Overlays). Da die genaue Wirkung von Overlays von der Reihenfolge ihres Aufrufs abhängen kann, sind Overlays sorgfältig in die Konfiguration einzufügen. In der Konfigurationsdatei "slapd.conf" werden die Overlays in umgekehrter Reihenfolge der Nennung innerhalb der Datei aufgerufen.

Im Folgenden werden einige grundlegende und sicherheitsspezifische Direktiven aufgeführt, deren Vorgabewerte bei der Konfiguration kontrolliert und gegebenenfalls angepasst werden sollten. Weitere Direktiven befinden sich im OpenLDAP Administrator's Guide (siehe [OLDAPGUIDE]) sowie den Manpages.

- suffix bzw. olcSuffix (Datenbank-Direktive)
- Dies ist die wichtigste Sub-Direktive eines Datenbank-Aufrufs. Mit ihr wird festgelegt, welcher Teil des Verzeichnisses in der jeweiligen Datenbank abzulegen ist, z. B. "DC=bsi, DC=bund, DC=de". Soll eine Datenbank einen untergeordneten Teilbaum aufnehmen, so muss diese Datenbank vor der übergeordneten Datenbank aufgerufen werden. Zum Beispiel muss "DC=grundschutz, DC=bsi, DC=bund, DC=de" vor "DC=bsi, DC=bund, DC=de" definiert werden, da sonst immer die übergeordnete Datenbank selektiert wird.

- include (nur slapd.conf)
- In dieser Direktive kann auf Dateien außerhalb der Konfigurationsdatei "slapd.conf" verwiesen werden, deren Inhalt dann bei der Auswertung der "slapd.conf" an die Stelle der Direktive tritt. Die Direktive wird empfohlen, um beispielsweise Schema-Definitionen und Zugriffskontrolllisten separat zu verwalten. Die Direktive kann auch in diesen externen Dateien verwendet werden. Der slapd-Server erkennt allerdings keine Ringverweise, was zum Einlesen einer scheinbar unendlich großen Konfiguration führen kann ("slapd.conf" enthält "include ACL1.conf", "ACL1.conf" enthält "include ACL2.conf", "ACL2.conf" enthält "include ACL1.conf"). In einem solchen Fall ist der slapd-Server nicht nutzbar, gegebenenfalls wird der Betrieb des kompletten IT-Systems durch den Ressourcenbedarf des slapd-Servers gestört. Es ist ebenfalls darauf zu achten, dass die für den Betrieb des slapd-Servers verwendete Benutzerkennung ein Leserecht auf die externen Dateien eingeräumt bekommt. Wenn eine "slapd.conf"-Konfiguration in eine "slapd-config"-Konfiguration umgewandelt wird, werden die über "include" eingefügten Dateien einbezogen.

- idleTimeout bzw. olcIdleTimeout (globale Direktive)
- Über diese Direktive wird ein Wert in Sekunden festgelegt, nachdem für eine ungenutzte Verbindung zu einem Client ein "unbind" erzwungen wird. Diese Direktive ist in der Voreinstellung mit 0 belegt und dadurch deaktiviert. Es wird empfohlen, hier einen Wert größer Null zu setzen, damit ungenutzte Verbindungen zu nicht ordnungsgemäß heruntergefahrenen Clients oder zu verlassenen Workstations nicht für Angriffe verwendet werden können. Der Wert sollte sorgsam festgelegt werden und die in der Institution übliche Nutzung nicht behindern. Sinnvoll ist z. B. ein Wert kleiner 900, damit ungenutzte Verbindungen nach spätestens 15 Minuten Inaktivität getrennt werden.

- referral bzw. olcReferral (globale Direktive)
- Diese Direktive benennt einen LDAP-Server, den der slapd-Server an einen anfragenden Client zurückmeldet, wenn der slapd-Server die vom Client gewünschte Operation nicht selbst durchführen kann. Die Direktive sollte mit einem übergeordneten LDAP-Server belegt werden, sofern ein solcher vorhanden ist, um die Verfügbarkeit zu verbessern. Es ist darauf zu achten, keine Ringverweise zwischen gleichberechtigten Servern einzurichten, da dies von einigen Client-Anwendungen nicht bemerkt wird.

- readonly bzw. olcReadonly (Datenbank-Direktive)
- Mit dieser Direktive wird eine Datenbank in einen Nur-Lese-Zustand versetzt.

- rootDN bzw. olcRootDN und rootPW bzw. olcRootPW (Datenbank-Direktiven)
- Über diese beiden Direktiven werden eine administrative Benutzerkennung für die jeweilige Datenbank und das zugehörige Passwort festgelegt. Limits oder Zugriffsbeschränkungen (siehe APP.2.3.M5 *Sichere Vergabe von Zugriffsrechten auf dem OpenLDAP*) haben auf diese Benutzerkennung keine Auswirkungen. Die sichere Ablage eines Passwortes, wie in der Maßnahme *APP.2.3.M6 Sichere Authentisierung gegenüber OpenLDAP* beschrieben, ist auch für das Passwort des "rootDN" durchzuführen.

- sizeLimit bzw. olcSizeLimit (globale Direktive)
- Die Direktive schränkt die Anzahl von Ergebnissen für Suchoperationen ein. Der Vorgabewert für die Direktive beträgt 500. Der Wert ist zu prüfen und gegebenenfalls anzupassen, er sollte aber nicht auf "unlimited" gesetzt werden, um Denial-of-Service-Attacken auf den Verzeichnisdienst zu erschweren und vollständige Kopien der Datenbank durch unberechtigte Benutzer zu verhindern.

- timeLimit bzw. olcTimeLimit (globale Direktive)
- Mit dieser Direktive wird die Zeit in Sekunden angegeben, bevor eine Suche abgebrochen wird. Der Vorgabewert für die Direktive beträgt 3600. Der Wert ist zu prüfen und gegebenenfalls anzupassen, er sollte aber nicht auf "unlimited" gesetzt werden, weil er sonst Denial-of-Service-Attacken auf den Verzeichnisdienst erleichtert.

- limits bzw. olcLimits (Datenbank-Direktive)
- Diese Direktive erlaubt Einschränkungen analog zu sizeLimit und timeLimit auf Datenbankebene. In diesem Fall werden globale Limits nicht beachtet. Hier sind auch Limits pro Benutzer möglich. Die Benutzerangabe erfolgt dabei analog zur Benutzerangabe im Rahmen von Zugriffskontrolllisten (siehe APP.2.3.M5 *Sichere Vergabe von Zugriffsrechten auf dem OpenLDAP*). Es wird empfohlen, benutzerspezifische Limits zu setzen, um beispielsweise nicht authentisierte Benutzer von der Erkundung der Verzeichnisstruktur abzuhalten oder Einschränkungen zu lockern, wenn sie die Replikation behindern.

Weitere Direktiven werden in anderen Maßnahmen zu OpenLDAP angesprochen, insbesondere in der Maßnahme APP.2.3.M4 *Konfiguration der durch OpenLDAP verwendeten Datenbank*.

APP.2.3.M4 Konfiguration der durch OpenLDAP verwendeten Datenbank

In OpenLDAP können durch die Konfigurationsdirektiven Einstellungen für das tatsächlich verwendete Datenbankmanagementsystem (DBMS) vorgenommen werden. Die Einstellungen sind nur für die BerkeleyDB über die Backends "back-bdb" oder "back-hdb" möglich. Sie haben keinen unmittelbaren Einfluss auf die Funktion und Bedienung von OpenLDAP, haben aber große Auswirkungen auf die Performance des Verzeichnisdienstes. Im Folgenden werden nur sicherheitsrelevante Einstellungen und häufige Fehlerquellen aufgeführt. Für weitere Einstellungen sollte gegebenenfalls ein Datenbankspezialist zurate gezogen werden. Beispielsweise ergeben sich aus den Einstellungen zur Zwischenspeicherung und Transaktionsprotokollen Geschwindigkeitsvorteile zu Lasten einer optimalen Integrität, die sorgsam im Einzelfall abzuwägen sind.

- dbDirectory bzw. olcDbDirectory
  Über die Direktive kann der Speicherort für Datenbankdateien im IT-System festgelegt werden, auf dem der slapd-Server betrieben wird. Die Benutzerkennung, in deren Kontext OpenLDAP ausgeführt wird," muss Schreibrechte auf das angegebene Verzeichnis haben.
- dbConfig bzw. olcDbConfig
  Die in dieser Direktive vorgenommenen Einstellungen sind datenbankspezifisch und werden in die Datei "DB_CONFIG" des DBMS eingetragen. Wenn eine solche Datei noch nicht existiert, wird sie durch die Nutzung dieser Direktive erstellt. Es ist zu beachten, dass spätere Änderungen in der Zieldatei selbst, beispielsweise mit einem Texteditor, die hier gewählten Einstellungen überschreiben. Deshalb muss festgelegt sein, wie und durch wen an welcher Stelle Einstellungen vorgenommen werden. Änderungen der Direktive erzwingen immer einen Neustart des DBMS, jedoch nicht des slapd-Servers. Dies kann je nach Umfang und Einstellungen der Datenbank eine längere Zeit in Anspruch nehmen, währenddessen der Verzeichnisdienst nicht verfügbar ist. Änderungen der Datenbank-Konfiguration sollten deshalb sorgfältig geplant und möglichst in Wartungsfenstern z. B. nachts oder am Wochenende umgesetzt werden.
- dbIndex bzw. olcDbIndex
  Mit dieser Direktive können Attribute von Verzeichnisdienstobjekten festgelegt werden, für die ein Index erstellt werden soll. Ohne einen Index müssen bei einer Suche sämtliche Objekte aufgerufen und geprüft werden. Um die Verfügbarkeit zu verbessern, sollten deshalb häufige Suchen durch einen Index unterstützt werden. Fehlende aber wünschenswerte Indizes können aus den OpenLDAP-Protokollen (siehe APP.2.3.M12 *Protokollierung und Überwachung von OpenLDAP (Datenschutzbeauftragte)*) erkannt werden. Erscheint dort häufig der Hinweis, dass der Zugriff auf einen bestimmten Attributsindex fehlschlug, sollte ein entsprechender Index eingerichtet werden. Die in der Direktive angegebenen Indizes werden vom slapd-Server automatisch erzeugt. Sollte der slapd-Server während des Indizierungsvorgangs gestoppt werden, so wird die Indizierung nicht automatisch fortgesetzt. In diesem Fall ist sie mit dem Werkzeug slapindex manuell durchzuführen.
- dbMode bzw. olcDbMode
  Über diese Direktive werden die Benutzerrechte festgelegt, die für neu angelegte Datenbankdateien gelten. Die Voreinstellung 0600 bzw. -rw------- gewährt lediglich der Benutzerkennung Zugriff, in deren Kontext der slapd-Server betrieben wird. Diese Voreinstellung ist sinnvoll und sollte nicht geändert werden.

APP.2.3.M5 Sichere Vergabe von Zugriffsrechten auf dem OpenLDAP

Die richtige Vergabe und korrekte Umsetzung von Zugriffsrechten sind elementare Voraussetzungen, um die Informationssicherheit zu gewährleisten. Wann immer ein Benutzer eine Operation gegen ein Objekt im Verzeichnisdienst richtet, muss entschieden werden, ob es zulässig ist, diese Operation auszuführen. Das Berechtigungskonzept und die Erstellung einer Sicherheitsrichtlinie für Verzeichnisdienste ist festzulegen (nähere Informationen finden Sie im Baustein APP.2.1 *Allgemeiner Verzeichnisdienst).* Die dort getroffenen Regelungen müssen in OpenLDAP technisch umgesetzt werden. Allgemeine Informationen zu diesem Thema finden Sie auch im Baustein APP.2.1 *Allgemeiner Verzeichnisdienst.* Der LDAP-Standard bestimmt lediglich, dass eine Zugriffskontrolle stattfinden soll und definiert im Rahmen des Standards Server-Antworten für den Fall, dass Operationen wegen unzureichender Berechtigungen abgewiesen werden. Wie eine Zugriffskontrolle jedoch konkret umzusetzen ist, wird im LDAP-Standard nicht spezifiziert und ist in hohem Maße vom eingesetzten Verzeichnisdienst abhängig. Auf die Vergabe von Zugriffsrechten in OpenLDAP wird deshalb in dieser Maßnahme umfassend eingegangen.

Zugriffskontrolllisten in OpenLDAP

In OpenLDAP werden Zugriffskontrolllisten (Access Control Lists, ACLs) in Form von Direktiven in der Konfiguration geführt. Bei jeder von einem Benutzer ausgelösten Operation wird ermittelt, ob diese durch eine Direktive gedeckt ist.

Eine Zugriffsdirektive hat folgende Syntax:

access to [Zielobjekt]

by [Benutzer] [Berechtigungsumfang]

by [Benutzer] [Berechtigungsumfang]

...

Als Zielobjekt können dabei unter anderem Suffixe, Objekte oder Attribute bestimmt werden. Sogar das Ergebnis einer LDAP-Suche oder bestimmte Attributbelegungen können hier vorgegeben werden. Dabei sind fast beliebige Detailtiefen und Kombinationen möglich, auf die hier nicht eingegangen werden kann. Besonders zu nennen ist jedoch das Zielobjekt *****, das alle möglichen Zielobjekte des Verzeichnisdienstes umfasst.

Benutzer

Als Benutzer sieht OpenLDAP unter anderem folgende Eintragungen vor:

- ***** für alle Benutzer des Verzeichnisdienstes, einschließlich nicht authentisierter Benutzer
- **anonymus** für nicht authentisierte Benutzer
- **users** für authentisierte Benutzer (für die Unterscheidung von authentisierten und nicht authentisierten Benutzern siehe *APP.2.3.M6 Sichere Authentisierung gegenüber OpenLDAP*)
- **self** für Benutzer, die einen "bind" mit der Identität des Zielobjektes vollzogen haben
- **Distinguished Names** (DNs) für voll qualifizierte Benutzer oder reguläre Ausdrücke
- **Attributsfilter**, um den Zugriff auf ein Objekt zu gewähren, bei dem der Benutzer in ein Attribut eingetragen ist, beispielsweise als Vorgesetzter einer Person
- **Gruppenattribute**, um Zugriffsrechte über statische oder dynamische Gruppenmitgliedschaften zu steuern
- **IP-Einträge** für alle Benutzer, deren Client aus einem vorgegeben IP-Adressraum oder mit einer vorgegebenen Domäne verbunden ist

Obwohl von OpenLDAP akzeptiert, sollte die Zugriffssteuerung in keinem Fall anhand der IP-Adressen vorgenommen werden, da IP-Adressen einfach gefälscht werden können.

Berechtigungsumfang

Als Berechtigungsumfang kennt OpenLDAP folgende Werte:

- **none**: keine Zugriffsberechtigung
- **disclose**: Existenzprüfung zur Fehlerverfolgung
- **auth**: Möglichkeit, einen "bind" als Zielobjekt durchzuführen
- **compare**: Durchführung von Vergleichen
- **search**: Anwendung von Suchfiltern auf das Zielobjekt
- **read**: Lesender Zugriff auf das Zielobjekt
- **write**: Schreibender Zugriff auf das Zielobjekt (ändern, umbenennen, löschen)
- **manage**: Vollzugriff einschließlich der benötigten Rechte, um auf operationelle Attribute zuzugreifen

Daneben existieren noch spezielle Berechtigungen wie "selfwrite". Diese ermöglicht es, lediglich den eigenen DN zu schreiben, beispielsweise um eigene Gruppenmitgliedschaften zu pflegen. Jeder Berechtigungsumfang enthält automatisch alle jeweils vorgenannten. So gibt eine read-Berechtigung auch die Rechte zu "disclose", "auth", "compare" und "search"-Aktionen. Dies ist in der Regel sinnvoll und die Verwendung der "access levels" ist meist ausreichend. Andernfalls können Berechtigungen über privilege-Operatoren detaillierter vergeben werden.

Mehrere "by"-Klauseln

Innerhalb einer Zugriffsdirektive können beliebig viele "by"-Klauseln aufeinander folgen. Die Auswertung innerhalb einer Direktive wird gestoppt, sobald eine zutreffende "by"-Klausel gefunden wird. Dies ist der Fall, sobald ein in der "by"-Klausel genannter Benutzer dem anfragenden Benutzer entspricht oder diesen beinhaltet. Eine klassische Zugriffsdirektive ist z. B.

access to *

by self write

by anonymus auth

by group.exact="CN=admin, ou=groups, DC=bsi, DC=bund, DC=de" write

by users read

Durch diese Direktive kann jeder Benutzer seinen eigenen Eintrag verändern, ein anonymer Benutzer kann jeden Eintrag benutzen, um sich zu authentisieren, Mitglieder der Administratorengruppe können Einträge verändern und ein authentisierter Benutzer kann alle Einträge lesen. Die letzte "by"-Klausel könnte auch "by * read" lauten und hätte den selben Effekt. Da für nicht authentisierte Benutzer bereits die zweite "by"-Klausel zutrifft, wird die vierte Klausel immer nur für authentisierte Benutzer (users) geprüft, die keine Administratoren sind. Wären die erste und vierte "by"-Klausel vertauscht, würden keine Schreibrechte auf Einträge bestehen, da die hinter der "users"-Klausel folgende "group"-Klausel sowie die "self"-Klausel nicht mehr verarbeitet würden. Trifft keine Benutzerangabe in einer Direktive auf einen anfragenden Benutzer zu, wird diesem auch keine Berechtigung gewährt. Bei der Auswertung wird jede Direktive behandelt, als würde sie mit der Klausel "by * none" abschließen, auch wenn diese nicht dort steht.

Mehrere Zugriffsdirektiven

Es können beliebig viele Zugriffsdirektiven aufeinanderfolgen. Die Direktiven werden der Reihe nach abgearbeitet. Eine ACL wird nicht weiter ausgewertet, sobald eine zutreffende Direktive gefunden wird. Eine Direktive gilt als zutreffend, wenn das angefragte Zielobjekt dem aus der Direktive entspricht oder in diesem enthalten ist. Zum Beispiel führen die Direktiven

access to dn.subtree="DC=grundschutz, DC=bsi, DC=bund, DC=de"

by users write

access to dn.subtree="DC=bsi, DC=bund, DC=de"

by users read

dazu, dass authentisierte Benutzer alle Inhalte des fiktiven Teilverzeichnisses bsi.bund.de lesen können und auf Inhalte von grundschutz.bsi.bund.de schreibend zugreifen dürfen. Wären die Direktiven in umgekehrter Reihenfolge angegeben, würde das Schreibrecht entfallen, da eine Operation mit dem Zielobjekt "DC=grundschutz" bereits eine Teilmenge von "DC=bsi, DC=bund, DC=de" ist. Trifft keine Zielobjektangabe irgendeiner Direktive auf ein angefragtes Zielobjekt zu, so wird auf das Zielobjekt auch keine Berechtigung gewährt. Jede Zugriffskontrollliste wird bei der Auswertung behandelt, als würde sie der Direktive "access to * by * none" abschließen, auch wenn diese nicht dort steht.

Reihenfolge und Control Flags

Aus diesen Beispielen wird ersichtlich, dass die Reihenfolge von ACL-Einträgen von großer Bedeutung ist. Es gilt grundsätzlich, dass spezielle Rechte zuerst und allgemeine Rechte zuletzt definiert werden müssen.

Sollte dennoch der Bedarf bestehen, die Berechtigungen weiter auszuwerten, nachdem eine zutreffende Regel gefunden wurde, kann dies durch die Steuerungsschalter ("Control Flags") "continue" (für die Prüfung weiterer "by"-Klauseln innerhalb einer Direktive) und break (für die Prüfung weiterer Direktiven) erreicht werden. Die Control Flags sollten äußerst sparsam eingesetzt werden, da sie eine Zugriffskontrollliste unübersichtlich machen. Es muss beachtet werden, dass eine weitere zutreffende Regel die schon gewährten Rechte ersetzt. Das Control Flag "continue" kann durch eine korrekte Planung der ACL eigentlich immer vermieden werden. Es wird nur benötigt, wenn die "privilege"-Operatoren eingesetzt werden.

Das Control Flag "break" ist dazu geeignet, eine umfassende Berechtigung für spezielle Benutzer an den Anfang einer ACL zu stellen. Zum Beispiel gewährt die folgende Direktive einem für Replikationszwecke eingesetzten Benutzer Leserechte auf das gesamte Verzeichnis, während die Direktive für alle anderen Benutzer "überlesen" wird:

access to *

by dn.exact="[DN des Replikations-Benutzers]" read

by * break

ACL in der slapd-config

Die bisher beschriebene Syntax gilt für die Konfiguration mittels der Konfigurationsdatei "slapd.conf". Wird die Datenbank "slapd-config" verwendet, gilt entsprechend:

olcAccess: {n}to [Zielobjekt]

by [Benutzer] [Berechtigungsumfang]

by [Benutzer] [Berechtigungsumfang]

...

Der optionale Index {n} steuert die Reihenfolge der Einträge, die sich im Gegensatz zur Konfigurationsdatei "slapd.conf" nicht aus deren Positionen in der Datei ergeben kann, da die Verzeichnisdienstobjekte olcAccess auf der gleichen Ebene stehen. Ohne einen Index ist die konfigurationsinterne Reihenfolge und damit die Wirksamkeit der Einträge nicht vorhersehbar.

ACLs global und datenbankspezifisch

Zugriffskontrolllisten lassen sich global und auf Datenbankebene festlegen. Die Zusammenhänge müssen bei der Umsetzung von OpenLDAP korrekt berücksichtigt werden. Datenbank-Direktiven haben Vorrang vor globalen Direktiven. Dabei wird die globale Zugriffskontrollliste an die datenbankspezifische angehängt und die Gesamtliste für die Auswertung durch die Direktive "access to * by * none" abgeschlossen, auch wenn diese nicht eingetragen wurde. Spezielle Direktiven zu Beginn einer globalen ACL werden deshalb bei Kombination mit einer datenbankspezifischen Zugriffskontrollliste oft nicht wie gewünscht umgesetzt.

Zugriffsrechte über Gruppenmitgliedschaften

Die Vergabe von Berechtigungen über Gruppenmitgliedschaften ermöglicht es, die Zugriffsrechteverwaltung und die technische Wartung des slapd-Servers organisatorisch zu trennen. Um Zugriffsrechte zu verwalten, müssen nur noch Gruppenobjekte geändert werden, ein Zugriff auf die Konfiguration selbst ist nicht mehr notwendig.

Werden Zugriffsrechte über Gruppenmitgliedschaften verwaltet, so sind folgende Punkte zu beachten:

- OpenLDAP löst in der Version 2.4 keine Zugriffsrechte auf, wenn sich Gruppen innerhalb von Gruppen befinden. Als Lösungsansatz bietet OpenLDAP das "Set"-Konzept an. Solange "Sets" in der Version 2.4 als experimentell eingestuft werden, sollten sie in produktiven Umgebungen nicht eingesetzt werden.
- Es wird empfohlen, das Overlay "memberof" (Member of) einzusetzen. Wenn ein DN einem Gruppenobjekt zugeordnet wird, sorgt das Overlay "memberof" dafür, dass die entsprechende Eigenschaft auch beim DN als operationelles Attribut vermerkt wird. Dadurch werden aufwändige Suchoperationen im Rahmen der Zugriffskontrolle vermieden.

In OpenLDAP besteht für eine ebenfalls von der Konfiguration losgelöste Verwaltung von Zugriffsrechten die Möglichkeit, über den Mechanismus "Access Control Information" (ACI) Zugriffsrechte beim jeweiligen Benutzer zu hinterlegen. ACI ist jedoch sehr aufwändig in der Konfiguration, da jeder Benutzer einzeln einzurichten ist. Zudem ist die Syntax des Mechanismus noch nicht standardisiert, der Mechanismus hat in der Version 2.4 zudem nur einen experimentellen Status. Solange ACI einen experimentellen Status hat, sollte es nicht verwendet werden.

Testen von Zugriffsberechtigungen

Jede Änderung der Zugriffskontrollliste sollte anschließend durch das Werkzeug slapacl überprüft werden. Über das Werkzeug werden ein Benutzer und eine Operation angegeben und slapacl ermittelt, ob diese Operation vom angegebenen Benutzer erfolgreich durchgeführt werden könnte, ohne die Operation tatsächlich durchzuführen. Diese Prüfung sollte insbesondere dann durchgeführt werden, wenn der Zugriff abgelehnt werden soll. Das Tool slapacl prüft gegen die Konfigurationsdatei "slapd.conf". Wirksam ist die geänderte Zugriffskontrollliste aber erst nach einem Start oder Neustart des slapd-Servers. Darum sollte der slapd-Server beim Einsatz der slap*-Werkzeuge immer gestoppt sein. Selbst wenn der Einsatz der slap*-Werkzeuge keine technischen Auswirkungen hat, können Ergebnisse bei laufendem slapd-Server zu falschen Schlussfolgerungen führen.

Es wird empfohlen, aus dem Berechtigungskonzept Testfälle abzuleiten und diese mit dem Werkzeug slapacl zu testen,

- wenn die Zugriffskontrolllisten wesentlich verändert wurden,
- wenn neue Backends, Datenbanken oder Suffixe definiert wurden oder
- wenn OpenLDAP aktualisiert wurde.

Keine Einschränkung des rootDN

Die ACLs gelten grundsätzlich nicht für den rootDN einer Datenbank. Wird er dennoch in Zugriffskontrolllisten einbezogen, so führt dies lediglich zu erhöhtem Administrationsaufwand und einem Performanceverlust. Andererseits ist zu beachten, dass der Verzicht auf Zugriffskontrolllisten nicht dazu führt, dass lediglich der "rootDN"-Zugriff auf den Verzeichnisdienst unter OpenLDAP hat. Ohne Zugriffskontrolllisten greift eine Voreinstellung, die allen, auch anonymen Benutzern, Leserecht auf alle Inhalte des Verzeichnisdienstes gewährt. Auf ACLs darf keinesfalls verzichtet werden.

Komplexität der Zugriffsberechtigungen

Zugriffskontrolllisten können in zahlreichen Einzelaspekten gesteuert werden und fast beliebig komplex sein. Administratoren sollten sich mit den umfangreichen Beispielkonfigurationen im frei verfügbaren OpenLDAP Administrator's Guide vertraut machen. Es wird jedoch darauf hingewiesen, dass sich die in dieser Maßnahme zusammengestellten "access levels" bewährt haben und für die Abbildung von Zugriffsrechten in der Regel ausreichend sind. Insbesondere mit regulären Ausdrücken und Suchfiltern ist vorsichtig zu verfahren, da diese sehr leicht zu umfangreich definiert werden und so ungewollt Zugriffsrechte gewähren. Darüber hinaus schränken sie die Verarbeitungsgeschwindigkeit bei Zugriffen deutlich ein, da ihre Prüfung Ressourcen verbraucht. Je umfangreicher die Zugriffsrechte in der slapd-Server-Konfiguration wird, desto wichtiger sind umfangreiche Tests mittels slapacl. Kommt es hierbei immer wieder zu Fehlern, sollte das Design der Zugriffsrechte grundsätzlich überarbeitet werden.

APP.2.3.M6 Sichere Authentisierung gegenüber OpenLDAP

Um OpenLDAP zu nutzen, ist es in der Regel notwendig, dass der Verzeichnisdienst einer Sitzung die Identität eines Benutzers zuordnen kann. Nur dann kann der Verzeichnisdienst sinnvoll eingesetzt werden, um z. B. Betriebssystemressourcen zu verwalten und nur dann greifen die festgelegten Zugriffsrechte (siehe APP.2.3.M5 *Sichere Vergabe von Zugriffsrechten auf dem OpenLDAP*). Im Rahmen des "binds" am slapd-Server wird deshalb die Identität des Benutzers angegeben. Geschieht dies nicht, wird von einem anonymen Zugriff (anonymus) gesprochen. Wird die Identität im Rahmen des "binds" angegeben, so sollte der Benutzer nachweisen, dass er tatsächlich die Identität hat, die er vorgibt. Ist ein solcher Nachweis nicht notwendig, kann sich jeder Benutzer mit einer beliebigen Identität anmelden, es handelt sich dann um eine nicht authentisierte Nutzung (unauthenticated).

Anonyme Benutzer

Wenn nicht im Rahmen der Planung von OpenLDAP (siehe APP.2.3.M1 *Planung und Auswahl von Backends und Overlays für OpenLDAP*) entschieden wurde, dass der Verzeichnisdienst anonym genutzt werden darf, muss die anonyme Nutzung durch die Konfigurationsdirektive "disallow bind_anon" unterbunden werden.

Wenn der Verzeichnisdienst zwischen verschiedenen Benutzern unterscheiden soll, muss auch eine Authentisierung stattfinden. Eine Anmeldung ohne Identitätsnachweis sollte außerhalb von Teststellungen nicht zugelassen werden. Die Authentisierung ist mit der Konfigurationsdirektive "require authc" zu erzwingen.

Authentisierung mittels Passwort

Die grundsätzliche Methode, die OpenLDAP zur Authentisierung eines Benutzers vorsieht, ist die Kombination einer Benutzerkennung und eines Passwortes, sie wird als "simple bind" bezeichnet. Diese Authentisierungsmethode gilt dann als sicher, wenn das verwendete Passwort nur dem zugehörigen Benutzer bekannt ist.

Übertragung des Passworts

Nach den Spezifikationen des Standards LDAPv3 wird das Passwort zur Authentisierung im Klartext an den Server übertragen. Daher muss die Kommunikationsverbindung zwischen Client und Server verschlüsselt werden (siehe *APP.2.3.M6 Sichere Authentisierung gegenüber OpenLDAP*), damit das Passwort nicht von einem Angreifer abgehört werden kann.

Es wird dringend empfohlen, die mögliche Verschlüsselung der Kommunikationsverbindung durch den slapd-Server nicht nur anzubieten, sondern als Voraussetzung für eine "bind"-Operation zu erzwingen. Andernfalls hängt die Sicherheit einer Verbindung von der Entscheidung und der Fachkenntnis des Benutzers sowie den Fähigkeiten der eingesetzten Client-Software ab. Über die Direktive "security" können global oder datenbankspezifisch Anforderungen an die bestehende Verbindungssicherheit über die Verschlüsselungsstärke für verschiedene Operationen festgelegt werden, beispielsweise durch "security simple_bind=XYZ". Die Angabe XYZ ist durch einen Security Strength Factor (SSF) zu ersetzen. Der SSF ist eine Zahl, die für das Verschlüsselungsverfahren und die verwendete Schlüssellänge steht, die zur Verschlüsselung der eigentlichen Nachrichten mit einer symmetrischen Chiffre verwendetet wird, wie beispielsweise 56 für DES, 112 für Triple DES und 128, 192, oder 256 für AES. Sie sollte mindestens auf 112 festgelegt werden. Gegebenenfalls sind aktuelle Forschungsergebnisse und die Empfehlungen des BSI zu berücksichtigen. In der Direktive aufgeführte Operationen werden bei einer niedrigeren Verbindungssicherheit abgewiesen.

Ablage des Passworts

Ist sichergestellt, dass das Passwort nur gesichert übertragen wird, kann das Passwort immer noch auf Seiten des Servers gefährdet sein. Wird ein Server kompromittiert oder gelingt beispielsweise ein Zugriff auf eine Datensicherung der Verzeichnisdienstobjekte, könnte ein Angreifer Kenntnis von Passwörtern der Benutzer erlangen. Deshalb sind lediglich die Prüfsummen (Hashwerte) von Passwörtern zu speichern. Dem steht entgegen, dass der LDAP-Standard keine gehashten Passwörter unterstützt. OpenLDAP realisiert serverseitig eine Ablage der gehashten Passwörter und unterstützt verschiedene Hashing-Algorithmen. Es sollte ein Algorithmus aus der Gruppe Secure Hash Algorithm (SHA) in der Variante SSHA, das heißt "gesalzen" verwendet werden. Gesalzen bedeutet, dass das Passwort vor Bildung des Hashwertes um einen weiteren Wert ergänzt wird, um Wörterbuchattacken auf das Passwort zu erschweren. Keinesfalls sollte als Hashing-Algorithmus CRYPT ausgewählt werden. CRYPT wird betriebssystemspezifisch implementiert, weshalb die Authentisierung gegenüber OpenLDAP nach einer Migration auf ein anderes Betriebssystem gegebenenfalls nicht mehr funktioniert.

Der slapd-Server wird über die Direktive "password-hash {Algorithmus}" angewiesen, nur den, mit dem angegebenen Algorithmus erzeugten Hashwert eines Passworts, im Verzeichnis abzulegen. Die geschweiften Klammern sind dabei Teil der Syntax, so wird SSHA mittels "password-hash {SSHA}" festgelegt. Die Direktive gilt immer dann, wenn Passwörter über den slapd-Server eingerichtet oder geändert werden, das heißt mittels der Applikation "ldappasswd" oder über eine andere Client-Anwendung.

Werden LDIF-Dateien erzeugt und importiert, so müssen in der Datei angegebene Inhalte des Feldes "userPassword" bereits als Hashwerte vorliegen, wenn ein Hashwert genutzt werden soll. Das gleiche gilt für die Angabe des rootDN-Passworts in der Konfiguration (siehe APP.2.3.M3 *Sichere Konfiguration von OpenLDAP*). Um Hashwerte von Passwörtern zu erzeugen, ist das slap*-Werkzeug slappasswd zu benutzen. Über den Parameter "-h" wird der zu verwendende Hashing-Algorithmus angegeben, der empfohlene Wert SSHA entspricht der Voreinstellung. Hinter dem Parameter "-s" wird das Passwort im Klartext angegeben. Die Ausgabe des Werkzeugs ist dann mit einem vorangestellten {SSHA} in die LDIF- oder Konfigurationsdatei zu übernehmen. Wird das Werkzeug in der Kommandozeile verwendet, ist die in der Regel eingerichtete Eingabe-Historie vorher abzuschalten, weil das Passwort sonst im Klartext darin gespeichert wird.

Qualität des Passworts

Selbst wenn Passwörter verschlüsselt übertragen und als Hash-Wert abgelegt werden, besteht immer noch die Gefahr, dass Benutzer zu schwache Passwörter verwenden. Sie können beispielsweise durch Wörterbuchattacken leicht ermittelt werden. Es sollte organisatorische Vorgaben geben, damit Benutzer keine schwachen Passwörter wählen (siehe Baustein ORP.4 *Identitäts- und Berechtigungsmanagement*). OpenLDAP unterstützt derartige Vorgaben technisch durch das Overlay "ppolicy" (Password Policy). Das Overlay setzt Regeln wie eine minimale Länge eines Passwortes oder ein minimales und maximales Alter bis zur möglichen bzw. nötigen Änderung eines Passworts um. Außerdem kann es diverse Qualitätsprüfungen von Passwörtern vornehmen und führt pro Benutzer eine Liste früherer Passwörter, um zu verhindern, dass diese erneut verwendet werden. Über Passwortregeln hinaus sperrt das Overlay "ppolicy" das Passwort-Attribut nach mehrmals fehlgeschlagener Authentisierung für einen vorgegebenen Zeitraum für jeglichen Zugriff, um eine Brute-Force-Attacke auf das Passwort zu verhindern. Die jeweiligen Vorgaben, zum Beispiel wie lang ein Passwort sein muss oder nach wie vielen Fehleingaben eine Sperrung erfolgt, können in Richtlinien (policies) detailliert festgelegt werden. Richtlinien lassen sich benutzerspezifisch oder für das gesamte Verzeichnis sowie für Teilbäume zuordnen. Der rootDN wird nicht durch das Overlay "ppolicy" eingeschränkt.

Weitere Authentisierungsmechanismen

OpenLDAP ist in der Lage, für die Authentisierung von Benutzern auf Funktionen anderer Anwendungen zurückzugreifen. So können auch Authentisierungsmechanismen verwendet werden, deren Sicherheit über diejenige von Benutzerkennung und Passwort hinausgeht (strong bind). Notwendig ist dafür die Abstraktionsschicht Simple Authentication and Security Layer (SASL). SASL unterstützt über sogenannte Mechs verschiedene Authentisierungs- und Verschlüsselungsmechanismen und kann selbst wiederum auf externe Verfahren zurückgreifen. So können Benutzer unter anderem über SSL/TLS-Zertifikate (siehe Baustein APP.1.2 *Web-Browser*) oder durch das Kerberos-Verfahren authentisiert werden. Die Authentisierung wird von OpenLDAP an SASL delegiert. Besteht für den Informationsverbund ein hoher oder sehr hoher Schutzbedarf oder existiert bereits eine Authentisierungsinfrastruktur außerhalb von OpenLDAP, sollte die Anbindung via SASL erfolgen.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "OpenLDAP".

APP.2.3.M7 Schulung von Administratoren von OpenLDAP

Um OpenLDAP sicher einzurichten und zu betreiben, werden detaillierte Kenntnisse über OpenLDAP und seine grundlegenden Konzepte benötigt. Eine Schulung der Administratoren zu OpenLDAP und den zugehörigen Sicherheitsthemen ist daher unerlässlich.

Schulungsinhalte

Wie tief sich ein Administrator mit den einzelnen Punkten beschäftigen muss, hängt von seinem Tätigkeitsfeld ab. Allgemeine Inhalte zu Verzeichnisdiensten werden im Baustein APP.2.1 *Allgemeiner Verzeichnisdienst* aufgeführt. Schulungsinhalte sollten für OpenLDAP in jedem Fall die folgenden Stichpunkte umfassen und diese erläutern.

Grundlagen

- Überblick über den Aufbau von OpenLDAP, Verständnis von Backends und Overlays
- Planung, Einrichtung, Konfiguration ("slapd.conf" und "slapd-config")
- Grundlegende Kenntnisse, die zur Installation der Anwendung aus dem Quelltext befähigen
- Verständnis im Umgang mit Informationsquellen zu Open Source Software
- Kenntnis des LDAP Data Interchange Formats (LDIF)
- Objektklassen und operationelle Attribute
- Kenntnis der Werkzeuge von OpenLDAP und des systematischen Unterschieds zwischen ldap*- und slap*-Werkzeugen

Schema-Verwaltung

- Problematik und Auswirkungen von Schema-Veränderungen
- Attributseinschränkungen durch Overlays innerhalb der Schemata
- Unterscheidung von normalen und operationellen Attributen

Replikation

- Verwendete Mechanismen zur Replikation bei OpenLDAP ("refreshOnly" und "refreshAndPersist")
- Suchfilter und operationelle Attribute
- Ausblick auf die Delta-Replikation
- Ausblick auf Multi-Master- und Mirror-Mode-Betrieb im Zusammenhang mit Replikationskonflikten

Datensicherung

- Problematik des Erstellens einer Datensicherung von OpenLDAP
- Sicherung der Konfiguration für beide Konfigurationsmodi
- Wiedereinspielen von Datensicherungen mittels "slapadd"

Vergabe von Zugriffsrechten

- Vergabe von Zugriffsrechten auf Verzeichnisdienstobjekte
- Zusammenwirken von globalen und datenbankspezifischen ACLs
- Mögliche Zugriffsrechte

Authentisierung

- Hash-Algorithmen
- Kerberos
- SASL
- SSL/TLS-Zertifikate

APP.2.3.M8 Einschränkungen von Attributen bei OpenLDAP

Der slapd-Server kann durch Overlays in die Lage versetzt werden, Restriktionen umzusetzen, ohne dass dafür Schemas angepasst oder erstellt werden müssen. Derartige Einschränkungen sind sinnvoll, um die Qualität und Integrität der Verzeichnisdienstinhalte zu verbessern. Folgende Overlays können verwendet werden:

- constraint
  Das Overlay "constraint" (Constraints) ermöglicht, dass Werte einem bestimmten regulären Ausdruck entsprechen müssen. So kann beispielsweise erzwungen werden, dass das Attribut "mail" lediglich mit Mailadressen der eigenen Institution belegt werden kann.
- unique
  Das Overlay "unique" (Attribute Uniqueness) ermöglicht, dass ein ausgesuchter Wert lediglich einmal im Verzeichnisbaum vorhanden sein darf. So kann beispielsweise verhindert werden, dass eine Personalnummer zwei verschiedenen Benutzern zugewiesen wird.
- refint
  Das Overlay "refint" (Referential Integrity) wahrt die referenzielle Integrität von Referenz-Attributen. Werden zum Beispiel Distinguished Names (DNs) als Gruppenmitglieder eingetragen oder der DN eines Vorgesetzten in einem Attribut beim Mitarbeiter hinterlegt, so ändert das Overlay "refint" diese Referenzen, wenn der jeweilige DN verändert wird. Dafür führt "refint" bei der Änderung jedes DNs eine Suche durch, ob der DN in solche Attribute eingetragen ist. Änderungen setzt das Overlay "refint" im Attribut um, im Fall der Löschung entfernt es den DN.
  Achtung: Entfernt das Overlay das letzte Mitglied aus einer Gruppe, so wird stattdessen der in der Sub-Direktive "refint_nothing" definierte DN eingefügt, da leere Gruppen das Gruppenschema verletzen können. Hier ist darauf zu achten, einen geeigneten DN, wie einen fachlichen Administrator, vorzugeben, damit kein DN mit geringeren Rechten durch die Gruppe unangemessene Rechte erhalten würde.

Bei derartigen Beschränkungen ist zu beachten, dass diese nur für neue oder geänderte Attribute und Objekte gelten. Bestehen Verstöße gegen die festgelegten Regeln, bevor die Overlays aktiviert werden oder werden unpassende Datensätze durch einen direkten Zugriff auf die verwendete Datenbank eingefügt, so wirken die genannten Overlays nicht.

Solche Restriktionen dürfen ausschließlich auf Nutzerdaten angewendet werden. Werden die Beschränkungen zum Beispiel verwendet, um operationelle Attribute vorzugeben oder werden sie innerhalb der "slapd-config"-Konfiguration erzwungen, kann dies zu unvorhersehbarem Verhalten bis hin zur Unbrauchbarkeit des slapd-Servers führen.

APP.2.3.M9 Partitionierung und Replikation bei OpenLDAP

Die Aufteilung von Teilbäumen eines Verzeichnisdienstes auf verschiedene Server (Partitionierung) ist eine effektive Möglichkeit, um durch Lastverteilung eine höhere Verfügbarkeit zu erreichen. Damit die Aktualität der Verzeichniskopien sichergestellt ist, müssen Veränderungen an den Daten durch Replikation zwischen den Servern ausgetauscht werden. Welcher Replikationsmodus angemessen ist, muss in Anhängigkeit von Netzverbindungen und Verfügbarkeitsanforderungen gewählt werden.

In dieser Maßnahme ist die mögliche Umsetzung dieser Konzepte mit OpenLDAP beschreiben, für die generelle Planung von Partitionierung und Replikation sehen Sie bitte im Baustein APP.2.1 *Allgemeiner Verzeichnisdienst*.

Partitionierung

Die Partitionierung von Verzeichnisdiensten unter OpenLDAP ist sehr einfach zu konfigurieren. Wird ein Teil des Verzeichnisses ausgelagert oder soll ein Server wissen, welcher andere Server gewisse Teilbäume vorhält, so ist in der globalen Konfiguration dieses Servers der entsprechende Suffix als ein Objekt der Objektklasse "referral" anzulegen. Die Referenzadresse des Servers mit dem ausgelagerten Teilbaum wird dem Attribut "ref" zugeordnet. Operationen von Clients, die diesen Teil des Verzeichnisdienstes betreffen, beantwortet der Server mit einem Verweis auf diese Adresse. Die Zuordnung wird als "Subordinate Knowledge Information" bezeichnet. Der Server "weiß", welcher Teil des Verzeichnisbaumes auf welchem Server zu finden ist. Soll sichergestellt werden, dass der Server bei Suchanfragen ausgelagerte Teilbäume selbst durchsucht, ist die jeweilige Datenbank mit der Direktive "subordinate" bzw. "olcSubordinate" mit der Datenbank des Servers zu verbinden. Dieser Vorgang wird als Gluing (leimen) bezeichnet.

Ein untergeordneter Server wird im Gegenzug nicht mit der genauen Information darüber versorgt, von welchen anderen Servern welche Teilbäume oberhalb oder gleichberechtigt mit seinem gespeichert werden. Wann immer eine Operation nicht zu einem Suffix des Servers passt, wird diese mit einem globalen "Referral" (Verweis) beantwortet, das heißt, der anfragende Client wird an einen Server verwiesen, der die Antwort liefern könnte. Bei Partitionen wird hier der übergeordnete Verzeichnisdienst eingetragen. Das Referral wird in diesem Zusammenhang auch als "Superior Knowledge Information" bezeichnet, obwohl die Direktive auch unabhängig von Partitionierungen verwendet werden kann. Die über die Adressen in den Referrals identifizierten Verzeichnisdienste müssen nicht mit OpenLDAP betrieben werden.

Durch das Overlay "chain" (Chaining) kann der Server Referrals auch selbst verfolgen. Der Client bemerkt dadurch nichts von einer Partitionierung und bekommt eine abschließende Antwort immer vom ursprünglich angefragten Server. Dies funktioniert unabhängig von den Fähigkeiten des Clients, der gegebenenfalls selbst keine Referrals verarbeiten kann.

Replikation

Bei OpenLDAP wird die Replikation über den "LDAP Sync Replication Engine" (syncrepl) Mechanismus umgesetzt. Der Mechanismus ist auf die BerkeleyDB abgestimmt und wird nur von den Backends "back-bdb" und "back-hdb" unterstützt. Das bedeutet, OpenLDAP kann nicht ohne Weiteres als Agent eingesetzt werden, um Verzeichnisdienste zu replizieren, für die der slapd-Server lediglich einen Proxy darstellt.

Vor der Entwicklung des "syncrepl"-Mechanismus wurde der "stand-alone LDAP update replication daemon" (slurpd) zur Replikation verwendet. Hierbei handelte es sich um ein Programm, das wie der slapd-Server als Dienst ausgeführt wurde und Kopien der Verzeichnisdienstinhalte pflegte. Dieser Dienst hat nicht zuverlässig funktioniert und wurde mit der Version 2.4 offiziell aus OpenLDAP entfernt. Hinweise auf "slurpd" in veralteten Dokumentationen sind als historisch anzusehen. Der "slurpd" darf keinesfalls verwendet werden.

Master und Slave, Provider und Consumer

Traditionell werden die an der Replikation beteiligten Server als Master und Slave bezeichnet. Der Master ist der eigentliche Verzeichnisdienst, über diesen Server kann schreibend auf Verzeichnisdienstinhalte zugegriffen werden. Der Slave übernimmt nur alle Informationen vom Verzeichnisdienst und gewährt auf diese Kopie lesenden Zugriff. Diese strikte Trennung gilt in OpenLDAP seit der Version 2.3 nicht mehr. Bei der Replikation in OpenLDAP übernimmt ein sogenannter Consumer-Dienst Daten von einem Provider -Dienst. Es wichtig zu verstehen, dass ein Consumer gegenüber dem Provider als Client auftritt, obwohl der Consumer seine Replik selbst als Server für andere Clients zur Verfügung stellt. Die Einstellungen zur Serversicherheit des Consumers gelten für die Verbindung zum Provider nicht. Stattdessen gilt die Client-Konfiguration, diese ist auf einem Consumer sorgfältig vorzunehmen, obwohl sie für Server eigentlich nicht benötigt wird. Es ist insbesondere zu berücksichtigen, dass der Consumer ein "bind" beim Provider vornehmen muss und etwaige Zugriffsbeschränkungen und Suchlimits des verwendeten Benutzers die Replikation behindern können.

refreshOnly und refreshAndPersist

Die Replikation kann in einem pull- oder einem push-Mode betrieben werden. Beim pull-Mode, der in OpenLDAP als "refreshOnly" bezeichnet wird, fragt der Consumer in festgelegten Abständen den Provider auf Änderungen ab. Dabei sendet der Consumer in Form eines "Sync Cookies" die Aktualität der von ihm gehaltenen Daten. Aufgrund dieser Information wird beim Provider eine Suche gestartet, die alle Änderungen seit dem vom Consumer gemeldeten Zeitpunkt umfasst. Der Provider "kennt" in diesem Fall den Consumer nicht, er beantwortet lediglich Suchabfragen. Damit diese Suchen korrekte Ergebnisse bringen, ist es besonders wichtig, dass die Uhren von Provider und Consumer möglichst synchron laufen (siehe Baustein NET.1.2 *Netzmanagement*). Beim "push-Mode", der in OpenLDAP als "refreshAndPersist" bezeichnet wird, bleibt die Verbindung zwischen Provider und Consumer bestehen und der Provider sendet alle Änderungen immer an den Consumer. Bei der Auswahl der geeigneten Replikationsmethode gilt als Faustregel, dass "refreshOnly" umso sinnvoller ist, je größer die zu replizierenden Datenmengen sind und "refreshAndPersist" umso eher eingesetzt werden sollte, je wichtiger eine zeitnahe Aktualisierung des Providers ist.

Einrichtung einer Replikation

Um die Replikation eines Verzeichnisdienstes mit OpenLDAP einzurichten, sind mehrere Schritte nötig:

- Der Consumer muss installiert (siehe APP.2.3.M2 *Sichere Installation von OpenLDAP*) und konfiguriert (siehe APP.2.3.M3 *Sichere Konfiguration von OpenLDAP*) werden. Dies kann und sollte nach Möglichkeit durchgeführt werden, indem Kopien der Provider-Konfiguration auf den Provider übertragen werden. Bei der Consumer-Konfiguration ist besonders wichtig, dass auf dem Consumer die gleichen Schemas eingerichtet werden, wie auf dem Provider.
- Auf dem Consumer muss für die zu replizierende Datenbank die Datenbank-Direktive "syncrepl" eingerichtet werden. Mit den Sub-Direktiven "searchbase", "filter", "scope" und "attrs" lässt sich bestimmen, was repliziert werden soll. So können neben dem gesamten Verzeichnisdienst zum Beispiel nur Teilbäume repliziert werden oder auch nur bestimmte Attribute von Objekten. Bei der Einrichtung ist besonders zu beachten, dass im Fall der Online-Konfiguration auch der Konfigurationssuffix "CN=config" repliziert werden kann. Weitere Sub-Direktiven bestimmen die Adresse des Providers, replikationsspezifische Einstellungen zur Sicherung der Kommunikation zwischen Consumer und Provider, die Replikationsmethode und die Wiederaufnahme der Verbindung zum Provider, wenn diese abbricht (refreshAndPersist) oder der Provider nicht erreicht werden kann (refreshOnly).
- Besonders wird außerdem auf die Sub-Direktive "schemachecking" hingewiesen. Ist "schemachecking" deaktiviert (was dem Vorgabewert entspricht), können durch die Replikation auch solche Daten eingefügt werden, die nach den Schemas eigentlich unzulässig sind. Dies kann sinnvoll sein (insbesondere bei Teilrepliken), aber die Integrität der Repliken einschränken.
- Obwohl die Einstellungen zur Replikation hauptsächlich auf dem Consumer vorzunehmen sind, muss auch der Provider für eine korrekte Replikation konfiguriert werden. Damit er Suchanfragen des Consumers in Abhängigkeit von einem Änderungszeitpunkt beantworten kann, muss sich der Provider selbst vorgenommene Änderungen merken beziehungsweise eine Übersicht aktueller Zeitstempel, sogenannter "context change sequence numbers" (contextCSNs) führen. Dies wird durch den Aufruf des Overlay "syncprov" (Sync Provider) erreicht.
- Um die Consumer-Datenbank erstmals zu befüllen, wird empfohlen, nur die benötigten Datensätze aus einer Datensicherung des Providers einzuspielen (siehe APP.2.3.M13 *Datensicherung beim Einsatz von OpenLDAP*), da eine vollständige Übertragung aller Verzeichnisdienstinhalte über das Netz unnötig Zeit und Ressourcen beansprucht. Weil syncrepl über Mechanismen zum Datenabgleich verfügt, ist es nicht notwendig, dass die verwendete Datensicherung aktuell ist. Wird eine Datensicherung eingespielt, die noch keine contextCSNs enthält, ist der Parameter "-w" anzugeben, wenn die Datenbank mit slapadd befüllt wird, damit contextCSNs erzeugt werden. Dies wird insbesondere bei einer ersten Replikation der Fall sein, da der Provider üblicherweise noch nicht auf einen solchen Betrieb vorbereitet war und das Overlay "syncprov" noch nicht aufgerufen wurde.

Delta-Replikation

Grundsätzlich sendet der Provider alle Attribute von Einträgen, die geändert wurden, als Suchergebnis oder im Rahmen der Replikation. Er tut dies selbst dann, wenn im Eintrag nur eines der Attribute verändert wurde. In Verbindung mit dem Overlay "accesslog" (siehe auch APP.2.3.M12 *Protokollierung und Überwachung von OpenLDAP (Datenschutzbeauftragte)*) ist es auch möglich, die Veränderungen von Attributen detailliert aufzuzeichnen und dann mit dem "syncrepl"-Mechanismus lediglich die Änderungen zu übermitteln. Dies setzt eine umfangreichere Konfiguration voraus. Bei häufigen Änderungen von kleinen Attributen an relativ großen Objekten sollte diese Möglichkeit geprüft werden, bei wenigen Objekten oder geringen Anzahlen ist die Delta-Replikation nicht notwendig.

Multi-Master- und Mirror-Mode-Betrieb

Es ist auch möglich, einen Multi-Master-Betrieb einzurichten. Bei einem Multi-Master-Betrieb gibt es mehr als einen Server, auf den schreibend zugegriffen werden kann, und die Master sind untereinander sowohl Provider als auch Consumer. Der Sinn dieser Betriebsvariante besteht darin, dass beim Ausfall eines Servers immer noch schreibender Zugriff auf den Verzeichnisdienst besteht, ohne dass (wie bei einem Slave/nur-Consumer) erst die Konfiguration angepasst werden muss. Dieser Betrieb ist nicht unumstritten und wird von einigen Mitgliedern des OpenLDAP-Teams als nicht sinnvoll angesehen, da er die Konsistenz eines Verzeichnisses bedrohen kann. Dies geschieht, wenn auf den beiden Mastern zeitgleich konkurrierende Änderungen vorgenommen werden. Ein Multi-Master-Betrieb ist für eine OpenLDAP-Installation in einem Informationsverbund mit normalem Schutzbedarf nicht notwendig. Sollten hohe oder sehr hohe Anforderungen an die Verfügbarkeit bestehen, kann eine Multi-Master-Konfiguration geprüft werden. Als Faustregel kann gelten, je wichtiger die unterbrechungsfreie Verfügbarkeit ist, desto eher ist ein Multi-Master-Betrieb sinnvoll, je wichtiger die Integrität der Daten zu jedem Zeitpunkt ist, desto weniger sinnvoll ist der Multi-Master-Betrieb.

Als Alternative zwischen dem Single-Master- und Multi-Master-Betrieb besteht die Möglichkeit eines Mirror-Mode-Betriebs. Bei dieser Betriebsvariante bestehen ebenfalls mehrere Server, über die schreibend auf den Verzeichnisdienst zugegriffen werden kann. Allerdings legt eine externe Monitoring-Komponente immer einen aktiven Server fest, der Änderungen durchführt. Fällt ein Server aus, bestimmt die Monitoring-Komponente automatisch den anderen Server zum aktiven Server. Die Delta-Replikation wird in dieser Betriebsart noch nicht unterstützt. Nachteilig ist auch, dass beim Ausfall der Monitoring-Komponente der eigentlich redundant ausgelegte Verzeichnisdienst nicht mehr verfügbar ist.

APP.2.3.M10 Sichere Aktualisierung von OpenLDAP

OpenLDAP wird ständig von den Entwicklern von OpenLDAP weiterentwickelt. Es ist deshalb sinnvoll, im Fall von Schwachstellen der Software sogar notwendig, die bestehende OpenLDAP-Installation durch eine neuere Version zu ersetzen.

Überwachung neuer Versionen

Die OpenLDAP-Entwickler informieren über die Mailingliste openldap-announce (siehe [OLDAPLIST]) über alle neuen Releases und Änderungen des Stable Release (Release Notes). Diese Mailingliste sollte von Administratoren abonniert und die Nachrichten sorgfältig gelesen. Sofern nicht über Sicherheitslücken berichtet wird oder ein neues Release eine für den Anwender wertvolle Funktion einführt, besteht kein Bedarf, neu veröffentlichte Releases zeitnah zu installieren. Wird eine neuere als die eingesetzte Version zum Stable Release erklärt, wird empfohlen, eine Aktualisierung von OpenLDAP für das nächste Wartungsfenster zu planen. Bei sicherheitsrelevanten Änderungen, wie behobenen Schwachstellen, muss OpenLDAP so schnell wie möglich aktualisiert werden.

Soll die bestehende OpenLDAP-Installation aktualisiert werden, sind alle relevanten Release Notes zu prüfen, um Änderungen zur bestehenden OpenLDAP-Installation zu identifizieren. Hierbei sind neben der unmittelbar zur geplanten Version gehörenden Nachricht alle Release Notes von Versionen relevant, die zwischen der eingesetzten und der geplanten Version veröffentlicht wurden. Insbesondere ist darauf zu achten, ob Änderungen eingesetzte Backends oder Overlays sowie Softwareabhängigkeiten betreffen. Ist dies der Fall, so ist die Planung von OpenLDAP zu aktualisieren (siehe APP.2.3.M1 *Planung und Auswahl von Backends und Overlays für OpenLDAP*).

Durchführung der Aktualisierung

Im Rahmen der Vorbereitung sind die Installationspakete für die geplante OpenLDAP-Version herunterzuladen und zu überprüfen (siehe APP.2.3.M2 *Sichere Installation von OpenLDAP*). Werden Binärpakete eines Distributors verwendet, stellt er gegebenenfalls auch spezielle Aktualisierungspakete bereit. Vor der Aktualisierung ist der slapd-Server anzuhalten und es ist eine aktuelle Datensicherung des bestehenden Verzeichnisses durchzuführen (siehe APP.2.3.M13 *Datensicherung von OpenLDAP*). Anschließend ist die neue Version von OpenLDAP zu installieren (siehe APP.2.3.M2 *Sichere Installation von OpenLDAP*). Die Installation kann in ein neues Zielverzeichnis erfolgen, um zur bisher verwendeten Version zurückkehren zu können. Die neu installierte Software ist zu konfigurieren, dies geschieht in der Regel durch die Übernahme der vorigen Konfiguration aus der Datensicherung. Anschließend müssen die Konfiguration mittels "slaptest" und die Zugriffsrechte mittels slapacl getestet werden, bevor der slapd-Server neu gestartet wird.

Folgende Punkte sind im Rahmen der Aktualisierung von OpenLDAP besonders zu beachten:

- Oftmals setzen Administratoren eigene Skripte ein, um Aufgaben im Zusammenhang mit OpenLDAP zu automatisieren. Wird OpenLDAP aktualisiert, müssen derartige Skripte überprüft werden, ob sie mit der aktualisierten Version von OpenLDAP problemlos zusammenarbeiten.
- Insbesondere, wenn verschiedene Versionen von OpenLDAP parallel auf einem IT-System installiert sind, ist es von großer Bedeutung, dass immer die slap*-Werkzeuge der jeweiligen Version eingesetzt werden. Tests von Konfiguration und Zugriffsrechten müssen mit den "neuen" Versionen von slaptest und slapacl durchgeführt werden und die Datensicherung muss mit dem "neuen" slapadd eingespielt werden.

APP.2.3.M11 Einschränkung der OpenLDAP-Laufzeitumgebung

Um die Sicherheit von OpenLDAP auch im Betrieb aufrecht zu erhalten, sollten regelmäßig eine Reihe von Schritten durchgeführt werden, um eventuelle Probleme rechtzeitig zu entdecken.

Beim Betrieb von OpenLDAP sollten insbesondere folgende Aspekte berücksichtigt werden:

- Es ist darauf zu achten, dass der slapd-Server mit der beabsichtigten Konfiguration gestartet wird. Mit dem Parameter "-f [Pfad/Dateiname]" wird eine zu verwendende slapd.conf festgelegt, mit dem Parameter "-F [Pfad]" ein zu verwendendes slapd-config-Verzeichnis. Wichtig ist, dass sich die Konfigurationen nicht ergänzen, wenn gleichzeitig beide Parameter verwendet werden, sondern dass die slap-config-Konfiguration durch die slapd.conf-Konfiguration überschrieben wird.
- Der slapd-Server sollte beim Start mit dem Parameter "-h [Protokolle]" auf die benötigten Protokolle eingeschränkt werden, beispielsweise "-h ldaps://".
- Der slapd-Server ist durch den Parameter "-r [Verzeichnis]" auf ein Laufzeitverzeichnis einzuschränken (chroot-Mechanismus). Dieses Verzeichnis muss alle Konfigurationsdateien und Datenbanken beinhalten.
- Vor einem geplanten Anhalten des slapd-Servers sollte geprüft werden, ob dieser noch Operationen durchführt oder Verbindungen zu Clients bestehen (siehe APP.2.3.M12 *Protokollierung und Überwachung von OpenLDAP (Datenschutzbeauftragte)*). Dies gilt insbesondere für Operationen, die bei einem Neustart nicht fortgeführt werden wie der Indizierung). Der slapd-Server verfügt über keinen stop-Befehl, zum Anhalten ist der zugehörige Prozess zu beenden, zum Beispiel durch "kill -INT 'cat /usr/local/var/slapd.pid'".
- Änderungen an der Konfiguration müssen sorgfältig dokumentiert werden, so dass zu jeder Zeit nachvollzogen werden kann, wer aus welchem Grund welche Änderungen vorgenommen hat. Für die Änderungen an den Konfigurationsdateien wird empfohlen, ein Revisionskontrollprogramm (beispielsweise git, mercurial oder RCS) einzusetzen. So kann jederzeit ein früherer Stand der Konfiguration wiederhergestellt werden und es bleibt nachvollziehbar, wer welche Änderungen aus welchem Grund durchgeführt hat.
- Nach jeder Änderung der Konfiguration muss zunächst mit dem Programm slaptest geprüft werden, ob die Syntax der Konfigurationsdatei korrekt ist. Syntaxfehler in der Konfigurationsdatei können sonst dazu führen, dass der slapd-Server nicht startet oder Sicherheitslücken entstehen.
- Nach jeder Änderung von Zugriffsberechtigungen ist mit dem Programm slapacl zu prüfen, ob die gerade durchgeführte Änderung wirksam ist.
- Die Administratoren müssen sich über aktuelle Sicherheitslücken in der eingesetzten Software frühzeitig informieren (siehe auch Baustein OPS.1.1.1 *Allgemeiner IT-Betrieb*). Informationen über neu entdeckte Sicherheitslücken veröffentlichen die Entwickler von OpenLDAP im "Issue Tracking System" (siehe [OLDAPTRACK]).
- Die beschriebenen Maßnahmen in den Umsetzungshinweisen Zum Baustein OPS.1.1.5 *Protokollierung* müssen auch für OpenLDAP umgesetzt werden. Speicherort und Umfang der Protokolle hängen von APP.2.3.M12 *Protokollierung und Überwachung von OpenLDAP (Datenschutzbeauftragte)* ab.
- Zum sicheren Betrieb gehören auch regelmäßig durchzuführende Maßnahmen zur Notfallvorsorge und zur Datensicherung (siehe Baustein APP.3.4 *Samba* und APP.2.3.M13 *Datensicherung von OpenLDAP*).

APP.2.3.M12 Protokollierung und Überwachung von OpenLDAP [Datenschutzbeauftragter]

Da OpenLDAP in der Regel eine zentrale Komponente eines Netzes darstellt, sind Aktivitäten in OpenLDAP zu protokollieren und zu überwachen, um beispielsweise technische Probleme oder Angriffsversuche frühzeitig zu bemerken. Für OpenLDAP bestehen mehrere Möglichkeiten, Protokolle von Ereignissen anzulegen und den aktuellen Zustand des Systems zu überwachen.

Die Protokolldaten müssen unter Beachtung organisationsinterner Vorgaben regelmäßig ausgewertet werden, um Missbrauch und Systemfehler zu erkennen. Bei der Protokollierung und Überwachung eines zur Benutzerverwaltung eingesetzten Verzeichnisdienstes fallen zwangsläufig personenbezogene Daten an, die zur Leistungs- oder Verhaltenskontrolle geeignet sind. Wenn Protokollierung und Überwachung eingerichtet werden, sollten deshalb der Datenschutzbeauftragte (siehe auch Baustein OPS.1.1.5 *Protokollierung*) und die zuständige Mitarbeitervertretung beteiligt werden. Die Auswertung kann manuell oder mit Unterstützung eines Tools erfolgen. Im Vorfeld sollten kritische Ereignisse definiert werden, also solche, bei deren Auftreten ein Administrator zu benachrichtigen ist.

Debug und Syslog

Der slapd-Server verfügt über eine Debug-Funktion, um insbesondere technische Fehler zu identifizieren. Diese Funktion wird verwendet, wenn der slapd-Server mit dem Parameter "-d" gestartet wird:

slapd -d [Loglevel] -d [Loglevel] ....

Beim Start des slapd-Servers mit dem Parameter "-d" wird der slapd-Server im Gegensatz zum Aufruf ohne Debug-Funktion nicht vom aufrufenden Terminal getrennt und weiter im Vordergrund ausgeführt. Die Debug-Meldungen werden über die Standard-Ausgabe ausgegeben, in der Regel ist dies das aufrufende Terminal.

Der slapd-Server ist auch in der Lage, die Debug-Ausgaben an den Systemdienst Syslog zu leiten, der auch anderen zentralen Überwachungswerkzeugen als Basis dient. Statt des Parameters "-d" ist dafür der Parameter "-s" beim Aufruf zu verwenden, die Zahlen und Aliase der Loglevel bleiben gleich. Das gleiche Ergebnis wird durch die Angabe der Loglevel in der globalen Direktive "logLevel" (slapd.conf) bzw. "olcLogLevel" (slapd-config) erreicht. Syslog oder andere zentrale Werkzeuge werden insbesondere für große Strukturen empfohlen, da eine manuelle Kontrolle von Ereignissen dort kaum noch darstellbar ist. Bei akuten technischen Problemen ist die Debug-Funktion in der Konsole allerdings hilfreicher, da Syslog bei steigender Belastung oft nur zeitverzögert aktuelle Ereignisse ausgibt oder bei zu zahlreichen Nachrichten einige nicht verarbeitet.

Neben der Suche nach einem akuten technischen Fehler sind die technischen Protokolle geeignet, Unzulänglichkeiten der Konfiguration aufzudecken, die bisher nicht bemerkt wurden. Ist zum Beispiel aus den Protokollen ersichtlich, dass häufig nach einem bestimmten Attribut gesucht wird, für das kein Index existiert (index_param failed), so sollte ein entsprechender Index erzeugt werden, um aufwändige Suchläufe zu vermeiden.

Die Debug-Funktion ist nicht dazu geeignet, die fachliche Nutzung des Verzeichnisdienstes zu protokollieren. Die Ausgaben sollten deshalb regelmäßig gelöscht werden, nachdem sie analysiert wurden.

Protokollierung durch auditlog

Über das Overlay "auditlog" (Audit Logging) können alle Veränderungen an einer Datenbank in eine Datei im Format LDIF geschrieben werden. Das Overlay kann nur Veränderungen aufzeichnen und ist schlecht anpassbar. Der Funktionsumfang ist wesentlich geringer als der des neueren Overlays "accesslog". Das Overlay "auditlog" wird gelegentlich eingesetzt, wenn keine Notwendigkeit besteht, erfolgte Zugriffe zu erfassen und dies zum Beispiel aus Datenschutzgründen sicher vermieden werden soll.

Protokollierung durch accesslog

Mit dem Overlay "accesslog" (Access Logging) können alle Zugriffe auf eine Datenbank erfasst werden. Das Overlay wird auch im Rahmen der Delta-Replikation verwendet. Es wird benötigt, um die geänderten Attribute aufzuzeichnen, damit nur diese im Rahmen der Replikation an den Consumer übermittelt werden müssen (siehe APP.2.3.M9 *Partitionierung und Replikation bei OpenLDAP*).

Das Overlay zeichnet sich durch folgende Eigenschaften aus:

- Es ist möglich, die Protokollierung durch die Sub-Direktive "logops" auf bestimmte Operationen wie ausschließlich Schreibzugriffe zu beschränken.
- Es können auch nicht erfolgreiche Zugriffe aufgezeichnet werden (Sub-Direktive "logsuccess FALSE"). Treten erfolglose Zugriffsversuche gehäuft auf, sollte dies näher untersucht werden. Mögliche Gründe dafür sind:
  - Zugriffsrechte wurden fehlerhaft vergeben.
  - Anwender wurden unzureichend geschult.
  - Ein Angreifer versucht, unzulässige Operationen im Verzeichnisdienst durchzuführen.
  - Die Protokolldaten werden in einer anderen Datenbank abgelegt, die über die Sub-Direktive "logdb" festgelegt wird. Durch eine geschickte Rechtevergabe beziehungsweise Replikation der Datenbank besteht die Möglichkeit, die Aufzeichnungen von Zugriffen dem Einflussbereich der Administratoren zu entziehen.
  - Durch die Ablage der Zugriffe in einer LDAP-Datenbank sind die Einträge selbst via LDAP zugänglich. Entsprechend stehen komfortablere Auswertungsmöglichkeiten zur Verfügung, als dies bei einem normalen Protokoll in Form einer Textdatei der Fall ist.
  - Das Overlay kann über die Sub-Direktive "logpurge" angewiesen werden, Inhalte der Datenbank in bestimmten Intervallen zu löschen, zum Beispiel täglich alle Inhalte, die älter als zwei Wochen sind. So können unter anderem Vorgaben des Datenschutzes technisch unterstützt werden.

Das Overlay "accesslog" stellt die beste Möglichkeit dar, Protokolle über die fachliche Nutzung des Verzeichnisdienstes anzulegen. Dies ist insbesondere sinnvoll, um zum Beispiel regulatorische Anforderungen wie die Eingabekontrolle des Bundesdatenschutzgesetzes (BDSG) zu erfüllen.

Monitoring via back-monitor

In jedem Fall werden bei der Durchsicht von Protokollen relevante Ereignisse wie Sicherheitsvorfälle lediglich im Nachhinein betrachtet. Bei einer zentralen Software, wie dem Verzeichnisdienst einer Institution, ist der laufende Betrieb zu überwachen (Monitoring). OpenLDAP stellt dafür benötigte Funktionen über das Backend "back-monitor" zur Verfügung. Aufgrund der schützenswerten Daten des Monitorings sollte eine restriktive eigene ACL für das Backend in Betracht gezogen werden (siehe APP.2.3.M5 *Sichere Vergabe von Zugriffsrechten auf dem OpenLDAP*).

Das Suffix ist im Gegensatz zu den meisten anderen Datenbanken in OpenLDAP fest vorgegeben. Es ist immer "CN=monitor". "back-monitor" gehört zur Klasse der dynamischen Backends, das heißt, eine Suche mittels ldapsearch oder ähnlichen Tools greift nicht auf einen geschriebenen Datenbestand zu, sondern generiert die Daten bei Anfrage. Für den Benutzer geschieht dies allerdings transparent, so dass das Backend "back-monitor" mit dem Werkzeug ldapsearch von OpenLDAP ebenso wie mit grafischen Oberflächen oder speziellen Anwendungen für Überwachungszwecke abgefragt werden kann.

Die durch das Backend "back-monitor" verfügbaren Informationen sind sehr umfangreich und wachsen proportional mit dem eingerichteten Funktionsumfang von OpenLDAP. Es wird deshalb empfohlen, eine Dokumentation anzulegen, welche Werte anzuschauen sind. Sinnvolle Objekte für das Monitoring sind beispielsweise:

CN=Backends, CN=Monitor

Dieses Suffix liefert Informationen über vorhandene Backends. Die Kindelemente enthalten Informationen zum jeweiligen Backend, seinem Status und unterstützten Funktionen.

CN=Databases, CN=Monitor

"Databases" gibt Informationen über eingerichtete Datenbanken aus. Die Kindelemente enthalten Informationen zur jeweiligen Datenbank.

CN=Overlays, CN=Monitor

Dieser Teilbaum liefert Informationen über genutzte Overlays. Die Kindelemente enthalten Informationen zur jeweiligen Datenbank.

CN=Connections, CN=Monitor

"Connections" enthält Informationen über bestehende Verbindungen. Die Kindelemente enthalten jeweils Details zu einer Verbindung. Daneben gibt es zwei besondere Kindelemente, die die Anzahl von allen (CN=Total, CN=Connections, CN=Monitor) sowie der bestehenden Verbindungen (CN=Current, CN=Connections, CN=Monitor) angeben. Die bestehenden Verbindungen sollten unter anderem vor dem Anhalten des Verzeichnisdienstes geprüft werden.

CN=Listener, CN=Monitor

Dieses Suffix enthält Angaben über IP-Adressen und Ports, an denen der slapd-Server auf Verbindungen wartet. Hier sollte regelmäßig überprüft werden, dass nur bewusst eingerichtete Verbindungsmöglichkeiten aktiv sind.

CN=Operations, CN=Monitor

"Operations" liefert Informationen über initiierte und abgeschlossene Operationen. Die mögliche Ausgabe ist sehr umfangreich. Sie sollte nur anlassbezogen erfolgen und dann nach den entsprechenden Operationen wie "bind", "add", "delete" gefiltert werden. Die aktuell durchgeführten Operationen sollten zum Beispiel vor dem Anhalten des Verzeichnisdienstes geprüft werden.

CN=Statistics, CN=Monitor

Der Teilbaum liefert statistische Angaben über die vom Server übermittelten Daten. Für die Ausgaben sollte eine Historie von Erfahrungswerten geführt werden, um dann regelmäßig auf Anomalien prüfen zu können.

Die Überwachung von OpenLDAP sollte mit einer Überwachung des IT-Systems, auf dem OpenLDAP betrieben wird, einhergehen. Die Funktionsfähigkeit von OpenLDAP hängt auch wesentlich von der verfügbaren Prozessorleistung und dem Speicherplatz für die Datenbank ab. Diese Größen werden jedoch nicht von den Überwachungsfunktionen von OpenLDAP abgedeckt.

APP.2.3.M13 Datensicherung von OpenLDAP

Datensicherungen des OpenLDAP-Servers sind regelmäßig durchzuführen. Sie sind eine wichtige Voraussetzung, um aufgetretene Fehler zu korrigieren und gelöschte Daten wieder einspielen zu können.

Umfassende Datensicherung

Bei einer Datensicherung wird oftmals nur daran gedacht, die Nutzdaten zu sichern. Bei OpenLDAP sind das die Objekte im Verzeichnis. Um den tatsächlichen Weiter- bzw. Wiederbetrieb zu gewährleisten, müssen darüber hinaus auch die Konfigurationsdateien gesichert werden. Je nachdem, wie die Konfiguration durchgeführt wird (siehe APP.2.3.M3 *Sichere Konfiguration von OpenLDAP*), heißt das entweder, dass die Konfigurationsdatei "slapd.conf" zu sichern ist, oder aber, im Fall der Online-Konfiguration, das Suffix "CN=config". Darüber hinaus darf die erzeugte Sicherung physikalisch nicht auf dem gleichen IT-System verbleiben, da sie dann bei einem Ausfall des IT-Systems gegebenenfalls nicht verfügbar ist.

Datensicherung der Datenbanken

Die bewährte Methode zur Datensicherung von OpenLDAP ist es, das slap*-Werkzeug slapcat zu verwenden, um einen Datenexport im Format LDIF zu erzeugen, während der slapd-Server gestoppt ist. Der erzeugte Export kann vor der Ablage komprimiert werden, da die Klartext-Struktur der LDIF-Dateien unnötig große Dateien erzeugt.

Werden die Daten des Verzeichnisdienstes bei laufendem slapd-Server mittels slapcat exportiert, kann dies zu Inkonsistenzen der Datensicherung führen, wenn Daten während des Exports verändert werden. Es ist auch möglich, die zu sichernden Datenbanken in einen Nur-Lese-Zustand zu versetzen. Zu beachten ist aber, dass der Server dann nicht für schreibende Zugriffe verfügbar ist und auf diese Weise auch nicht die Online-Konfiguration gesichert werden kann. Zwar lässt sich auch das Suffix "CN=config" in einen Nur-Lese-Zustand versetzen, es kann aber nicht mehr ohne Neustart aus diesem Zustand befreit werden. Eine konsistente und vollständige Sicherung ist deswegen grundsätzlich nicht ohne einen Stopp des slapd-Servers möglich.

Rücksicherung

Für die Rücksicherung der Datenbestände sollte immer das Werkzeug slapadd eingesetzt werden. Prinzipiell ist auch das Werkzeug ldapadd oder eine geeignete Client-Anwendung in der Lage, Objekte aus LDIF-Dateien in einen Verzeichnisdienst einzufügen. Dies hat jedoch mehrere Nachteile:

- Das Werkzeug slapcat erzeugt den LDIF-Export entsprechend der physikalischen Reihenfolge der Objekte in der Datenbank. Wird diese Datei mittels ldapadd oder ähnlicher Client-Anwendungen in einen Verzeichnisdienst eingefügt, können Objekte gegebenenfalls nicht angelegt werden, wenn die ihnen übergeordneten Objekte noch nicht eingelesen wurden (weil sie in der gesicherten Datenbank physikalisch erst hinter den ihnen untergeordneten Objekten abgelegt wurden).
- Client-Anwendungen wie ldapadd kommunizieren mit dem laufenden slapd-Server über eine bestehende, möglichst verschlüsselte Netzverbindung. Der initiale Import einer Datensicherung auf diese Weise beansprucht unnötig viel Zeit, Bandbreite und Ressourcen.
- Der Import über ldapadd oder andere Client-Anwendungen erfordert einen laufenden slapd-Server, auf den schreibender Zugriff gewährt wird. Es besteht die Gefahr, dass während eines Imports durch andere Clients bereits auf unvollständige Daten zugegriffen wird oder Objekte in einer Weise angelegt oder geändert werden, die mit noch rückzusichernden Datensätzen in Konflikt stehen.

Sicherung einer Replik bei hohen Ansprüchen an die Verfügbarkeit

Bestehen Verfügbarkeitsanforderungen an den slapd-Server, die eine Unterbrechung des Serverbetriebs (Downtime) oder eine Beschränkung auf Lesezugriffe für den Zeitraum der Sicherung nicht zulassen, so stellt die Sicherung über eine Replik (siehe APP.2.3.M9 *Partitionierung und Replikation bei OpenLDAP*) eine gute Alternative dar. Dafür ist die oben beschriebene Vorgehensweise auf einen Consumer anzuwenden. Der Provider ist weiter verfügbar, während der Consumer angehalten wird. Nach Abschluss der Datensicherung werden beim Neustart des slapd-Servers auf dem Consumer über den "syncrepl"-Mechanismus alle in der Zwischenzeit am Provider vorgenommen Änderungen beim Consumer automatisch nachvollzogen. Unterschiede in einer gesicherten Konfiguration zwischen Provider und Consumer sind zu beachten.

Weitere Einsatzmöglichkeiten

Die hier beschriebene Datensicherung eignet sich auch gut, um damit initial eine Verzeichnisdienstreplik zu befüllen (siehe APP.2.3.M9 *Partitionierung und Replikation bei OpenLDAP*), um OpenLDAP zu aktualisieren (siehe APP.2.3.M10 *Sichere Aktualisierung von OpenLDAP*) oder die Migration zu einem anderen Verzeichnisdienst zu begleiten. In diesen Fällen ist jedoch Vorsicht geboten, wenn die Konfiguration als Teil des Verzeichnisbaums in einen Verzeichnisdienst geladen wird. Beispielsweise würde eine unangepasste Übertragung der Konfiguration eines Providers einen identischen Provider (statt eines Consumers) erzeugen, was Netzprobleme aufgrund zweier in kürzester Zeit inkonsistenter Provider zur Folge hätte.

3 Weiterführende Informationen

3.1 Wissenswertes

Einführung in OpenLDAP

OpenLDAP ist ein Verzeichnisdienst, der auf dem LDAP-Projekt der University of Michigan basiert. Das ursprüngliche Projekt hatte zum Ziel, ein Äquivalent für das Directory Access Protocol (DAP) aus dem Verzeichnisdienst-Standard X.500 zu entwickeln. DAP war auf den OSI-Stack zugeschnitten, während LDAP als Lightweight DAP, also "schlankeres" DAP den TCP/IP-Stack nutzt. Das Adjektiv "schlank" deutet dabei an, dass LDAP nicht den kompletten Funktionsumfang von X.500 DAP umsetzt. Die University of Michigan entwickelte auch einen Server, der mit dem Protokoll besonders gut umgehen kann. In diesem Zusammenhang wird von einem LDAP-Server gesprochen, obwohl LDAP eigentlich nur ein Protokoll bezeichnet. Solche Server sind als hierarchische Datenbanken darauf ausgelegt, das Protokoll LDAP besonders gut zu unterstützen und die mit dem Protokoll ausgetauschten Daten effizient zu speichern.

Open Source Software OpenLDAP

OpenLDAP ist Open Source Software. Die Entwickler von OpenLDAP haben auf der Basis des ursprünglichen Projektes der University of Michigan den Server weiterentwickelt und stellen ihre Arbeit inklusive des Quelltextes im Internet kostenlos der Allgemeinheit zur Verfügung. OpenLDAP ist auf Unix- und Linux-Betriebssystemen am weitesten verbreitet, die Software kann jedoch ebenso unter Microsoft Windows oder auf anderen Plattformen wie z/OS eingesetzt werden. Die Entwickler von OpenLDAP legen großen Wert darauf, dass die Software den LDAP-Standard einhält. Im Gegensatz zu abweichenden Implementierungen wie bei Active Directory, oder ausdrücklich abgewandelten Formen des Protokolls LDAP, wie beim Novell eDirectory, hält OpenLDAP den LDAP-Standard in der aktuellen Version 3 (LDAPv3) strikt ein. Dies zeigt sich unter anderem daran, dass OpenLDAP für Konfigurationsdateien und den Import und Export von Daten das LDAP Data Interchange Format (LDIF) verwendet. Daher wird OpenLDAP auch als Referenz-Implementation von LDAPv3 bezeichnet.

OpenLDAP unterstützt neben LDAPv3 auch den LDAP-Standard in der Version 2 (LDAPv2), garantiert dafür jedoch keine strikte Einhaltung des Standards. Zum ursprünglichen X.500 DAP bestehen keine Schnittstellen mehr. Es ist zwar grundsätzlich möglich, Daten zwischen LDAP-Servern und X.500 DAP Directory System Agents auszutauschen, OpenLDAP enthält jedoch keine entsprechende Funktion. OpenLDAP unterstützt nativ IPv4 ebenso wie IPv6, außerdem die Unix Interprozess Kommunikation (IPC).

Funktionsweise

Wie jeder LDAP-Server speichert OpenLDAP Daten in einer definierten hierarchischen Baumstruktur, dem Directory Information Tree (DIT). Das Kapitel “Einführung in Verzeichnisdienst-Grundlagen“ beschreibt die übliche Struktur und die verwendeten Begriffe. Seine Daten stellt OpenLDAP über eine Client-Server-Infrastruktur sitzungsorientiert zur Verfügung, d. h. jeder Benutzer des Verzeichnisdienstes nutzt Client-Anwendungen, um sich mit dem Server zu verbinden. Über den Client initiiert der Benutzer Operationen, wie die Suche nach einem Telefonbucheintrag oder die Änderung des eigenen Passworts. Der Server beantwortet diese Benutzeraktionen, beispielsweise indem er den gesuchten Eintrag übermittelt oder die erfolgreiche Passwortänderung bestätigt. Werden dabei Werte von Attributen gelesen oder verändert, so ist zu unterscheiden, ob es sich um normale Attribute handelt oder um so genannte operationelle Attribute, die OpenLDAP zur internen Verwaltung einsetzt. Zu Letzteren gehört zum Beispiel der Dinstinguished Name (DN) oder die Zeitstempel, die im Rahmen der Replikation von Bedeutung sind. Nachdem der Benutzer alle Operationen durchgeführt hat, wird die Verbindung zum Server beendet ("unbind" zum Ende einer Sitzung).

Architektur von OpenLDAP

Der LDAP-Server von OpenLDAP ist der slapd-Server (stand-alone LDAP daemon). Er ist neben den LDAP-Bibliotheken, die ein IT-System benötigt, um LDAP-Funktionen zu nutzen, der wichtigste Bestandteil der OpenLDAP-Software. Der slapd-Server speichert Daten des Verzeichnisdienstes nicht selbst, sondern nutzt dafür ein Datenbankmanagementsystem (DBMS), das nicht zur OpenLDAP-Software gehört.

Backends und Datenbanken

Als **Backend** wird eine Teilkomponente von OpenLDAP bezeichnet. Der slapd-Server kommuniziert nicht direkt mit einem DBMS, sondern bedient sich dafür der Funktionen eines Backends. Backends werden in der Form "back-*" benannt. Grob wird unterschieden zwischen

- Backends, die tatsächlich Daten speichern (z. B. "back-hdb" zum Zugriff auf die BerkeleyDB),
- Backends, die einen Proxy-Zugriff auf andere Datenspeicher gewähren (z. B. "back-ldap" zum Zugriff auf andere Verzeichnisdienste) und
- Backends, die Daten dynamisch generieren (z. B. "back-monitor" zur Anzeige des aktuellen Zustands von OpenLDAP).

Diese grundsätzliche Unterscheidung sollte bei der Planung der Komponenten bekannt sein, sie ist für die spätere Konfiguration und im Betrieb allerdings nicht mehr wichtig.

Unter einer **Datenbank** wird bei OpenLDAP eine Instanz eines Backends verstanden, zum Beispiel die Datenbank, in der das Teilverzeichnis "OU=BSI, O=Bund, C=DE" gespeichert ist. In der Regel können mehrere Instanzen des gleichen Backends benutzt werden, so kann es eine Datenbank für das Teilverzeichnis "I=Bonn, OU=BSI, O=Bund, C=DE" und eine für das Teilverzeichnis "I=Berlin, OU=BSI, O=Bund, C=DE" geben. Bei manchen Backends ist auch nur eine Instanz möglich, es gibt zum Beispiel nur eine "back-monitor"-Instanz zur Laufzeit. In der Praxis und auch in der Literatur über OpenLDAP werden die Begriffe Backend und Datenbank oft synonym verwendet. Es ist jedoch stets darauf zu achten, Datenbanken als logischen (Teil-)Datenbestand eines Backends nicht mit dem DBMS als eigene Softwarekomponente zu verwechseln.

Overlays

Overlays sind dafür da, das Verhalten eines bestehenden Backends zu beeinflussen, ohne das Backend selbst anpassen oder neu schreiben zu müssen. Dazu wird das Overlay dem slapd-Server vorgeschaltet, so das Nachrichten den Server gefiltert erreichen beziehungsweise verändert verlassen. Die meisten Overlays sind auf Datenbankebene anzuwenden, allerdings oft nicht auf einen Backend-Typ beschränkt.

Einen Überblick über die Architektur von OpenLDAP gibt die folgende Grafik:

Werkzeuge

Neben Bibliotheken und dem slapd-Server umfasst OpenLDAP auch eine Sammlung von Werkzeugen (Tools). Diese Werkzeuge werden in die ldap*-Werkzeuge und die slap*-Werkzeuge unterteilt.

Zu den ldap*-Werkzeugen gehören:

- ldapadd, um Einträge zu einem Verzeichnisdienst hinzuzufügen
- ldapauth, um sich an einem Verzeichnisdienst zu authentisieren
- ldapdelete, um Einträge aus einem Verzeichnisdienst zu entfernen
- ldapmodify, um bestehende Einträge in einem Verzeichnisdienst zu verändern
- ldapmodrdn, um den Distinguished Name (DN) eines Eintrags zu verändern
- ldappasswd, um das Passwort eines Personen-Objektes im Verzeichnisdienst zu verändern
- ldapsearch, um nach Einträgen im Verzeichnis zu suchen
- ldapwhoami, um die eigene Identität im Rahmen einer Sitzung auszugeben

Die ldap*-Werkzeuge nutzen das Protokoll LDAP selbst und richten Operationen als Clients immer an einen laufenden Verzeichnisdienst. Sie sind dabei vom Typ des slapd-Servers unabhängig, das heißt, sie können mit anderen LDAP-Servern kommunizieren und ihre Funktionen können wiederum durch andere Werkzeuge als die von OpenLDAP umgesetzt werden. Insbesondere werden in der Praxis grafische Werkzeuge eingesetzt.

Die slap*-Werkzeuge umfassen:

- slapacl, um die Wirksamkeit von Zugriffsrechten zu prüfen
- slapadd, um Einträge zu einem Verzeichnisdienst hinzuzufügen
- slapauth, um eine SASL-Identität gegen einen Verzeichnisdienst zu prüfen
- slapcat, um die Objekte aus einem Verzeichnisdienst zu exportieren
- slapdn, um einen Distinguished Name (DN) auf Zulässigkeit im bestehenden Verzeichnisdienst zu prüfen
- slapindex, um die Attribute (erneut) zu indizieren
- slappasswd, um zu einem Passwort den Hashwert zu generieren
- slaptest, um zu prüfen, ob eine Konfiguration syntaktisch korrekt ist

Die slap*-Werkzeuge nutzen **nicht** das Protokoll LDAP. Diese Werkzeuge arbeiten autark vom slapd-Server beziehungsweise umgehen ihn und greifen unter anderem direkt auf die Konfigurationsdateien oder die Dateien einer Datenbank zu. Die slap*-Werkzeuge sind auf den slapd-Server sowie die BerkeleyDB abgestimmt. Als Faustregel gilt, dass der slapd-Server **immer** laufen muss, wenn ldap*-Werkzeuge verwendet werden und **niemals** laufen sollte, wenn slap*-Werkzeuge eingesetzt werden.

Anpassung von OpenLDAP

OpenLDAP ist detailliert dokumentiert. Interne Zusammenhänge und Verarbeitungsschritte sind durch die Verfügbarkeit des Quelltextes bekannt. Es ist deshalb einfach möglich, Hilfsmittel für Administrationszwecke wie Skripte zu erstellen und einzusetzen. Es ist auch möglich, den Quelltext zu ändern und selbst zu übersetzen. Darüber hinaus existiert eine generische Programmschnittstelle (Application Programming Interface, API), durch die ohne Änderungen an OpenLDAP selbst eigene Backends und Overlays erstellt und genutzt werden können.

Weitere Informationen

Das IT-Grundschutz-Kompendium kann nur eine allgemeine Einführung in OpenLDAP leisten und berücksichtigt insbesondere Sicherheitsaspekte. Andere Aspekte, wie Einstellungen zur Verbesserung der Leistung werden nicht betrachtet, obwohl sie bei Planung und Installation eine große Rolle spielen können. Neben der vorhandenen Fachliteratur zu OpenLDAP ist die von den Entwicklern von OpenLDAP kostenlos bereitgestellte Dokumentation eine sehr gute Informationsquelle. Als Hauptdokument ist der zur eingesetzten Version gehörende OpenLDAP Administrator's Guide (siehe [OLDAPGUIDE]) zu nennen. Häufige Fragen und Antworten in der OpenLDAP FAQ (Frequently Asked Questions, FAQ) gesammelt (siehe [OLDAPFAQ]). In den FAQ finden sich allerdings auch Fragen und Antworten, die für eine frühere Version von OpenLDAP geschrieben wurden und aktuell nicht mehr gültig sind.

Für die umfangreichen Einstellungsmöglichkeiten und Parameter wird insbesondere auf die so genannten Manpages hingewiesen. Die Manpages von OpenLDAP werden in der Regel mit OpenLDAP zusammen installiert, sind aber auch im Internet verfügbar ([OLDAPMAPA]). Allerdings existieren zu Teilen der Software, insbesondere zu neu entwickelten Backends und Overlays, noch keine Manpages in hinreichender Qualität.

Für detailliertere Informationen oder im Problemfall empfiehlt sich ein Blick in die offiziellen Mailinglisten des Projekts [OLDAPLIST]). Die Listen können abonniert werden, ältere Nachrichten stehen unter der angegebenen Adresse auch in Archiven bereit.

Immer mehr Institutionen nutzen dezentrale, länderübergreifende oder gar weltweite Computer-Netze, um im Rahmen ihres Geschäftsbetriebs, ihrer Fachaufgaben oder Verfahren die benötigten Informationen auszutauschen und verteilte Anwendungen zu realisieren. Dabei müssen die Daten, aber auch die externen und internen Anwendungen vor Missbrauch geschützt werden.

Für den Datenaustausch innerhalb solcher Netze ist es von großer Bedeutung, dass eine Vielzahl von Informationen über die verschiedenen Kommunikationspartner, Benutzer und Ressourcen im Netz den Nutzern und Anwendungen, die diese benötigen, bereitgestellt werden. Dabei muss sichergestellt werden, dass nur autorisierte Nutzer und Anwendungen auf diese Informationen, wie beispielsweise Zertifikate, Eigenschaften usw., zugreifen können. Außerdem muss gewährleistet werden, dass die Informationen nicht manipuliert oder kompromittiert werden können. Nur dann ist sichergestellt, dass nur mit vertrauenswürdigen Partner Kommunikationsverbindungen aufgebaut und Daten hinreichend abgesichert ausgetauscht werden.

Vor allem, wenn viele gleichartige Informationen für verschiedene Verfahren zur Verfügung stehen sollen, sollten diese Daten effektiv und effizient verwaltet werden. Wenn diese Daten häufig abgerufen, aber selten geändert werden, sollte ein Verzeichnisdienst in das Netz integriert werden, um die Informationen in einer einheitlichen Art und Weise zu organisieren und gleichzeitig standardisierte Schnittstellen zu ihrer Nutzung anzubieten.

Darüber hinaus unterstützen Verzeichnisdienste "Single Sign-On", also Verfahren, die es ermöglichen, dass Benutzer nach nur einer Authentisierung ohne weitere Anmeldung auf weitere Ressourcen im Netz zugreifen können.

Heutige Verzeichnisdienste haben ihren Ursprung im X.500-Standard der International Telecommunication Union (ITU) zu Verzeichnisdiensten. X.500 wurde auch als ISO 9594 (siehe [ISO9594]) verabschiedet. Von diesem Standard haben aktuelle Verzeichnisdienste im Wesentlichen dessen internen Aufbau hinsichtlich Namens- und Datenstrukturen übernommen.

Ein Nachteil des X.500-Standards ist jedoch das komplexe Zugangsprotokoll des Verzeichnisdienstes, das Directory Access Protocol (DAP), welches zudem auf einem vollständigen ISO/OSI-Protokollstapel beruht. Als praktikable Alternative wurde das Lightweight Directory Access Protocol (LDAP) entwickelt, welches den Zugang zu Verzeichnisdiensten vereinfacht hat und so auch zu deren Popularität beigetragen hat. LDAP implementiert gegenüber DAP lediglich einen reduzierten Umfang an Funktionen und Datentypen und setzt auf einem TCP/IP-Stack auf.

LDAP hat sich inzwischen in der Version LDAPv3 als Industriestandard durchgesetzt und ist als Internetstandard im RFC 4511 (siehe [RFC4511]) spezifiziert. Praktisch alle Verzeichnisdienste bieten heute eine LDAP-Schnittstelle an, wenngleich daneben auch proprietäre Protokolle bzw. Schnittstellen zum Einsatz kommen.

Aufgrund des Protokolls werden Verzeichnisdienst-Server im administrativen Sprachgebrauch gelegentlich auch als LDAP-Server bezeichnet.

Verzeichnisdienste sind wie eine hierarchische Datenbank organisiert. Die hierarchische Gliederung der Objekte erfolgt in Form eines Baumes, wobei die einzelnen Knotenpunkte des Verzeichnisbaums aus den Container-Objekten bestehen, welche wiederum andere Objekte enthalten können. Die so genannten Leaf-Objekte (Blätter) stellen die Endpunkte des Verzeichnisbaums dar. Die Objekte (Einträge, Entries) bilden den "Directory Information Tree" (DIT). Jedes Objekt besitzt dabei einen eindeutigen Namen, den sogenannten Distinguished Name (DN).

Beispiel: "cn=Max Mustermann, l=Bonn, ou=BSI, o=Bund, c=DE"

Innerhalb einer Ebene können die Objekte durch den Relative Distinguished Name (RDN), z. B. "cn=Max Mustermann", unterschieden werden.

Die Objekte enthalten ihrerseits Eigenschaften (Attribute). Den Attributen werden schließlich Werte zugewiesen, zum Beispiel: "mail: max.mustermann@bsi.bund.de".

Jedem Eintrag im Directory Information Tree (DIT) ist mindestens eine Objektklasse (ObjectClass) zugeordnet, wie z. B. "objectClass inetOrgPerson". Es gibt Objektklassen, die als "Container" für weitere Einträge dienen können, und solche, die sich als "Blattobjekte" an den Enden der Äste in der Baumstruktur des DIT befinden. Der Directory Information Tree stellt innerhalb der Verzeichnisdienst-Struktur eine Grenze des Einflusses von Administratoren und somit auf den Verzeichnisdienst an sich dar.

In den Objektklassen sind Attribute definiert, die für entsprechende Einträge zur Verfügung stehen. Durch die Zuordnung der Attribute zu Objektklassen wird gesteuert, welche Attribute für die Einträge zur Verfügung stehen. Es gibt Attribute, die einen Wert erhalten müssen, und andere, die leer bleiben können. Beispielsweise kann das Attribut "mail", das in der Objektklasse "inetOrgPerson" deklariert wird, leer bleiben.

Es gibt Abhängigkeiten zwischen Objektklassen. Damit etwa die weit verbreitete Objektklasse "inetOrgPerson" verwendet werden kann, muss zunächst die Objektklasse "organizationalPerson" deklariert werden, diese wiederum braucht die Objektklasse "person" und diese die Objektklasse "top". Die im RFC 2798 definierte Objektklasse "inetOrgPerson" ist eine der meist genutzten Klassen, um in LDAP Personen in ihrem organisatorischen Umfeld darzustellen.

Die Definitionen der Objektklassen werden in einem so genannten Schema festgehalten. Ein Schema definiert jeweils Objektklassen mit ihren verbindlichen oder optionalen Attributen. Schemata werden in so genannten Schemadateien gespeichert. So ist beispielsweise die Objektklasse "inetOrgPerson" mit ihren Attributen in der Datei "inetorgperson.schema" beschrieben. Verzeichnisdienste liefern mit ihren Installationspaketen bereits eine Menge an Schemadateien mit. Nichtsdestotrotz besteht die Möglichkeit, bei Bedarf Schemata zu erweitern oder ein eigenes Schema zu entwickeln.

Sollen Veränderungen an der Definition einzelner Objektklassen vorgenommen werden, z. B. durch Erweiterung des zugehörigen Attributsatzes, so geschieht dies über eine Änderung bzw. Erweiterung des Schemas. Somit ist eine Schemaänderung gewissermaßen die sensibelste Operation überhaupt, welche an einem Verzeichnisbaum vorgenommen werden kann. Eine solche Änderung hat Auswirkungen auf den gesamten Baum, so dass die bisherige Konzeption des Baums neu überdacht werden muss. Die Administration des Verzeichnisdienst-Schemas verlangt daher eine hohe Kompetenz im Verzeichnisdienst sowie ein sehr hohes Sicherheitsbewusstsein.

Auch wenn die Daten eines Verzeichnisdienstes in einer Datenbank gespeichert sind, besitzen Verzeichnisse einige Eigenschaften, die sie von anderen, insbesondere relationalen Datenbanken (siehe Baustein APP.4.3 *Relationale Datenbanksysteme*) unterscheiden:

- Verzeichnisdienste sind in hierarchischer Art und Weise organisiert, in denen die Objekte mit ihren Attributen als Einträge abgelegt sind. Die Objekte eines Verzeichnisdienstes bilden die realen Objekte (z. B. Benutzer oder Rechner) eines Netzes nach. Die Beziehungen der Objekte untereinander werden durch die Baumstruktur ihrer Einträge widergespiegelt.
- Verzeichnisdienste verwenden eine bestimmte genormte Struktur, die gegebenenfalls erweitert werden kann. Die Struktur wird durch das verwendete Schema definiert. Ein Schema definiert jeweils Objektklassen mit ihren verbindlichen oder optionalen Attributen. Diese Attribute können mehrwertig sein, also auch mehrere Werte annehmen.
- Verzeichnisdienste bieten einen einfachen und schnellen Weg für einfach strukturierte suchende und lesende Anfragen. Um mit einem Verzeichnisdienst in Kontakt zu treten, werden Netzprotokolle verwendet. Die meisten Verzeichnisdienste unterstützen hierzu das Lightweight Directory Access Protocol (LDAP), genutzt werden häufig aber auch proprietäre Protokolle und Software-Schnittstellen.
- Verzeichnisdienste stellen ein fein-granulares Sicherheitsmodell bereit. Zugriffsrechte können beispielsweise für einen Eintrag definiert werden und dann für alle darunter liegenden Einträge im Verzeichnisbaum übernommen werden.
- Verzeichnisdienste sind zwar Datenbanken, unterstützen aber keine verteilten Transaktionen oder Rollback-Operationen (Zurücksetzen). Zugunsten einer höheren Verfügbarkeit in einer verteilten Umgebung können weder Objekte noch ihre Attribute für eine Änderung gesperrt werden. Zumindest zeitliche Inkonsistenzen zwischen Datenbank-Repliken werden dafür in Kauf genommen.

Gegenüber hierarchischen Datenbanken, wie sie typischerweise für Verzeichnisdienste Verwendung finden, bieten relationale Datenbanken u. a. folgende Merkmale:

- Mit der Abfragesprache SQL sind komplexere Möglichkeiten von Operationen, wie z. B. "Aggregation" zur Zählung und "Join" zur Verknüpfung gegeben.
- Die Daten liegen in einer Normalform vor, es gibt keine mehrwertigen Attribute.
- Relationale Datenbanken sind für zusammengesetzte und konkurrierende Schreiboperationen aufgrund von Locking-Mechanismen und Transaktionen geeignet.

Verzeichnisdienste sind für kurze Verbindungen und einfache Abfragen beispielsweise zur Existenz von Ressourcen, Werten von Attributen oder Lesen von ganzen Objekten prädestiniert.

Aus dieser Gegenüberstellung folgt daher, dass Verzeichnisdienste beispielsweise nicht für eine Personalverwaltung eingesetzt werden sollten, auch wenn viele Attribute von Personen innerhalb einer Institution von dem Verzeichnisdienst zur Verfügung gestellt werden. Dazu gehören z. B. die Zuordnung von Benutzern zu Telefonnummer, E-Mail-Adresse, Abteilung, aber auch zu Login-Namen, Passwörtern oder Zertifikaten. Andere Eigenschaften wie Gehaltsstufe, Kontonummer, Urlaubstage oder Arbeitszeitvereinbarungen sind hingegen Daten der Personalverwaltung, die nicht Bestandteil eines Verzeichnisdienstes sein sollten.

Somit können einzelne, für den Verzeichnisdienst relevante Daten auch über andere relationale Datenbanken einer Institution, wie im obigen Beispiel die Datenbank für die Verwaltung der Personaldaten, gepflegt werden. Dadurch können Abhängigkeiten zwischen der Datenbank des Verzeichnisdienstes und anderer Datenbanken entstehen. Im Rahmen der Datensicherung und auch bei der Notfallvorsorge ist daher darauf zu achten, von welchen anderen Datenbanken der Verzeichnisdienst seine Einträge erhält.

Zugriffsrechte und Vererbung

Jedem einzelnen Objekt und jeder Objektklasse eines Verzeichnisdienstes können Zugriffsrechte auf die einzelnen Attribute des Objektes erteilt werden. Die explizite Zuweisung erfolgt dabei durch Eintragung von Rechteinhabern in die Access Control List (ACL). Mögliche Rechte reichen dabei von Supervisor, d. h. einem vollständigen Administrationsrecht, bis hin zum Browsen, was das Durchlaufen des entsprechenden Verzeichnisbaum-Abschnittes gestattet. Die Zugriffsrechte auf die Objekte vererben sich dabei standardmäßig in der Baumhierarchie von oben nach unten. Einfluss auf den Vererbungsprozess kann durch das Einführen von Filtern genommen werden, die auch die automatische Vererbungen explizit unterbinden können.

Effektive Rechte

Letztendlich kommen beim Verzeichnisdienst-Zugriff die effektiven Rechte eines Benutzers bzw. einer Benutzergruppe zum tragen. Die effektiven Rechte werden dabei dynamisch bei jedem einzelnen Zugriff berechnet und basieren auf den dem Benutzer bzw. der Benutzergruppe zugewiesenen Rechten.

Authentisierung

Die Benutzer greifen über geeignete Client-Software auf den Verzeichnisdienst zu. Der Zugriff der Clients auf den Verzeichnisdienst erfolgt dabei über proprietäre Protokolle, dabei wird der private Schlüssel des sich anmeldenden Benutzers vom Verzeichnisdienst verschlüsselt an den Client geschickt. In den Verschlüsselungsvorgang wird das Benutzerpasswort einbezogen. Gibt der Benutzer sein Passwort ein, kann der Client den privaten Schlüssel entschlüsseln. Zwischen dem Client und dem Verzeichnisdienst-Server findet ein so genanntes Challenge-Response-Verfahren zur Authentisierung statt. Nach erfolgreicher Authentisierung besitzt der Benutzer die für ihn definierten Zugriffsrechte auf den Verzeichnisdienst.

LDAP-Zugriff

Netzapplikationen und Internet-Benutzer greifen in der Regel über das LDAP-Protokoll (Lightweight Directory Access Protocol) auf den Verzeichnisdienst zu. Hierbei gibt es verschiedene Anbindungsarten, wie beispielsweise den "anonymous bind" oder den "proxy user anonymous bind". In der Voreinstellung hat der anonyme Login dabei die Rechte des anonymen Benutzers. Standardmäßig besitzt dieser uneingeschränkte Lese-Rechte auf den gesamten Verzeichnisbaum. Eine Authentisierung ist für die anonyme Anmeldung nicht erforderlich, dies sollte bei weiteren Sicherheitsbetrachtungen berücksichtigt werden.

Die Passwort-Authentisierung kann so konfiguriert werden, dass das Passwort entweder im Klartext übertragen werden darf oder nicht. Passwörter sollten nie im Klartext übertragen werden. Für eine gesicherte Anbindung mittels Lightweight Directory Access Protocol steht das Secure Sockets Layer Protokoll (SSL-Protokoll) wahlweise mit ein- oder zweiseitiger Authentisierung zur Verfügung.

Zertifikatsserver

Ein Zertifikatsserver spielt eine wichtige Rolle für die Rechtevergabe und damit für die Systemsicherheit. Ebenso hängen die Authentisierungen im Netz sowie der Aufbau eines verschlüsselten Kanals (via Secure Sockets Layer, SSL) vom Zertifikatsmanagement ab. Daher erfordert der Zertifikatsserver eine besonders sorgfältige Administration.

Partitionierung

Zur Verbesserung der Skalierbarkeit und Leistungsfähigkeit des Verzeichnisdienstes empfiehlt sich eine Partitionierung der Verzeichnisdatenbank auf mehrere Server. Für die Partitionierung sind eine Reihe von Regeln zu beachten, wie beispielsweise bereits im Baustein APP.2.1 *Allgemeiner Verzeichnisdienst* beschrieben.

Replikation

Verzeichnisdienste unterstützen verschiedene Arten von Replikationen zur Erhöhung der Fehlertoleranz und des Systemdurchsatzes. Aspekte der Replikation sind auch im Baustein APP.2.1 *Allgemeiner Verzeichnisdienst* beschrieben.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "OpenLDAP" finden sich unter anderem in folgenden Veröffentlichungen:

[ISO9594] ISO/IEC 9594-8:2017

International Organization for Standardization (Hrsg.), Information technology – Open System Interconnection – The Directory – Part 8: Publiy-key and attribute certification framework, ISO/IEC JTC 1/SC 6, 05-2017

[MASTERAR] Konzeption und Erstellung eines IT-Grundschutz-Bausteins für den Verzeichnisdienst OpenLDAP:

Masterarbeit, Ruhr-Universität-Bochum, Juli 2010, httsp://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Extern/Diplomarbeiten/OpenLDAP_Steinkamp.pdf, zuletzt abgerufen am 18.07.2018

[OLDAPFAQ] OpenLDAP: Frequently Asked Questions

https://www.openldap.org/faq, zuletzt abgerufen am 18.07.2018

[OLDAPLIST] OpenLDAP: Mailingliste

https://www.openldap.org/lists/openldap-announce, zuletzt abgerufen am 18.07.2018

[OLDAPMAPA] OpenLDAP: Manual Pages

https://www.openldap.org/software/man.cgi, zuletzt abgerufen am 18.07.2018

[OLDAPTRACK] OpenLDAP: Issue Tracking System

httsp://www.openldap.org/its, zuletzt abgerufen am 18.07.2018

[OLDPGUID] OpenLDAP: Administrator´s Guide

https://www.openldap.org/doc, zuletzt abgerufen am 18.07.2018

[OpenLDAP] OpenLDAP: community developed LDAP software

https://www.openldap.org/, zuletzt abgerufen am 18.07.2018

[RFC2849] The LDAP Data Interchance Format (LDIF)

Technical Specification, RFC2849, June 2000

[RFC4511] Network Working Group

Lightweight Directory Access Protocol (LDAP): The Protocol, RFC4511, June 2016

APP.3: Netzbasierte Dienste

Umsetzungshinweise zum Baustein APP.3.6 DNS-Server

1 Beschreibung

1.1 Einleitung

Diese Umsetzungshinweise decken die grundsätzlichen Sicherheitseigenschaften des Domain Name System (DNS) und der hierfür benötigten Server ab. DNS ist ein Netzdienst, der dazu eingesetzt wird, Hostnamen von IT-Systemen in IP-Adressen umzuwandeln. Üblicherweise wird zu einem Hostnamen die entsprechende IP-Adresse gesucht (Vorwärtsauflösung). Ist hingegen die IP-Adresse bekannt und der Hostname wird gesucht, wird dies als Rückwärtsauflösung bezeichnet. Die Bezeichnung DNS-Server steht im eigentlichen Sinne für die verwendete Software, wird jedoch meist auch als Synonym für den Rechner benutzt, auf dem diese Software betrieben wird.

DNS-Server können nach ihren Aufgaben unterschieden werden, dabei gibt es grundsätzlich zwei verschiedenen Typen: Advertising DNS-Server und Resolving DNS-Server. Advertising DNS-Server sind üblicherweise dafür zuständig, Anfragen aus dem Internet zu verarbeiten. Resolving DNS-Server hingegen verarbeiten Anfragen aus dem internen Netz.

Ein Ausfall eines DNS-Servers kann sich gravierend auf den Betrieb einer IT-Infrastruktur auswirken. Dabei ist nicht direkt das ausgefallene DNS-System problematisch, sondern die daraus resultierende Einschränkung DNS-basierter Dienste. Unter Umständen sind Webserver, E-Mail-Server nicht mehr erreichbar und die Fernwartung funktioniert nicht mehr. Da DNS von sehr vielen Netzanwendungen benötigt wird, müssen laut Spezifikation (RFC 1034) mindestens zwei autoritative DNS-Server (Advertising DNS-Server) für jede Zone betrieben werden.

Da eine funktionierende Namensauflösung eine Grundvoraussetzung für viele Anwendungen und damit für einen reibungslosen Betrieb ist, sollten DNS-Server sorgfältig geplant, umgesetzt und fachgerecht betrieben werden. Deshalb liegt der Fokus dieser Umsetzungshinweise auf der Verfügbarkeit von DNS-Servern und der Integrität der übertragenen Informationen sowie auf Problemen, die im Zuge eines DNS-Server-Betriebs auftreten können.

1.2 Lebenszyklus

Planung und Konzeption

Bevor ein DNS-Server ausgewählt und die Infrastruktur geplant wird, sollte geprüft werden, ob der gewünschte Domainname im Besitz der Institution bzw. noch verfügbar ist (siehe APP.3.6.M8 *Verwaltung von Domainnamen)*. Soll DNS Security Extensions (DNSSEC) eingesetzt werden, sollte die Maßnahme APP.3.6.M17 *Einsatz von DNSSEC* umgesetzt werden. Bei der Planung wird festgelegt, wie die DNS-Server in die Netzinfrastruktur des Informationsverbunds integriert werden (siehe APP.3.6.M1 *Planung des DNS-Einsatzes*). Im Weiteren sollte entschieden werden, wie hoch die Leistungskapazität eines DNS-Servers sein muss. Das betrifft einerseits das IT-System selbst und andererseits die Übertragungskapazität der Netzanbindung (siehe APP.3.6.M11 *Ausreichende Dimensionierung der DNS-Server*).

Beschaffung

Es gibt unterschiedliche Softwareprodukte im Bereich der DNS-Server. Um eine geeignete Wahl zu treffen, muss überprüft werden, ob die potenziellen Produkte alle benötigten Funktionen haben und alle Sicherheitsanforderungen mit ihnen erfüllbar sind (siehe APP.3.6.M10 *Auswahl eines geeigneten DNS-Server-Produktes*).

Umsetzung

Nachdem die Planung abgeschlossen und die Software auf dem Betriebssystem des Servers installiert ist, muss der DNS-Server sicher eingerichtet und konfiguriert werden (siehe APP.3.6.M4 *Sichere Grundkonfiguration eines DNS-Servers*, APP.3.6.M6 *Absicherung von dynamischen DNS-Updates* und APP.3.6.M13 *Einschränkung der Sichtbarkeit von Domain-Informationen*). Darüber hinaus sollten die verantwortlichen Mitarbeiter geschult werden, damit sie mit den für sie relevanten Sicherheitsmaßnahmen ausreichend vertraut sind (siehe APP.3.6.M12 *Schulung der Verantwortlichen*).

Betrieb

Während des laufenden Betriebs ist es wichtig, sich über aktuelle Sicherheitslücken zu informieren, um eventuell vorhandene Softwareaktualisierungen zu installieren oder anderweitige Sicherheitsvorkehrungen umzusetzen (siehe APP.3.6.M5 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*). Weiterhin sollte durch Paketfilterregeln die Kommunikation des DNS-Servers mit anderen DNS-Servern und Clients auf ein Minimum beschränkt werden (siehe APP.3.6.M16 *Integration eines DNS-Servers in eine "P-A-P"-Struktur*). Um einen reibungslosen Betrieb zu gewährleisten und eventuelle Störungen oder Anomalien festzustellen, ist es notwendig den DNS-Server laufend zu überwachen und dessen Protokolldaten regelmäßig auszuwerten (siehe APP.3.6.M7 *Überwachung von DNS-Servern* und APP.3.6.M15 *Auswertung der Logdaten*).

Wenn ein DNS-Server konfiguriert wird oder die DNS-Informationen manuell geändert werden, sollten vorher die Domain-Informationen gesichert werden, um sie, falls erforderlich, wieder zurückspielen zu können.

Aussonderung

Werden DNS-Server außer Betrieb gesetzt, sollten diese geregelt entsorgt werden (siehe APP.3.6.M19 *Aussonderung von DNS-Servern*).

Notfallvorsorge

Im Rahmen der Notfallvorsorge sollten Notfallpläne für die relevanten Gefährdungslagen erstellt werden (siehe APP.3.6.M9 *Erstellen eines Notfallplans für DNS-Server*). Außerdem müssen Advertising DNS-Server redundant ausgelegt werden (siehe APP.3.6.M2 *Einsatz redundanter DNS-Server*).

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "DNS-Server" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

APP.3.6.M1 Planung des DNS-Einsatzes

Um DNS-Server sicher umzusetzen, muss eine angemessene Planung im Vorfeld stattfinden. Hierzu ist zunächst ein Konzept zu erstellen, das unter anderem beschreibt, wie DNS aufgebaut werden soll und welche Domain-Informationen schützenswert sind. Hierbei sollten die Verantwortlichen auch festlegen, wie DNS in das Netz des Informationsverbundes eingebunden werden soll. Es sind jedoch nicht nur Aspekte zu planen, die direkt mit dem Begriff Sicherheit verknüpft sind, sondern darüber hinaus auch normale betriebliche Gesichtspunkte, die Anforderungen im Bereich der Sicherheit nach sich ziehen können.

APP.3.6.M2 Einsatz redundanter DNS-Server

Um eine hohe Ausfallsicherheit zu gewährleisten, muss auf eine ausreichende Hardware-Redundanz geachtet werden. Deswegen sollte es immer mindestens zwei getrennte Advertising DNS-Server geben. Die Ausfallsicherheit lässt sich weiter erhöhen, wenn die Server räumlich getrennt werden.

APP.3.6.M3 Verwendung von separaten DNS-Servern für interne und externe Anfragen

Advertising und Resolving DNS-Server übernehmen unterschiedliche Aufgaben und sollten daher auch unbedingt getrennt werden. Es empfiehlt sich daher für Advertising und für Resolving DNS-Server jeweils eigene physische Server einzusetzen. Der Advertising DNS-Server verwaltet die von außen verfügbaren Domain-Informationen und unterstützt nur iterative Anfragen, der Resolving DNS-Server verwaltet die nach innen sichtbaren Informationen und unterstützt sowohl iterative als auch rekursive Anfragen.

Clientanwendungen benötigen einen Resolver, um DNS zu nutzen. Dieser ist standardmäßig in den gängigen Betriebssystemen integriert. Es muss jedoch sicher gestellt werden, dass die Resolver der internen IT-Systeme die internen Resolving DNS-Server zur Namensauflösung verwenden. Sie sollten auf keinen Fall standardmäßig externe DNS-Server befragen. Zusätzlich sollten im Zuge dessen auch die DNS-Suffixe, die von den Resolvern verwendet werden, festgelegt werden, beispielsweise *bsi.bund.de*. Dadurch wird bei der Namensauflösung von *hostx* automatisch der Rest des Domainnamens zum Fully Qualified Domain Name (FQDN) *hostx.bsi.bund.de* ergänzt.

APP.3.6.M4 Sichere Grundkonfiguration eines DNS-Servers

-Server stellen attraktive Ziele für Angreifer dar. Wenn sie es schaffen, diese Server zu manipulieren, können dadurch alle Dienste beeinflusst werden, die DNS verwenden, zum Beispiel Webserver, E-Mail-Server oder Remote-Administrationsanwendungen. Deshalb ist eine sorgfältige Grundkonfiguration der DNS-Server unerlässlich.

DNS-Server-Version

Die Version des verwendeten DNS-Server-Produktes kann einem Angreifer wertvolle Informationen liefern. Daher sollte die Versionsnummer verborgen werden, beispielsweise indem sie durch *unknown* ersetzt wird. Diese Maßnahme erhöht zwar nicht direkt das Sicherheitsniveau eines DNS-Servers, erschwert einem Angreifer aber die Informationsbeschaffung.

Anfragen

Eine erhöhte Gefahr durch Cache-Poisoning-Angriffe besteht dann, wenn DNS-Server bedingungslos Anfragen akzeptieren. Daher ist es wichtig einzuschränken, welche Anfragen akzeptiert werden.

Resolving DNS-Server sind für Anfragen von Resolvern aus dem Netz der Institution zuständig, in der Regel handelt es sich dabei um rekursive Anfragen. Das bedeutet, dass Resolving DNS-Server rekursive Anfragen aus dem internen Netz akzeptieren müssen. Anfragen aus dem Internet dürfen nicht akzeptiert werden, da hierfür der Advertising DNS-Server zuständig ist.

Anfragen mit Ursprung aus dem Internet müssen immer iterativ behandelt werden, dadurch liefert der Advertising DNS-Server nur Informationen über seine verwalteten Zonen und kann keine gefälschten Antworten versenden.

Um das Sicherheitsniveau von Resolving DNS-Servern zu erhöhen, muss ein weiterer Mechanismus eingesetzt werden. Wie bereits erwähnt, müssen Resolving DNS-Server rekursive Anfragen von institutionsinternen IT-Systemen akzeptieren. Resolving DNS-Server werden also zwangsläufig Namen auflösen müssen, für die sie nicht autoritativ sind. Ein Angreifer könnte hier gefälschte Antworten einschleusen. Die Zuordnung von Antworten zu Anfragen erfolgt über:

- IP-Adresse
- ID der Anfrage (Zufallszahl)
- Source Port der Anfrage

Da IP-Adresse und ID zu wenig Schutz bieten, sind zusätzlich zufällige Source Ports zu verwenden, wenn Anfragen versendet werden. Aktuell wird auch dazu übergegangen, mehrere IP-Adressen für Resolving DNS-Server zu konfigurieren und diese zu randomisieren.

Zonentransfers

Grund und Ziel von Zonentransfers ist, Primary DNS-Server und Secondary DNS-Server miteinander zu synchronisieren. Der Primary DNS-Server liest die Domain-Informationen aus den Zonendateien aus, über einen Zonentransfer gelangen diese auf den oder die Secondary DNS-Server und werden somit synchron gehalten. Es muss sicher gestellt werden, dass der Zonentransfer zwischen dem Primary und dem Secondary DNS-Server auch wirklich funktioniert.

Um zu verhindern, dass unberechtigte Personen einen Zonentransfer starten und somit die gesamten Domain-Informationen einer Zone erhalten, müssen Zonentransfers so konfiguriert werden, dass diese nur zwischen Primary und Secondary DNS-Servern möglich sind. Dies muss zumindest über die Beschränkung auf die IP-Adressen der DNS-Server erfolgen, noch sicherer ist es Transaction Signatures (siehe APP.3.6.M18 *Erweiterte Absicherung von Zonentransfers*) zu verwenden.

Die Einschränkungen über IP-Adressen sehen wie folgt aus: Am Primary DNS-Server muss für jede Zone konfiguriert werden, welche die dazu gehörenden Secondary DNS-Server sind. Dies erfolgt über die Angabe einer oder mehrerer IP-Adressen. Auf dem oder den Secondary DNS-Servern für eine Zone muss konfiguriert werden, welcher der dafür zuständige Primary DNS-Server ist.

Um zu gewährleisten, dass der Zonentransfer funktioniert, sollte nach jeder Änderung an den Einstellungen für den Zonentransfer die einwandfreie Funktion überprüft werden. Dazu kann beispielsweise ein Zonentransfer durchgeführt werden. Danach wird in den Logdateien überprüft, ob Fehler aufgetreten sind. Bei nicht allzu umfangreichen Zonen ist es möglich, die vom Primary DNS-Server verwalteten Domain-Informationen händisch mit denen des Secondary DNS-Servers zu vergleichen.

Ausschließen bestimmter DNS-Server

Sind DNS-Server bekannt, die falsche Domain-Informationen liefern, muss verhindert werden, dass die Resolving DNS-Server der Institution, Anfragen an diese DNS-Server senden. Werden private IP-Netze wie *10/8, 172.16/12* und *192.168/16* in der Institution nicht genutzt, sollten aus Sicherheitsgründen Anfragen aus diesen Netzen ignoriert werden.

APP.3.6.M5 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates

Die Verantwortlichen müssen sich über aktuelle Sicherheitslücken in der eingesetzten Software frühzeitig informieren. Idealerweise sollten hierzu mindestens zwei verschiedene Informationsquellen, darunter auch eine herstellerunabhängige genutzt werden. Unter können beispielsweise alle bisher publizierten Schwachstellen im DNS-Server-Produkt BIND nachgelesen werden.

Bei Produkten, für die vom Hersteller (noch) keine Sicherheitspatches verfügbar sind, muss rechtzeitig geprüft werden, ob es noch zu verantworten ist, sie einzusetzen. Auch muss dann geprüft werden, welche zusätzlichen Maßnahmen umgesetzt werden können, um die betroffenen Systeme trotzdem zu schützen.

Bevor Updates oder Patches installiert werden, ist stets eine Datensicherung des Systems zu erstellen, die es ermöglicht, den Originalzustand wieder herzustellen, falls Probleme auftreten. Vorab muss auf einem Testsystem überprüft werden, ob die Sicherheitsupdates kompatibel sind und keine Fehler verursachen.

Es sollte dokumentiert werden, wann, von wem und aus welchem Anlass Patches und Updates eingespielt wurden. Aus der Dokumentation muss sich der aktuelle Patchlevel des Systems jederzeit schnell ermitteln lassen. So können sich die Verantwortlichen schnell darüber klar werden, ob eine neue Schwachstelle auch die eigenen Systeme gefährdet.

APP.3.6.M6 Absicherung von dynamischen DNS-Updates

Um dynamische Updates sicher nutzen zu können, muss gewährleistet sein, dass nur legitimierte IT-Systeme Änderungen an Domain-Informationen vornehmen können. Des Weiteren muss festgelegt werden, welche Domain-Informationen die einzelnen IT-Systeme ändern dürfen. Um sicherzustellen, dass Domain-Informationen nicht von unautorisierten IT-Systemen mithilfe von dynamischen Updates manipuliert werden, stehen zwei Möglichkeiten zur Verfügung:

- Beschränkung der berechtigten Hosts mittels IP-Adressen,
- Beschränkung der berechtigten Hosts mithilfe von TSIG (siehe APP.3.6.M18 Erweiterte Absicherung von Zonentransfers).

Bei der Beschränkung mittels IP-Adresse wird über die IP-Adresse die Quelle des dynamischen Updates identifiziert. Bei TSIG wird symmetrische Verschlüsselung benutzt, um die Quelle des dynamischen Updates zu identifizieren.

Neben der Anfälligkeit für IP-Spoofing gibt es bei der Verwendung von IP-Adressen ein weiteres Problem. Secondary DNS-Server können als Forwarder für dynamische Updates eingerichtet und der Primary DNS-Server so konfiguriert werden, dass er nur Updates von den Secondary DNS-Servern akzeptiert. Weil nur auf den Secondary DNS-Servern konfiguriert wird, von welchen IT-Systemen Updates akzeptiert werden, bleibt es dem Primary DNS-Server verborgen, woher die Updates stammen. Somit ist es nicht möglich, aufgrund der originalen Quelle einzuschränken, welche Hosts dynamische DNS-Updates vornehmen dürfen.

Neben der Identifikation der Quelle muss konfiguriert werden, welche Domain-Informationen verändert werden dürfen. Die Regeln müssen so konfiguriert werden, dass dynamische Updates reibungslos einsetzbar sind. Ein DHCP-Server benötigt beispielsweise die Berechtigung, die Zuordnung von Domainnamen und IP-Adressen zu ändern, jedoch besteht kein Grund einem DHCP-Server zu erlauben, den zuständigen DNS-Server für eine Zone zu ändern.

APP.3.6.M7 Überwachung von DNS-Servern

Um die Sicherheit eines DNS-Servers auch im Betrieb aufrecht zu erhalten, reicht es nicht aus, sich nur auf eine sorgfältige Planung und Anfangskonfiguration zu verlassen. Es müssen eine Reihe von Maßnahmen durchgeführt werden, um eventuelle Probleme und sicherheitskritische Lücken aufzudecken.

Die Kapazitätsanforderungen sollten bereits in der Planung festgelegt werden. Aufgrund der Tatsache, dass die Kapazitätsanforderungen von der

- Größe der Zone(n),
- Anzahl der Anfragen,
- Anzahl der rekursiven Anfragen,
- Anzahl der Zonentransfers,
- Anzahl der dynamischen Updates etc.

abhängen, ist es schwierig die benötigten Kapazitäten zu planen. Daher muss regelmäßig überwacht werden, wie ausgelastet ein DNS-Server ist, um falls erforderlich die Leistungskapazität der Hardware anzupassen. Des Weiteren kann eine erhöhte Auslastung ein Indikator für einen laufenden Angriff sein. Die Kommunikation des DNS-Servers ist daher geeignet zu protokollieren. Die Protokollierung sollte beispielsweise die Anzahl der Anfragen, Zonentransfers, dynamische Updates etc. umfassen (siehe OPS.1.1.7 *Protokollierung*).

APP.3.6.M8 Verwaltung von Domainnamen [Leiter IT]

Internet-Domainnamen (kurz: Domains) müssen bei Registrierungsstellen (Registraren) angemeldet werden. Eine Registrierungsstelle kann Namen für eine oder mehrere sogenannte Top-Level-Domains vergeben, z. B. die klassischen Domains *.com, .org, .gov* und die diversen Länder-Domains wie *.de* für Deutschland, *.at* für Österreich und *.ch* für die Schweiz. Domains werden jeweils für einen bestimmten Zeitraum registriert. Ist dieser Zeitraum abgelaufen, so muss die Registrierung gegen Zahlung einer Gebühr verlängert werden. Wird vergessen, eine Registrierung zu verlängern, kann das unangenehme Folgen haben. Es muss daher sichergestellt sein, dass die Registrierungen für alle Domains, die von einer Institution benutzt werden, regelmäßig und rechtzeitig verlängert werden. Dazu sollte in jeder Institution eine Stelle festgelegt werden, die die Verwaltung der Domainnamen bei den verschiedenen Registrierungsstellen koordiniert.

Für mehrere Top-Level-Domains (etwa *.com* und *.org*) gibt es verschiedene Registrierungsstellen. Ein Wechsel der Registrierungsstelle ist jederzeit möglich, aber meist mit Kosten verbunden. Es ist wichtig, für alle registrierten Domains einen Überblick über die jeweilige Laufzeit der Registrierung und den Preis für die Verlängerung zu haben, um eine rechtzeitige Verlängerung der Registrierung sicherzustellen.

Verhinderung von Domain-Grabbing

Wenn eine Institution ihre Domains nicht selbst registriert und verwaltet, sondern dies über einen Internetdienstleister abwickelt, muss sie bei der Vertragsgestaltung darauf achten, die Kontrolle über ihre Domains zu behalten. Das kann beispielsweise bei einem eventuellen Wechsel des Registrars oder bei der Auflösung von Namensstreitigkeiten wichtig sein.

Bei Fehlern und Versäumnissen des Dienstleisters bei der Verwaltung von Domainnamen müssen entsprechende Regelungen getroffen werden, da in solchen Fällen erheblicher Schaden entstehen kann.

Falls die Nameserver nicht in der Institution selbst betrieben, sondern bei einem Dienstleister gehostet werden, sollten in den Service-Level-Agreements insbesondere Anforderungen an die Verfügbarkeit der Nameserver und an die Bearbeitungszeiten für Änderungen im DNS der Institution definiert werden.

APP.3.6.M9 Erstellen eines Notfallplans für DNS-Server

Fällt der Netzdienst DNS in einem Informationsverbund aus, wirkt sich das gravierend auf den Betrieb der IT-Infrastruktur aus. Dabei ist nicht direkt das ausgefallene DNS-Systems problematisch, sondern die daraus resultierende Einschränkung DNS-basierter Dienste. Unter Umständen sind Webserver nicht mehr erreichbar und die Fernwartung funktioniert nicht mehr.

Je nachdem welche DNS-Server ausfallen, funktioniert die Namensauflösung innerhalb der Institution und/oder von außerhalb nicht mehr. Funktioniert die Namensauflösung von außerhalb nicht mehr, wird dies meistens schnell öffentlich bekannt werden, was bei regelmäßigen oder längeren Ausfällen einen Imageschaden zur Folge haben kann.

Es ist daher ein Konzept zu entwerfen, wie bei einem Ausfall die daraus resultierenden Folgen minimiert werden können. Darin sollten folgende Aspekte berücksichtigt werden:

- Die Notfallplanung für DNS-Server muss in den existierenden Notfallplan integriert werden.
- Ein Systemausfall kann zu Datenverlusten führen. Daher ist ein Datensicherungskonzept für die Zonendateien zu erstellen. Dieses ist in das existierende Datensicherungskonzept zu integrieren.
- Neben dem Notfallplan für den DNS-Server muss auch für das darunter liegende Betriebssystem ein Notfallplan existieren.
- Für den Betrieb eines DNS-Servers für Anfragen aus dem Internet wird eine funktionierende Internetanbindung vorausgesetzt.
- Die Systemkonfiguration ist zu dokumentieren. Wichtige Aufgaben müssen so beschrieben sein, dass das Gesamtsystem im Notfall von IT-Angestellten auch ohne vorherige Kenntnis dieser Systemkonfiguration wiederhergestellt werden kann.
- War die Störung das Resultat eines Angriffs, muss die Schwachstelle behoben und dokumentiert werden.
- Es muss ein Wiederanlaufplan erstellt werden, damit das oder die IT-System(e) wieder geregelt hochgefahren werden kann/können.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "DNS-Server".

APP.3.6.M10 Auswahl eines geeigneten DNS-Server-Produktes

DNS-Server-Produkte unterscheiden sich hinsichtlich ihres Leistungsumfangs und des Bedienkomforts. Wenn ein solches Produkt beschafft wird, sollte auf folgende Aspekte geachtet werden:

- Das DNS-Server-Produkt sollte sich in der Praxis bereits bewährt haben.
- Falls für ein bestimmtes Produkt bereits genügend geschultes Personal vorhanden ist und alle Anforderungen an die Funktionalität erfüllt sind, sollte dieses DNS-Server-Produkt verwendet werden.
- Es gibt DNS-Server-Produkte deren Implementierung von den Standards zu DNS (RFC 1034, 1035 etc.) abweicht. Ist geplant, verschiedene DNS-Server-Produkte zu benutzen, um z. B. Softwaremonokulturen zu vermeiden, sollte dies nur nach einer Kompatibilitätsprüfung gemacht werden.
- Für den Fall, dass DNSSEC eingesetzt wird, muss darauf geachtet werden, dass dies vom DNS-Server-Produkt unterstützt wird.
- Sofern die Master Files händisch editiert werden, sollte toolgestützt überprüfbar sein, ob die Zonendatei syntaktisch korrekt ist.

APP.3.6.M11 Ausreichende Dimensionierung der DNS-Server

Die Hardware, auf der ein DNS-Server betrieben werden soll, beeinflusst die Gesamtleistung des entstehenden Systems entscheidend. Dabei sollte auch bedacht werden, wie viele Anfragen ein DNS-Server durchschnittlich bedienen muss, ob es sich um einen Resolving DNS-Server handelt, der rekursive Anfragen akzeptiert oder ob es sich um einen Advertising DNS-Server handelt, der nur iterative Anfragen akzeptiert und ob DNSSEC eingesetzt werden soll.

Für DNS-Server ist ein ausreichender Hauptspeicher wichtig, dadurch wird verhindert, dass der Server Speicherinhalte auf die Festplatte auslagern muss und somit die Antwortzeiten steigen. Wird DNSSEC eingesetzt, ist es wichtig darauf zu achten, dass die Prozessorleistung entsprechend erhöht wird, um einen angemessenen Durchsatz bei kryptografischen Operationen aufrecht zu erhalten. Die ausgewählten Kapazitäten für Hauptspeicher und Prozessorleistung müssen im regulären Betrieb überprüft werden, da die tatsächlich benötigten Kapazitäten erst hier genau ermittelt werden können.

Um zu vermeiden, dass fremde Prozesse den DNS-Server beeinflussen, sollte auf der verwendeten Hardware ausschließlich der DNS-Server betrieben werden. Um Distributed-Denial-of-Service-Angriffe abwehren zu können, sollten DNS-Server über eine breitbandige und robuste Netzanbindung verfügen.

APP.3.6.M12 Schulung der Verantwortlichen [Leiter IT, Vorgesetzte]

Um einen DNS-Server korrekt und sicher administrieren zu können, müssen die verantwortlichen Mitarbeiter entsprechend geschult werden. Bereits kleine Konfigurationsfehler können dazu führen, dass sicherheitskritische Schwachstellen entstehen. Besonders solides Fachwissen ist erforderlich, wenn der Einsatz von DNS-Servern geplant wird und die Kommunikation auf legitime Teilnehmer eingeschränkt werden soll.

Neben den Aspekten der allgemeinen Betriebssystemsicherheit sind folgende Punkte von Bedeutung:

- Installation eines DNS-Servers
- Möglichkeiten DNS-Server in den Startprozess des Betriebssystems einzubinden
- Einführung in mögliche Gefährdungen
- Entwicklung eines Rechtekonzepts, sowohl für die Konfigurationsrechte durch Administratoren als auch für die Rechte des DNS-Server-Prozesses
- Unterschied zwischen Advertising und Resolving DNS-Server
- Konfiguration des DNS-Servers
- Mechanismen zur Absicherung von Anfragen
- Mechanismen zur Absicherung von Zonentransfers
- Mechanismen zur Absicherung von dynamischen Updates
- Einsatzmöglichkeiten und Konfiguration von DNSSEC
- Mechanismen zur Sicherstellung der Verfügbarkeit von DNS-Servern
- Mechanismen zur Sicherung der Zoneninformationen

Für Schulungen und Weiterbildungen sollte die Institution ein ausreichendes Budget einplanen.

APP.3.6.M13 Einschränkung der Sichtbarkeit von Domain-Informationen

Die Hauptfunktion von DNS ist es, Namen und IP-Adressen aufzulösen. Um diese Anforderungen erfüllen zu können, speichern DNS-Server unter anderem die Zuordnung von Namen und IP-Adressen sämtlicher Rechner und Netzkomponenten. Ein Teil dieser Informationen muss veröffentlicht werden, z. B. DNS-Server, Webserver, Mailserver, Fileserver, VPN-Verbindungspunkte. Wären diese Domain-Informationen nicht öffentlich zugänglich, könnte keine Verbindung mit Domainnamen über das Internet zu diesen Servern aufgebaut werden.

Domain-Informationen über interne Rechner und Netzkomponenten hingegen sind meistens nicht für die Öffentlichkeit bestimmt und sollten daher institutionsintern bleiben. Da Domain-Informationen oft etwas über die Funktion bzw. den Standort der betreffenden IT-Komponente aussagen, wird von DNS Information Leakage gesprochen, wenn diese Informationen veröffentlicht werden. Die Veröffentlichung selbst stellt für den Informationsverbund keinen direkten Schaden dar. Die gewonnenen Domain-Informationen können jedoch zur Vorbereitung eines Angriffs auf den Informationsverbund genutzt werden. Ein Angreifer kann sich einen Überblick über das Netz, die sicherheitsrelevanten Komponenten und die lohnenden Ziele verschaffen.

Der Namensraum eines Informationsverbundes sollte in einen öffentlichen und einen institutionsinternen Bereich aufgeteilt werden. Im öffentlichen Teil sollten nur solche Domain-Informationen (in der Regel IP-Adresse und Hostname) enthalten sein, damit Dienste, die von extern erreichbar sein sollen, reibungslos funktionieren.

Innerhalb der Institution muss die Sichtbarkeit der Informationen meist nicht eingeschränkt werden. Welche Domain-Informationen nach außen hin sichtbar sind und welche nicht, sollte bei der Planung des DNS-Einsatzes berücksichtigt werden.

APP.3.6.M14 Platzierung der Nameserver

Zur Sicherstellung einer ausreichenden Verfügbarkeit bei Leitungsstörungen sollten externe DNS-Server redundant angebunden sein und in unterschiedlichen Netzsegmenten angeschlossen werden. Darüber hinaus sollten sie nicht an dasselbe Netzkoppelelement angeschlossen werden. Somit wird durch Ausfall eines IP-Subnetzes oder eines Netzkoppelelements die Verfügbarkeit der Namensauflösung nicht beeinträchtigt.

Wohin ein DNS-Server platziert wird, hängt letztlich von der Netzinfrastruktur der jeweiligen Institution ab. Es gibt jedoch einige Grundregeln, die eingehalten werden sollten:

- Primary und Secondary DNS-Server sollten in verschiedenen IP-Subnetzen platziert werden. Des Weiteren sollten sie nicht an dasselbe Netzkoppelelement angeschlossen werden. Dadurch ist die Namensauflösung sichergestellt, auch wenn ein IP-Subnetz oder ein Netzkoppelelement ausfällt.
- Advertising DNS-Server sollten in der demilitarisierten Zone (DMZ) platziert werden. Weitere Hinweise hierzu finden sich im Baustein NET.1.1 Netzarchitektur und -design.
- Resolving DNS-Server sind für Anfragen von institutionsinternen IT-Systemen zuständig. Sie sollten daher innerhalb des vertrauenswürdigen Netzes der Institution so nah wie möglich bei den anfragenden IT-Systemen platziert werden, um lange Antwortzeiten und unnötige Netzbelastung zu vermeiden. Darüber hinaus dürfen Resolving DNS-Server nicht von externen IT-Systemen erreichbar sein.
- Wird die Sichtbarkeit der Informationen eingeschränkt, sollte der öffentliche Teil der Domain-Informationen vom Advertising DNS-Server in der DMZ verwaltet werden.
- Wird für die internen Nameserver ein Forwarder für die Auflösung des Internet-Domainnamensraums verwendet, so sollte dieser nicht im internen Netz platziert werden.
- Werden Caching-Only DNS-Server im firmeninternen Netz eingesetzt, sollten die Resolver auf den Clients keine Domain-Informationen zwischenspeichern. Das Zwischenspeichern übernimmt der Caching-Only DNS-Server. Durch den zentralen Speicher wird die Anzahl der Anfragen minimiert. Des Weiteren kann bei einem erfolgreichen Cache-Poisoning-Angriff der zentrale Cache des Caching-Only DNS-Servers einfach gelöscht werden, um die gefälschten Daten zu entfernen.
- Um DNS-Netzverkehr zu akzeptieren, müssen auf der Firewall entsprechende Regeln eingerichtet werden (siehe APP.3.6.M16 Integration eines DNS-Servers in eine "P-A-P"-Struktur). Bei der Planung sollte darauf geachtet werden, dass möglichst wenige Routen und Ports geöffnet werden müssen.

APP.3.6.M15 Auswertung der Logdaten

Die Logdateien des DNS-Servers sowie des unterliegenden Betriebssystems sollten regelmäßig überprüft und ausgewertet werden. Unregelmäßigkeiten in den Logdateien, die Hinweise auf mögliche Probleme sein können, sind beispielsweise:

- häufige Anfragen von bestimmten Quellen,
- häufige (fehlgeschlagenen) Zonentransfers,
- häufige Anfragen bezüglich bestimmter Domainnamen,
- häufige Anfragen bezüglich Domainnamen, die nicht existieren,
- häufige unerlaubte rekursive Anfragen.

Unregelmäßigkeiten müssen aber nicht unbedingt Hinweise darauf sein, dass der Server kompromittiert ist. Oft treten sie auch aufgrund fehlerhafter Einstellungen auf.

APP.3.6.M16 Integration eines DNS-Servers in eine "P-A-P"-Struktur

Gerade DNS-Server-Produkte sind immer wieder eine Quelle für Sicherheitsprobleme. Wegen der besonderen Bedeutung der Domain-Informationen und der erhöhten Anfälligkeit der DNS-Software für Angriffe ist ein besonderer Aufbau notwendig, um Domain-Informationen sicher bereitstellen und nutzen zu können.

Kommunikation durch Paketfilter auf Minimum beschränken

DNS-Server benötigen die nachfolgend aufgeführten Kommunikationskanäle:

- Resolving DNS-Server darf auf Port 53 des Advertising DNS-Servers UDP
- Advertising DNS-Server darf auf alle Ports des Resolving DNS-Servers UDP (nur bei stateless Firewall nötig)
- Resolving DNS-Server darf auf Port 53 seines Forwarders UDP
- Forwarder darf auf alle Ports des Resolving DNS-Servers UDP (nur bei stateless Firewall nötig)
- Externes Netz darf auf Port 53 des Advertising DNS-Servers UDP
- Advertising DNS-Server darf auf alle Ports externer DNS-Server UDP und TCP (nur bei stateless Firewall nötig)
- Internes Netz darf auf Port 53 des Resolving DNS-Servers UDP
- Resolving DNS-Server darf auf alle Ports des internen Netzes UDP (nur bei stateless Firewall nötig)
- Primary DNS-Server darf auf Port 53 seiner Secondary DNS-Server UDP und TCP
- Secondary DNS-Server darf auf Port 53 seines Primary DNS-Server UDP und TCP

Werden nur diese Regeln implementiert, kann nur beschränkt aus dem Internet auf den freigegebenen Diensten kommuniziert werden. Können die Kommunikationspartner noch weiter eingeschränkt werden, so kann ein Angreifer gar keine direkte Verbindung zum Internet-Server aufbauen.

Hinweis: Obige Regeln können bewirken, dass der DNS-Server nicht von jedem Rechner aus erreicht werden kann, da ICMP nicht durchgelassen wird. Deshalb empfiehlt es sich, den ICMP Subtype *icmp unreachable* vom Internet hin zum Internet-Server durchzulassen.

DNS-Server in einer "P-A-P"-Struktur

Um DNS sicher in eine "P-A-P"-Struktur zu integrieren, bietet sich der in Abbildung 1 gezeigte Aufbau an, bei dem keine direkte Verbindung zwischen einem Client im vertrauenswürdigen Netz und einem DNS-Server im nicht-vertrauenswürdigen Netz (und umgekehrt) stattfindet. Es werden zwei getrennte DNS-Server eingesetzt.

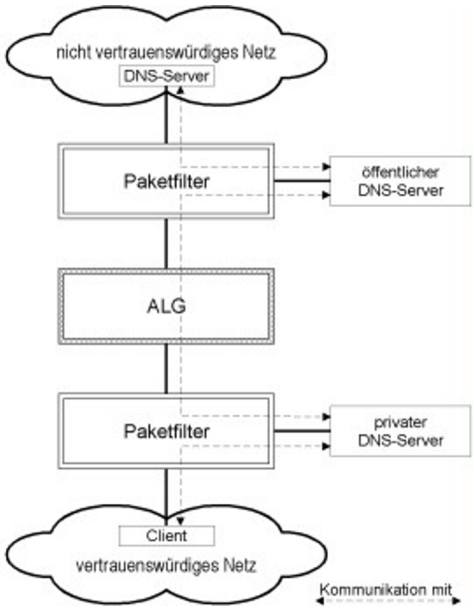


Abbildung: DNS-Server in einer "P-A-P"-Struktur

Der Advertising DNS-Server, der die extern verfügbaren Informationen enthält, wird in einer DMZ des äußeren Paketfilters angesiedelt. Er ist als Primary DNS-Server für die Domain des vertrauenswürdigen Netzes eingerichtet und enthält nur die unbedingt notwendigen Informationen, beispielsweise:

- Name und IP-Adresse des externen Mailservers (MX-Eintrag)
- Namen und Adressen von Informationsservern, die Informationen für die Öffentlichkeit anbieten. Dabei muss zwischen den Servern, die vor dem Application Level Gateway (ALG) angesiedelt sind und denen, die hinter dem ALG angesiedelt sind, unterschieden werden. Bei Ersteren muss die Adresse des Servers selbst eingetragen sein, bei Letzteren die Adresse des ALG.

Der Resolving DNS-Server wird in einer DMZ des inneren Paketfilters aufgestellt. Er enthält die Informationen über die Rechner des internen Netzes. Für Rechner des internen Netzes wird der Resolving DNS-Server als DNS-Server eingetragen: Alle Clients des vertrauenswürdigen Netzes nutzen ausschließlich den Resolving DNS-Server, bei Unix-Rechnern beispielsweise mittels Einträgen in der Datei */etc/resolv.conf*. Benötigt ein Client im vertrauenswürdigen Netz eine Domain-Information aus dem nicht-vertrauenswürdigen Netz, so stellt er die Anfrage an den Resolving DNS-Server. Als "Forwarder" nutzt dieser einen öffentlichen DNS-Server (oder einen extra eingerichteten Forwarder) für Anfragen, die externe Namen betreffen. Der direkte Zugriff auf den Resolving DNS-Server aus dem nicht-vertrauenswürdigen Netz sollte durch Paketfilterregeln unterbunden werden, sodass die Domain-Informationen des vertrauenswürdigen Netzes nur im vertrauenswürdigen Netz sichtbar sind.

Der eingesetzte Paketfilter muss so konfiguriert werden, dass zwischen den DNS-Servern nur der DNS-Dienst gestattet ist, d. h. Port 53 als (je nach betrachteter Richtung) Quell- bzw. Zielport. Vom Advertising DNS-Server sollten keinerlei Verbindungen ins interne Netz zugelassen werden. Der Server sollte nur über entsprechend abgesicherte Verbindungen (z. B. SSH-2) administriert werden.

In Tabelle 1 wird eine mögliche Konfiguration für Zugriffsregelungen beschrieben, die über entsprechende Paketfilterregeln umgesetzt werden kann. Dabei wird davon ausgegangen, dass die Server über eine SSH-Verbindung aus dem internen Netz administriert werden und dass für DNS als Trägerprotokoll UDP verwendet wird. Protokolldaten werden über Syslog auf einen Logserver übertragen.

Quelle	**Ziel**	**Entscheidung**	**Bemerkungen**
Kommunikation des öffentlichen DNS-Servers mit dem Internet			
Externes Netz	Advertising DNS-Server Port 53	erlauben	DNS-Anfragen und Antworten aus dem öffentlichen Netz
Externes Netz	andere Ports des Advertising DNS-Servers	verbieten	
Advertising DNS-Server	DNS-Server im Internet, alle Ports und UDP	erlauben	Auflösung von externen Namen durch den DNS-Server
Kommunikation des externen DNS-Servers mit dem internen Netz			
Advertising DNS-Server	Alle Verbindungen ins interne Netz	verbieten	
Internes Netz (ggfs. Einschränkung auf Administrationsnetz)	Advertising DNS-Server Port 22 (SSH)	erlauben	Administration und Datenübertragung erfolgen per SSH und SCP
Internes Netz	Alle anderen Zugriffe auf den Advertising DNS-Server	verbieten	DNS-Anfragen aus dem internen Netz erfolgen über den internen Server
Kommunikation der beiden DNS-Server untereinander			
Resolving DNS-Server	Advertising DNS-Server UDP Port 53	erlauben	Der Resolving DNS-Server leitet Anfragen an den Advertising Server

Quelle	Ziel	Entscheidung	Bemerkungen
			weiter (falls erforderlich kann ein eigener Forwarder eingerichtet werden)
Advertising DNS-Server	Resolving DNS-Server-alle Ports UDP	erlauben	
Kommunikation des internen DNS-Servers mit dem internen Netz			
Internes Netz	Resolving DNS-Server UDP Port 53	erlauben	DNS-Anfragen aus dem internen Netz erfolgen über den Resolving DNS-Server
Resolving DNS-Server-UDP Port 53	Internes Netz	erlauben	DNS-Antworten in das interne Netz
Resolving DNS-Server-sonstige Quellports	Internes Netz	verbieten	
Internes Netz (falls erforderlich Einschränkung auf Administrationsnetz)	Resolving DNS-Server Port 22 (SSH)	erlauben	Administration und Datenübertragung erfolgen per SSH und SCP
Protokollierung			
Resolving und Advertising DNS-Server	Loghost UDP-Port 514	erlauben	Übertragung der Protokolldaten zum Loghost

Tabelle 1: Konfiguration für Zugriffsregeln

Domain-Registrierung bei externem Dienstleister

Bei dieser Alternative werden wichtige Domain-Informationen bei einem externen Dienstleister gespeichert und nicht durch einen eigenen DNS-Server bereitgestellt. Der Unterschied zu den eben beschriebenen Szenarien besteht im Wesentlichen im Wegfall der Advertising DNS-Server. DNS-Anfragen aus dem externen Netz nach Domain-Informationen aus dem internen Netz werden nicht an den institutionsinternen Advertising DNS-Server, sondern an den DNS-Server des externen Dienstleisters gesendet und von diesem beantwortet. Der Resolving DNS-Server greift bei Anfragen nach externen DNS-Namen oder IP-Adressen direkt über die Firewall hinweg auf einen DNS-Server im externen Netz, meistens betrieben durch den Internet-Provider, zu.

Auch bei dieser Integrationsvariante sollten nur die unbedingt notwendigen Domain-Informationen extern angeboten werden, beispielsweise Name und IP-Adresse des Mailservers und des ALG. Bei besonders unbedenklichen institutionsinternen Nutzern kann der Resolving DNS-Server auch im internen Netz, anstatt in einer DMZ des inneren Paketfilters betrieben werden, was die Administration des Paketfilters etwas erleichtert.

Vorteile dieser Variante sind die geringen Investitionskosten und die geringe Komplexität bei der Integration in eine P-A-P-Struktur.

APP.3.6.M17 Einsatz von DNSSEC

DNSSEC wurde entwickelt, um DNS gegen Angriffe zu schützen, darunter auch Cache-Poisoning-Angriffe. Realisiert wird dies durch asymmetrische Kryptografie. Bei DNSSEC werden die gesamten Zoneninformationen mit einem privaten Schlüssel signiert. Diese Signaturen können mithilfe des zugehörigen öffentlichen Schlüssels geprüft werden. Das Schlüsselpaar wird als Zone-Signing-Key (ZSK) bezeichnet. Stellt ein DNSSEC unterstützender Resolver eine Anfrage an einen DNS-Server, auf dem DNSSEC konfiguriert ist, sendet der Server als Antwort die Domain-Informationen mit den Signaturen zurück. Der Resolver kann mithilfe der Signatur und dem öffentlichen Schlüssel überprüfen, ob die Domain-Informationen korrekt sind.

Um die Authentizität des ZSK sicherzustellen, wird dieser mithilfe von Key-Signing-Keys (KSK) signiert. Ein Hashwert des öffentlichen Teils des KSK wird der übergeordneten Domain übermittelt. Die übergeordnete Domain signiert mithilfe ihrer Schlüssel den Hashwert und bestätigt die Authentizität des Hashwertes. Somit entsteht eine Vertrauenskette (Chain-of-Trust). Setzt die übergeordnete Domain DNSSEC nicht ein, besitzt diese keine Schlüssel und kann keine Signatur erstellen, um die Authentizität der KSK zu bestätigen. Man kann jedoch seine DNS-Server anweisen, den eigenen Schlüsseln zu vertrauen, somit entstehen Vertrauensinseln (Island-of-Trust). Mit höherem Verbreitungsgrad von DNSSEC werden diese Vertrauensinseln größer und somit das Sicherheitsniveau höher. DNSSEC bietet folgende Sicherheitsmechanismen:

- Die Quelle der DNS-Informationen wird authentisiert.
- Die Integrität der Domain-Informationen wird sichergestellt, somit können Domain-Informationen nicht mehr manipuliert werden, da die Signatur diese Manipulation sichtbar macht. Kunden können beispielsweise sicher sein, mit dem richtigen Webserver oder Mailserver zu kommunizieren.
- Existiert ein Domainname nicht, wird eine authentisierte Fehlermeldung gesendet.

Die Schlüssel ZSK und KSK müssen sorgfältig verwaltet und regelmäßig getauscht werden. Da mit den ZSK mehr Datenmaterial signiert wird, sind diese öfter zu tauschen. Je nach Größe der signierten Zonen stellt ein Wechsel im Zeitrahmen von ein bis drei Monaten ein geeignetes Sicherheitsniveau dar. Bei den KSK sollte spätestens nach einem Jahr ein Wechsel erfolgen. Gelangen die KSK und ZSK an die Öffentlichkeit, müssen die Schlüssel umgehend getauscht werden.

Durch DNSSEC und die dadurch nötigen kryptografischen Operationen ist es gegebenenfalls notwendig, die Leistungskapazität von DNS-Servern anzupassen, auch die Rechenleistung muss eventuell erhöht werden. Es muss sichergestellt werden, dass auch bei Lastspitzen die Antwortzeit akzeptabel gehalten wird.

APP.3.6.M18 Erweiterte Absicherung von Zonentransfers

Um ein höheres Schutzniveau zu erreichen, können die Zonentransfers über Transaction Signatures (TSIG) abgesichert werden. Bei TSIG werden auf dem Primary DNS-Server und dem/den Secondary DNS-Server(n) symmetrische Schlüssel definiert. Wird ein Zonentransfer gestartet, erzeugt TSIG aus den Binärdaten der Anfrage mithilfe des symmetrischen Schlüssels und einer Hashfunktion einen Hash Message Authentication Code (HMAC). Der HMAC wird der Anfrage beigefügt. Der Secondary DNS-Server, der den Schlüssel ebenfalls kennt, berechnet den HMAC eigenständig. Stimmen erhaltener und berechneter HMAC überein, wird der Zonentransfer durchgeführt, ansonsten wird dieser abgelehnt. Diese Methode schützt im Gegensatz zur IP-Adressen-basierten Absicherung auch gegen IP-Spoofing. Bei TSIG ist jedoch zu beachten, dass nicht jedes DNS-Server-Produkt über diese Funktion verfügt. Auch können herstellerspezifische Abweichungen bei der jeweiligen Implementierung bestehen.

APP.3.6.M19 Aussonderung von DNS-Servern

Wird entschieden, einen DNS-Server nicht weiter zu betreiben, weil beispielsweise die Domain aufgelöst wird, sind bei dessen Außerdienststellung einige Punkte zu beachten. Der Aussonderungsplan soll unter anderem verhindern, dass Verweise auf nicht mehr existierenden DNS-Server im Domain-Namensraum verbleiben.

Löschen/Entsorgen der Speichermedien

Die Speichermedien aller betroffenen Rechner sollten vor der Wiederverwendung sicher gelöscht werden. Wird die Hardware entsorgt, so sollte dies ebenfalls auf sichere Weise geschehen.

Löschen des DNS-Servers aus dem Domain-Namensraum

Wurde der DNS-Server nicht bei der übergeordneten Domain registriert, müssen keine weiteren Schritte unternommen werden. Ist der DNS-Server jedoch bei der übergeordneten Domain registriert, muss die Aussonderung den Administratoren der übergeordneten Domain bekannt gegeben werden, damit diese in der übergeordneten Domain alle Zoneneinträge der ausgesonderten DNS-Server löschen.

System aus dem Netzverbund löschen

Alle Referenzen auf Netz- und Betriebssystemebene sind zu löschen. Ist der ausgesonderte Server als Standard DNS-Server bei internen Systemen der Institution eingetragen, müssen diese Einträge gelöscht werden. Zonentransfers, die zwischen dem ausgesonderten DNS-Server und noch existierenden DNS-Servern konfiguriert sind, müssen ebenfalls gelöscht werden.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

APP.3.6.M20 Prüfung des Notfallplans auf Durchführbarkeit (A)

Der Notfallplan für DNS-Server muss regelmäßig praktisch getestet werden. Nur so kann sichergestellt werden, dass die in den Wiederanlaufplänen beschriebenen Maßnahmen tatsächlich durchführbar sind. Gleichzeitig lernen die Mitarbeiter in den Übungen die beschriebenen Abläufe kennen und trainieren ihre Umsetzung. Schließlich vermittelt die Übung Erkenntnisse zu den tatsächlichen Wiederherstellungs- und Wiederanlaufzeiten.

APP.3.6.M21 Hidden-Master (CIA)

Eine sogenannte Hidden-Master-Konfiguration stellt sicher, dass der primäre Advertising DNS-Server von außen nicht erreichbar ist und auch in den DNS-Zonen-Daten nicht sichtbar wird. Anfragen werden ausschließlich von mindestens zwei sekundären Advertising DNS-Servern beantwortet, die ihre Daten über eine gesicherte Leitung vom versteckten primären Advertising DNS-Server beziehen.

APP.3.6.M22 Anbindung der DNS-Server über unterschiedliche Provider [Leiter IT] (IA)

Bei der Registrierung eines Domainnamens müssen mindestens zwei DNS-Nameserver (*Primary und Secondary Nameserver*) angegeben werden, die für die Zuordnung von Rechnernamen zu IP-Adressen zuständig sind. Ein Nameserver wird oft vom Internet-Zugangsprovider betrieben, kann aber auch von der Institution selbst betrieben werden. Zur Vorbeugung vor DoS-Angriffen sollten Primary und Secondary Nameserver in verschiedenen Netzen angesiedelt und über unterschiedliche Provider angebunden sein.

3 Weiterführende Informationen

3.1 Wissenswertes

Der Domain Name System (DNS) ist ein Netzdienst, um Hostnamen von IT-Systemen in Computernetzen aufzulösen. Vorwärtsauflösung ist, wenn die IP-Adresse zu einem Hostnamen ermittelt wird. Wird dagegen der Hostname zu einer IP-Adresse ermittelt, wird dies als Rückwärtsauflösung bezeichnet.

Domain-Namensraum

DNS ist eine verteilte Datenbank, die den baumförmigen Domain-Namensraum verwaltet (siehe Abbildung 2). Der Baum besteht aus Knoten und Blättern, die als Label bezeichnet werden. Die Verkettung der durch Punkte getrennten Labels ergibt einen Domainnamen. Der Domain-Namensraum ist in verschiedene Domains unterteilt. Die oberste Ebene, die Wurzel, wird als Punkt dargestellt und als *root* bezeichnet. Darunter folgen die Top-Level-Domains wie beispielsweise *.com*, *.edu*, *.de*, *.at*, danach die Second-Level-Domains wie *.bund* usw.

Im Domain-Namensraum werden Informationen über die Zuordnung von IP-Adressen zu Domainnamen gespeichert. DNS kann als eine Art Telefonbuch in Computernetzen bezeichnet werden, dessen Hauptaufgabe es ist, Namen aufzulösen. Es genügt beispielsweise den Domainnamen *www.bsi.bund.de* im Browser einzugeben, DNS findet im Domain-Namensraum die zugehörige IP-Adresse und der Browser kann sich mit dem Ergebnis der Suche zum entsprechenden Webserver verbinden.

Grundsätzlich muss zwischen Domains und Zonen unterschieden werden. Eine Zone, wie in Abbildung 3 dargestellt, ist eine Verwaltungseinheit, die ein DNS-Server über ein Master File einliest. Ein Master File enthält alle Domain-Informationen einer Zone, und wird von den zuständigen Administratoren verwaltet. Beispiele für Zonen sind *arpa*, *com*, *example, a, b* und *c,* wobei *com*, *example, a, b* und *c* jeweils eine eigene Zone darstellen. Unter einer Domain hingegen wird beispielsweise eine Domain wie *com* und alle darunter liegenden Subdomains, in diesem Fall *example*, *a*, *b*, *c verstanden*.

Für jede Zone sind mindestens zwei DNS-Server autoritativ, dies bedeutet, dass diese DNS-Server die Domain-Informationen dieser Zone verwalten. Zusätzlich kennt jeder DNS-Server die autoritativen DNS-Server für seine Subdomains. Das bedeutet, dass beispielsweise der DNS-Server für *com* den DNS-Server für *example* kennt, und somit bei einer Namensauflösung an diesen verweisen kann.

Resolver

Clientanwendungen benötigen einen Resolver, um an DNS teilzunehmen. Dieser ist oft Teil des Betriebssystems. Wenn eine Clientanwendung eine Namensauflösung benötigt, stellt sie eine Anfrage an den Resolver. Dieser packt die Anfrage in ein DNS-konformes Paket, sendet dieses an einen DNS-Server, interpretiert die Antwort und übermittelt die Daten an die entsprechende Anwendung zurück. Um die Leistungsfähigkeit von DNS zu steigern, speichert der Resolver die Antwortdaten für eine bestimmte Zeit im Cache. Solange sich die Daten im Cache befinden, wird bei einer wiederholten Auflösung der DNS-Server nicht erneut befragt.

DNS-Server

DNS-Server sind Anwendungen, die Informationen über einen bestimmten Bereich des Domain-Namensraums verwalten. Die Informationen sind in sogenannten Zonendateien gespeichert. Verwaltet ein DNS-Server mehrere Domains, beispielsweise *bund.de* und die zugehörige Subdomain *bsi.bund.de*, werden diese in jeweils eigenen Zonen gespeichert. Die Informationen über eine Zone liest ein DNS-Server aus den Master Files ein.

DNS-Server werden nach ihren Aufgaben unterschieden, es gibt grundsätzlich zwei verschiedenen Typen:

- Advertising DNS-Server
- Resolving DNS-Server

Advertising DNS-Server sind üblicherweise dafür zuständig, Anfragen bezüglich eigener Domains aus dem Internet zu verarbeiten. Haben sie die gewünschten Domain-Informationen gespeichert, liefern sie die entsprechende Antwort. Andernfalls verweisen sie an einen anderen DNS-Server. Die Hauptaufgabe eines Advertising DNS-Servers ist es, seine gespeicherten Domain-Informationen zur Verfügung zu stellen.

Resolving DNS-Server hingegen verarbeiten üblicherweise Anfragen aus dem institutionsinternen Netz. Haben sie die gewünschten Domain-Informationen gespeichert, liefern sie, ebenso wie Advertising DNS-Server, die entsprechende Antwort. Andernfalls verweisen Resolving DNS-Server jedoch nicht an einen anderen DNS-Server, sondern übernehmen die Namensauflösung selbst.

DNS-Server, die Anfragen mithilfe der eigenen Zoneninformationen beantworten können, werden als autoritativ bezeichnet. Erhält ein DNS-Server eine Anfrage, die nicht seine eigene(n) Zone(n) betreffen und zu denen er auch keine Informationen im Cache hat, kann ein DNS-Server auf drei Arten reagieren:

- Delegierung Delegierung bedeutet, dass ein Teil der Informationen über den Domain-Namensraum in eine Subdomain ausgelagert wurde. Wenn der DNS-Server beispielsweise eine Anfrage für bund.de erhält, wird der DNS-Server die Anfrage an den zuständigen DNS-Server weiterleiten. Da ein DNS-Server alle für die delegierten Zonen zuständigen DNS-Server kennen muss, kann er die Anfrage direkt an die zuständigen DNS-Server weiterleiten.
- Auflösung über Root-NameserverEs gibt insgesamt 13 Root-DNS-Server. Diese Root-DNS-Server haben gespeichert, welche DNS-Server für die Top-Level-Domains autoritativ sind. Befinden sich die gewünschten Daten außerhalb der verwalteten Domain und sind auch keine Daten im Cache vorhanden, muss eine rekursive Auflösung, beginnend bei den Root-Nameservern, gestartet werden. Diese Verhaltensweise entspricht einem Resolving DNS-Server.
- Weiterleitung (Forwarding)Kann ein DNS-Server die gewünschten Informationen nicht liefern, leitet er die Anfrage an einen vorher konfigurierten DNS-Server weiter.

Kommunikation

Wie bereits beschrieben, kommunizieren Anwendungen über die Resolver-Schnittstelle mit DNS-Servern, unabhängig davon, ob es sich dabei um einen Advertising oder Resolving DNS-Server handelt. Resolver senden stellvertretend für Anwendungen, die Namensauflösungen benötigen, Anfragen an DNS-Server und interpretieren die erhaltenen Antworten, um diese an die Anwendung zurück zu liefern. Grundsätzlich wird zwischen zwei Arten von Anfragen unterschieden:

- iterative Anfragen:Iterativ bedeutet, dass der befragte DNS-Server, sofern er die benötigten Daten nicht gespeichert hat, an den nächsten zuständigen DNS-Server verweist. Der befragte DNS-Server ist also ein Advertising DNS-Server. Der anfragende Resolver muss selbst die gesamte Namensauflösung durchführen. Eine Namensauflösung zu www.bsi.bund.de über die Root-DNS-Server (Root-DNS-Server beantworten nur iterative Anfragen und sind somit Advertising DNS-Server) würde wie folgt aussehen. Im ersten Schritt fragt der Resolver bei den Root-DNS-Servern nach dem Advertising DNS-Server, der für de. zuständig ist. Im zweiten Schritt wird durch den Resolver vom für de zuständigen Advertising DNS-Server der DNS-Server ermittelt, der für bund.de zuständig ist. Danach wird von diesem der Advertising DNS-Server für bsi.bund.de erfragt. Schließlich kann der Advertising DNS-Server für bsi.bund.de die IP-Adresse zu www.bsi.bund.de an den Resolver liefern.
- Rekursive Anfragen:Bei der rekursiven Anfrage funktioniert die Auflösung sehr ähnlich. Jedoch übernimmt der für den Resolver zuständige DNS-Server die komplette Namensauflösung, wie oben beschrieben. Es handelt sich also um einen Resolving DNS-Server. Der Resolver des Clients muss nur eine Anfrage stellen.

Ein Advertising DNS-Server akzeptiert nur iterative Anfragen, ein Resolving DNS-Server hingegen akzeptiert sowohl iterative als auch rekursive Anfragen. Rekursive Anfragen bedeuten im Vergleich zu iterativen Anfragen eine höhere Belastung für den DNS-Server.

Zonentransfers

Da DNS von sehr vielen Netzanwendungen benötigt wird, müssen laut Spezifikation (RFC 1034) mindestens zwei autoritative DNS-Server für jede Zone betrieben werden. Da es zu aufwändig ist, für jeden DNS-Server eigene Master Files zu verwalten, die konsistent sein müssen, wird eine Synchronisation über Zonentransfer durchgeführt. Der DNS-Server, der die Domain-Informationen direkt aus den Master Files bezieht, wird als Primary oder Master DNS-Server bezeichnet. Jeder weitere DNS-Server wird als Secondary oder Slave DNS-Server bezeichnet und bezieht die Daten über einen Zonentransfer vom Primary DNS-Server. Ein Secondary DNS-Server kontrolliert in regelmäßigen Abständen, ob sich die Domain-Informationen seiner Zone(n) geändert haben oder er wird von seinem Primary DNS-Server über Änderungen informiert. Ist dies der Fall, wird vom Secondary DNS-Server ein Zonentransfer initiiert, um seine Domain-Informationen auf den neusten Stand zu bringen.

Caching-Only DNS-Server

Der Caching-Only DNS-Server ist ein Spezialfall eines Resolving DNS-Servers. In der Regel ist ein DNS-Server, unabhängig davon, ob es sich um einen Advertising oder Resolving DNS-Server handelt, für eine oder mehrere Zonen autoritativ. Das bedeutet, er hat die Domain-Informationen über diese Zonen aus den Master Files ausgelesen beziehungsweise von seinem Master DNS-Server über einen Zonentransfer erhalten. Caching-Only DNS-Server sind hingegen für keine Zone autoritativ, sie haben selbst keine Zonen gespeichert. Sie dienen in der Regel dazu, Anfragen entgegenzunehmen und die Namensauflösung durchzuführen. Caching-Only DNS-Server werden oft als Forwarder für institutionsinterne Resolving DNS-Server eingesetzt, wenn diese Domain-Informationen aus dem Internet auflösen müssen.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "DNS-Server" finden sich unter anderem in folgenden Veröffentlichungen:

[BSICS055] Sichere Bereitstellung von DNS-Diensten:

Handlungsempfehlungen für Internet-Service-Provider (ISP) und große Unternehmen, BSI-Veröffentlichungen zur Cyber-Sicherheit (BSI-CS 055), Version 1.0, April 2013,
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_055.pdf, zuletzt abgerufen am 05.10.2018

[BSIDNSSEC] Umsetzung von DNSSEC

Handlungsempfehlungen zur Einrichtung und zum Betrieb der Domain Name Security Extensions, BSI-Veröffentlichungen zur Cyber-Sicherheit (BSI-CS 121), Juni 2015,
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Umsetzung_von_DNSSEC.html, zuletzt abgerufen am 05.10.2018

[ISILANA] Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA)

Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.1, August 2014
https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-LANA/lana_node.html, zuletzt abgerufen am 05.10.2018

[NIST800-81-2] Secure Domain Name System (DNS) - Deployment Guide

NIST Special Publication 800-81-2, September 2013
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf, zuletzt abgerufen am 05.10.2018

Umsetzungshinweise zum Baustein APP.4.2 SAP-ERP-System

1 Beschreibung

1.1 Einleitung

Enterprise Resource Planning Systeme von SAP (kurz SAP-ERP-Systeme) werden eingesetzt, um interne und externe Geschäftsabläufe zu automatisieren und technisch zu unterstützen. Die SAP-ERP-Systeme verarbeiten daher typischerweise vertrauliche Informationen, sodass alle Komponenten und Daten geeignet geschützt werden müssen.

Ein SAP-ERP-System (aktuell unter den Produktbezeichnungen SAP Business Suite und SAP S/4HANA auf dem Markt) setzt sich aus verschiedenen Modulen zusammen, mit denen die Organisationsstruktur einer Institution abgebildet werden kann. Zu den Modulen eines SAP-ERP-Systems zählen unter anderem Rechnungswesen, Personalwirtschaft und Logistik. Die Kernkomponenten des SAP-ERP-Systems sind SAP NetWeaver (Applikationsserver-Middleware) und SAP HANA (Applikationsserver und Datenbank). SAP NetWeaver ermöglicht es, SAP-ABAP- und SAP-JAVA-Anwendungen anzubinden und Prozesse systemweit zu steuern. SAP HANA kann in Echtzeit große Datenmengen für alle Geschäftsbereiche analysieren.

Die Grundlage und die Struktur für diese Umsetzungshinweise sind die Richtlinien aus verschiedenen SAP-Dokumenten, z. B. SAP Security Baseline Template (siehe [SAPSBAS]), SAP Security Guides (siehe [SAPSG]) und SAP Security Whitepapers (siehe [SAPSWP]). Das SAP Security Baseline Template setzt sich aus verschiedenen SAP Empfehlungen und Quellen zusammen, z. B. SAP EarlyWatch Alert, SAP Security Optimization Service, Security Notes. Die fünf Themenschwerpunkte des Baseline Templates sind:

- Infrastruktursicherheit (Infrastructure Security: SAP verwendet den Begriff Infrastruktursicherheit, anders als im IT-Grundschutz, nicht so umfassend und geht weniger auf baulichen Maßnahmen und Gebäude ein),
- Sicherheitscode (Secure Code),
- sichere Installation (Secure Setup),
- sicherer Betrieb (Secure Operation),
- Sicherheitsrichtlinien (Security Compliance).

Im SAP-Hinweis 2253549 - The SAP Security Baseline Template (S-User notwendig) (siehe [SECNOTE]) finden sich aktuelle Hinweise zum SAP Security Baseline Template.

Alle Maßnahmen und Empfehlungen aus dem vorliegenden Baustein sollten gemeinsam mit den genannten SAP-Dokumentationen betrachtet werden. Die angegebenen SAP-Hinweise (SAP-Notes, OSS-Hinweise) sind im SAP Support Portal (siehe [SECNOTE]) zu finden.

1.2 Lebenszyklus

Planung und Konzeption

Es muss ein umfassendes Berechtigungskonzept für SAP-ERP-Systeme erstellt werden (siehe APP.4.2.M6 *Erstellung und Umsetzung eines Benutzer- und Berechtigungskonzepts*). Außerdem müssen Passwortrichtlinien definiert (siehe APP.4.2.M13 *Passwortsicherheit*) und die unter dem SAP-ERP-System liegenden Datennetze geschützt werden (siehe APP.4.2.M3 *Netzsicherheit*). Für unterschiedliche Benutzer können auch spezifische Sicherheitsrichtlinien für Passworte und Anmelderestriktionen festgelegt werden (siehe APP.4.2.M19 *Definition der Sicherheitsrichtlinie für Benutzer*).

Umsetzung

Nachdem alle notwendigen Konzepte für den Einsatz eines SAP-ERP-Systems erstellt wurden, ist der nächste Schritt, das SAP-ERP-System zu installieren (siehe APP.4.2.M11 *Sichere Installation des SAP-ERP-Systems*). Diese Phase beinhaltet viele weitere Maßnahmen, die insbesondere für eine sichere Konfiguration des SAP-ERP-Systems wichtig sind, z. B. APP.4.2.M5 *Konfiguration und Absicherung der SAP-Benutzerverwaltung*, APP.4.2.M15 *Sichere Konfiguration des SAPRouters* und APP.4.2.M21 *Konfiguration des Security Audit Logs*. Ebenso ist die Erstkonfiguration sowohl für den ABAP-Stack als auch für den Java-Stack erforderlich, keiner der beiden Stacks darf unkonfiguriert bleiben (siehe APP.4.2.M1 *Sichere Konfiguration des SAP-ABAP-Stacks* und APP.4.2.M2 *Sichere Konfiguration des SAP-JAVA-Stacks*).

Kern eines jeden SAP-ERP-Systems ist die Datenbank. Sie speichert nicht nur die Geschäftsdaten der Institution, sondern auch die internen Funktionen und Verwaltungsinformationen des SAP-ERP-Systems. Sicherheitsprobleme im Bereich der Datenbanken wirken sich daher sofort immer auf das gesamte SAP-ERP-System aus. Maßnahmen, mit denen sich die Datenbanken schützen lassen, sind in APP.4.2.M7 *Absicherung der SAP-Datenbanken* zusammengefasst.

SAP-ERP-Systeme kommunizieren über verschiedene Schnittstellen miteinander oder sie nutzen andere externe Client- oder Server-Systeme. Generell kann ein SAP-ERP-System viele unterschiedliche Kommunikationskanäle nutzen, die auch von den installierten Applikationen und Modulen abhängen. In der Regel werden jedoch einige wenige Basis-Kommunikationsmechanismen und -Schnittstellen genutzt. Relevante Maßnahmen dafür sind z. B.:

- APP.4.2.M8 *Absicherung der SAP RFC-Schnittstelle*
- APP.4.2.M9 *Absicherung und Überwachung des Message-Servers*
- APP.4.2.M24 *Aktivierung und Absicherung des Internet Communication Frameworks (ICF)*

Weiterhin ist es wichtig, die Betriebssysteme abzusichern, auf denen die SAP-ERP-Systeme laufen (siehe APP.4.2.M16 *Umsetzung von Sicherheitsanforderungen für das Betriebssystem Windows* und APP.4.2.M17 *Umsetzung von Sicherheitsanforderungen für das Betriebssystem Unix*).

Betrieb

Während des Betriebs muss das SAP-ERP-System ständig kontrolliert und aktualisiert werden. SAP aktualisiert seine ERP-Produkte regelmäßig. Dabei gibt es auch immer wieder Neuerungen im Sicherheitsumfeld, beispielsweise weitere Schalter oder zusätzliche Berechtigungsprüfungen. Das eingesetzte Personal muss diesbezüglich sowohl seinen Wissensstand dauerhaft aktuell halten als auch Prozesse definieren, die eine Umsetzung im Regelbetrieb zeitnah erlauben (siehe z. B. APP.4.2.M10 *Regelmäßige Implementierung von Sicherheitskorrekturen*).

Vor allem müssen Sicherheitsverstöße schnell erkannt und behoben werden (siehe APP.4.2.M32 *Implementierung eines kontinuierlichen Monitorings auf die Sicherheitseinstellungen*, APP.4.2.M32 *Echtzeiterfassung und Alarmierung von irregulären Vorgängen* und APP.4.2.M14 *Identifizierung kritischer SAP-Berechtigungen*). Oft wird auch kundeneigener Programmcode in das SAP-ERP-System eingebracht. Dieser Prozess muss geeignet abgesichert werden (siehe APP.4.2.M26 *Schutz des kundeneigenen Codes im SAP-System*).

Notfallvorsorge

ERP-Systeme können für die gesamte Steuerung von zentralen Geschäftsprozessen genutzt werden. Bei einem Ausfall sind die Geschäftsprozesse bzw. Fachaufgaben betroffen und können nicht mehr erfüllt werden. Dies kann von einfachen Materialbestellungen über Lohnabrechnungen bis hin zu Produktionsanlagen reichen. Es ist daher essenziell ein Notfallkonzept für diese Systeme zu erstellen (siehe APP.4.2.M28 *Erstellung eines Notfallkonzepts*). Außerdem sollten Notfallbenutzer eingerichtet werden, die über weitgehende Rechte verfügen (siehe APP.4.2.M29 *Einrichten eines Notfallbenutzers*).

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "SAP-ERP-System" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

APP.4.2.M1 Sichere Konfiguration des SAP-ABAP-Stacks

Die initiale Konfiguration des ABAP-Stacks ist aufwändig und umfasst viele Einzelschritte. Der Aufwand erhöht sich, wenn neben der Konfiguration der SAP-Basis auch Applikationen und Module konfiguriert werden müssen. Im Folgenden werden die wichtigsten Schritte dargestellt, die bei der initialen Konfiguration des ABAP-Stacks durchzuführen sind. Dabei wird nur auf die sichere Konfiguration der SAP-Basis eingegangen.

Mandanten für den Betrieb festlegen

Zunächst muss ein Mandant für den Betrieb des SAP-ERP-Systems festgelegt werden. Als Mandant (engl. Client) wird in einem SAP-ERP-System eine technische Unterteilung verstanden und darf nicht mit dem Mandantenbegriff im Sinne von "Kunde" verwechselt werden. Nach der Installation dürfen die existierenden Standardmandanten mit den Nummern 000 (SAP Referenzmandant), 001 (Produktionsvorbereitungsmandant) und 066 (Earlywatch-Mandant) nicht genutzt werden. Nachdem die für den Betrieb erforderlichen Mandanten aufgebaut worden sind, sollten vor regulärer Inbetriebnahme des Systems die Mandanten 001 und 066 gelöscht werden (siehe SAP-Hinweis 1749142 [SECNOTE]).

Ein SAP-ERP-System kann mehrere Mandanten mit unterschiedlichen Verwendungszwecken enthalten. Alle Mandanten eines SAP-ERP-Systems hängen jedoch über den SAP-Referenzmandanten zusammen, in den Konfigurationen erfolgen, die global für das gesamte SAP-ERP-System gelten.

Mandanten mit sehr unterschiedlichen Sicherheitsanforderungen sollten nicht zusammen in einem SAP-ERP-System betrieben werden. So darf etwa ein Produktivmandant nie zusammen mit einem Entwicklungsmandanten in einem SAP-ERP-System ausgeführt werden.

Sicherheitsrelevante IMG-Aktivitäten durchführen (Customizing)

Der SAP Implementation Guide (IMG, SAP Reference IMG) ist eine von SAP vordefinierte, systeminterne Liste mit Konfigurationsschritten für ein SAP-ERP-System. Sie ist hierarchisch aufgebaut und jeweils auf die verwendete Systemversion und die installierten Komponenten abgestimmt. Daneben ist es möglich, eigene IMGs zu erstellen (Projekt IMGs), in denen nur die im Rahmen der Systemverwendung notwendigen Konfigurationsschritte aus dem SAP Reference IMG enthalten sind. IMGs bieten zudem die Möglichkeit festzuhalten, welche Konfigurationen bereits durchgeführt wurden. Folgende Aktivitäten sind im IMG durchzuführen:

- Aktivierung bzw. Deaktivierung der HTTP-Services, falls diese für den späteren Einsatz nicht benötigt werden (Transaktion: SICF, siehe APP.4.2.M24 *Aktivierung und Absicherung des Internet Communication Frameworks (ICF)*)
- Vergeben von Berechtigungen für RFC-Schnittstellen (Transaktion PFCG, siehe APP.4.2.M8 *Absicherung der SAP RFC-Schnittstelle*)
- Content-Server-Administration (Transaktion: CSADMIN, siehe APP.4.2.M24 *Aktivierung und Absicherung des Internet Communication Frameworks (ICF)*)
- SAP Web Dispatcher konfigurieren (siehe dazu auch APP.4.2.M25 *Sichere Konfiguration des SAP Web Dispatchers*)

Alle Aktivitäten unter dem Stichwort "Systemadministration" sind durchzuführen.

Profilparameter anpassen

Profilparameter sollen das SAP-ERP-System vor Angriffen von außen schützen. Informationen zur Einstellung der Profilparameter sind in den folgenden Abschnitten beschrieben:

- Profilparameter zur Einstellung der Passwortsicherheit (siehe APP.4.2.M7 *SAP-Passwortsicherheit*)
- Profilparameter zur Absicherung der:
  - Web Dispatcher (siehe APP.4.2.M25 *Sichere Konfiguration des SAP Web Dispatchers*)
  - RFC-Schnittstelle (siehe APP.4.2.M8 *Absicherung der SAP RFC-Schnittstelle*)
  - Message-Server (siehe APP.4.2.M9 *Absicherung und Überwachung des Message-Servers*)
  - Konfiguration des Security Audit Logs (siehe APP.4.2.M21 *Konfiguration des Security Audit Logs*)

Parameter mit dem Präfix auth/, login/, snc/ oder ssf sollten aus Sicherheitsperspektive immer besonders genau betrachtet werden. Sie lassen sich über die Transaktion RZ10 verwalten und über die Transaktion RSPFPAR anzeigen.

Systemänderbarkeit konfigurieren

Für Produktivsysteme wird empfohlen, die Systemänderbarkeit global auf nicht änderbar zu setzen. Damit können Änderungen nur noch über das Transportsystem eingespielt werden und somit nur über definierte Prozeduren und Abläufe erfolgen. Wichtig ist jedoch, einen geordneten Änderungsmanagementprozess zu definieren und einzuhalten.

Für Test- und Qualitätssicherungssysteme sollten die gleichen Einstellungen wie im Produktivsystem verwendet werden, also ebenfalls global nicht änderbar. Änderungen sind im Entwicklungssystem vorzunehmen und nach dem erfolgreichen Qualitätssicherungsprozess in das Produktivsystem zu transportieren.

Für Entwicklungssysteme sollten die Komponenten, die durch die Entwicklung nicht betroffen sind, ebenfalls auf nicht änderbar gesetzt werden. Die Komponenten, in denen entwickelt wird, müssen hingegen auf änderbar gesetzt werden.

Mandanten-Konfiguration durchführen

Es können auch einzelne Mandanten davor geschützt werden, dass sich ihre Eigenschaften verändern lassen. Diese Einstellung ist für alle produktiven Mandanten zu benutzen. Dadurch wird auch beeinflusst, ob Mandanten-Veränderungen automatisch aufgezeichnet werden, sodass Einstellungsveränderungen nach der Prüfung als Transportauftrag verfügbar sind und in andere Mandanten transportiert werden können, die mit den gleichen Einstellungen betrieben werden sollen. Die Einstellungen erfolgen über die Transaktion SCC4. Für die eigenen Produktivmandanten sind folgende Einstellungen empfohlen:

(Hinweis: Die angegebenen Bezeichnungen der Einstellungswerte finden sich so in der abgekürzten Schreibweise im SAP-ERP-System.)

- Rolle des Mandanten: Produktiv
- Änderungen und Transporte für mandantenabhängige Objekte: keine Änderung erlauben
- Änderungen an mandantenübergreifenden Objekten: keine Änderungen von Repository- und mand.unabh. Cust.-Obj.
- Schutz bezüglich Mandantenkopierer und Vergleichstool: Schutzstufe 2: kein Überschreiben, keine ext. Verfügbarkeit

Entsprechende Einstellungen sollten im Test- und Qualitätssicherungssystem gelten. Für andere Mandanten (Entwicklung, Schulung, Demo) sind die Einstellungen geeignet zu definieren.

Ausführbare Betriebssystemkommandos absichern

Die Kommandos werden mit den Betriebssystemrechten des technischen Betriebssystembenutzers ausgeführt, unter dem das SAP-ERP-System abläuft. Das sind in der Regel weitreichende Administratorrechte. Der Zugriff auf diese Funktion muss daher abgesichert werden. Insbesondere darf es nicht möglich sein, dass Kommandos angelegt oder verändert werden. Daher sollten folgende Hinweise umgesetzt werden:

- Die Berechtigungen, externe Betriebssystemkommandos auszuführen (Berechtigung S_LOG_COM) oder zu pflegen, (Berechtigung S_RZL_ADM mit ACTVT=01) sind restriktiv zu vergeben.
- Der Zugriff auf die Transaktion SM49 "Externe Betriebssystemkommandos ausführen" ist auf die berechtigten Administratoren einzuschränken.
- Der Zugriff auf die Transaktion SM69 "Externe Betriebssystemkommandos pflegen" ist auf die berechtigten Administratoren einzuschränken.
- Für Betriebssystemkommandos können Parameterwerte vorgegeben werden. Das verhindert, dass sich zusätzliche Parameter an die Kommandos anhängen lassen. Davon sollte Gebrauch gemacht werden. Dies trifft insbesondere für selbst definierte Kommandos zu.

Single-Sign-On sicher konfigurieren

Weitere Informationen zu diesem Thema finden sich in APP.4.2.M31 *Konfiguration von SAP Single-Sign-On*.

APP.4.2.M2 Sichere Konfiguration des SAP-JAVA-Stacks

Mit dem Java-Stack eines SAP-ERP-Systems ist es möglich, Java-basierte Anwendungen einzusetzen. Der Java-Stack wird durch einen Applikationsserver gebildet, der die J2EE (Java 2 Enterprise Edition) Spezifikation umsetzt. Im Vergleich zum ABAP-Stack gibt es unterschiedliche Sicherheitsmechanismen und -konzepte.

Im Folgenden werden die aus Sicherheitssicht wichtigsten Schritte aufgezeigt, die bei der initialen Konfiguration des Java-Stacks durchzuführen sind. Die Darstellung beschränkt sich auf die Konfiguration des Applikationsservers und geht damit nicht auf sonstige installierte Applikationen ein.

Java-Stack Installation

Die Installation des Java-Stacks auf einem SAP-ERP-System sollte nur durchgeführt werden, wenn Java-basierte Produkte oder Applikationen eingesetzt werden. Falls der Java-Stack nicht separat installiert werden kann und nicht genutzt wird , muss er so konfiguriert werden, dass darauf nicht zugegriffen werden kann. Dazu sollten alle Dienste des Java-Stacks deaktiviert werden.

Schulung zum Java-Stack

Administratoren des Java-Stacks müssen Kenntnisse in der Architektur und den Sicherheitskonzepten der J2EE-Architektur besitzen. Hier sind insbesondere Kenntnisse bezüglich der statischen Konfiguration der Sicherheit für J2EE-konforme Objekte notwendig, die über das Administrationswerkzeug durch den Administrator durchgeführt wird. Es kommt dabei ein rollenbasiertes Sicherheitskonzept zum Einsatz.

Zu beachten ist, dass SAP den J2EE Java Authentication and Authorization Service (JAAS) um die SAP-spezifischen User-Management- Engine- (UME)- Funktionen erweitert hat. Damit wurde die statische Konfiguration der Sicherheitseinstellungen um eine dynamische Konfigurationsmöglichkeit durch den Programmcode ergänzt, die über die UME gesteuert werden kann. In der UME können daher beispielsweise erlaubte Aktionen in den Programmen zu Rollen zusammengefasst werden. Benutzern kann dann diese Rolle zugeordnet werden, so dass sie damit die benötigten Berechtigungen erhalten.

Administratoren muss zudem bewusst sein, dass der Java-Stack mit einer separaten Benutzer- und Berechtigungsverwaltung ausgestattet ist, so dass hier immer administrative Aufgaben durchgeführt werden müssen. Dazu sollten sie die UME benutzen.

Unnötige Dienste abschalten

Der Java-Stack bietet viele Dienste an, die nicht alle in jedem Szenario benötigt werden. Daher sind aus Sicherheitsgründen alle nicht benötigten Dienste zu deaktivieren. Problematisch dabei ist, dass Dienste voneinander abhängig sein können. Es kann zudem zwischen Systemdiensten und Nicht-Systemdiensten unterschieden werden.

Die Administration, Konfiguration und das Monitoring der J2EE-Instanz erfolgt über den NetWeaver Administrator (NWA), den Nachfolger des Visual- Administrator- Tools. Durch Filter ist es möglich, Dienste im configtool abzuschalten. Dazu müssen folgende Schritte durchgeführt werden:

- Starten des configtool für die Datei: <SAP_install_dir>/<system_name>/<instance_name>/j2ee/configtool directory
- Expertenmodus wählen
- Konfigurationsvorlage oder eine relevante Instanz zum Hinzufügen der Filter wählen
- Filter wählen
- Es kann ausgewählt werden zwischen Start, Stopp oder Abschalten
- Komponente wählen (Service, Library, Applikation oder alle)
- Lieferanten der Komponente eingeben
- Namen der Komponente auswählen
- Durch hinzufügen werden die benutzerdefinierten Regeln der Tabelle hinzugefügt
- In der Tabelle mit den benutzerdefinierten Aktionen Set auswählen und die Änderungen anwenden.

Systeminterne Schlüssel setzen oder neu erzeugen

Für den Betrieb von vertrauenswürdigen Umgebungen und SSL/TLS-Kommunikationen sollten die Systemschlüssel neu generiert werden.

APP.4.2.M3 Netzsicherheit

Die Anwendungs- und Datenbankserver der SAP-Backendsysteme befinden sich in der Regel in der gleichen Netzzone, die vom internen Client-Netz getrennt sein sollte. Nur die erforderlichen Ports sollten zwischen dem Client-Netz und dem Applikationsservernetz geöffnet werden. Die folgenden Einstellungen sollten zur Absicherung des Netzes umgesetzt werden:

Isolierung des Netzes

Das SAP-Servernetz (High Security Area) muss vom Client-Netz (Internal Workstation Network) und von der demilitarisierten Zone (DMZ) über Firewalls getrennt werden. Nur für die erforderliche Konnektivität darf es erlaubt sein, die Firewall zu passieren. Vor allem die Zugriffe auf Datenbanken und auf Betriebssystemebenen müssen blockiert werden. Wenn der direkte Zugriff auf den Datenbankport von SAP-HANA-Systemen wegen Entwickler- oder Administriationstätigkeiten über das HANA Studio erfolgen muss (für Entwickler und Administratoren sollte vordringlich auf die SAP HANA WebIDE verwiesen werden), dann sollte dies nur über ein abgesichertes Administrationsnetz oder einen Terminalserver erfolgen (siehe für Details Baustein SAP HANA)

Datenverschlüsselung

Die gesamte Kommunikation von nicht vertrauenswürdigen Netzen muss authentisiert und verschlüsselt werden. Das interne Netz (Internal Workstation Network) muss als nicht vertrauenswürdig angesehen werden, sofern nicht andere ausreichende Sicherheitsmechanismen vorhanden sind, die es als ein vertrauenswürdiges Netz kennzeichnen.

DMZ Authentisierung

Wenn der Zugang aus dem Internet erfolgt, muss dieser in der DMZ authentisiert und überprüft werden, bevor weitere Verbindungen zu oder Interaktionen mit den inneren Netzen möglich sind.

Absicherung des SAProuters

Alle SAProuter müssen sicher konfiguriert und betrieben werden. Das schließt vor allem folgende Punkte ein:

- Alle anwendbaren Sicherheitshinweise für SAProuter müssen implementiert werden und anstehende Sicherheitskorrekturen müssen regelmäßig aktualisiert und umgesetzt werden.
- Die SAProuter-Routingtabelle muss eingerichtet und gewartet werden, damit der Zugriff beschränkt wird.
- Auf Betriebssystemebene müssen die ausführbaren Programme des SAProuters und auch die SAProuter-Konfigurationsdaten (vor allem die Routing-Tabelle) vor unberechtigten und unerwünschten Änderungen geschützt werden.

Weitere Maßnahmen dazu sind in APP.4.2.M15 *Sichere Konfiguration des SAPRouters beschrieben*.

Absicherung des Web-Dispatchers

Alle SAP Web Dispatcher müssen sicher konfiguriert und betrieben werden. Eine ausführliche Beschreibung dazu ist in der APP.4.2.M25 *Sichere Konfiguration des SAP Web Dispatchers* beschrieben.

Administrativer Zugang

Der administrative Zugang ist für alle Arbeitsstationen einzuschränken, für die ein solcher Zugang geplant ist. Die Firewalls zwischen den Netzsegmenten müssen entsprechend konfiguriert werden. Alle administrativen Zugänge dürfen nur über eine authentisierte und verschlüsselte Verbindung erfolgen. Der Zugang darf nur auf Anfrage erfolgen, wenn die Verbindung nicht auf einer täglichen oder regelmäßigen Basis erforderlich ist.

APP.4.2.M4 Absicherung der ausgelieferten SAP-Standardbenutzer-Kennungen

Es müssen alle Passwörter der ausgelieferten SAP-Standardbenutzer-Kennungen in jedem Mandanten geändert werden. Welche Einstellungen für die jeweiligen Standardbenutzer zu berücksichtigen sind, wird im Folgenden beschrieben:

SAP*

- Bevor der Benutzer SAP* abgesichert wird, sollte ein Notfallbenutzer eingerichtet werden.
- Der Benutzer muss in allen Mandanten über einen Benutzerstammsatz verfügen. Dieser muss gesperrt sein und die Berechtigungen müssen entzogen werden.
- Der Benutzer darf nicht gelöscht werden.
- Der Benutzer ist der Benutzergruppe SUPER zuzuordnen und das Passwort muss geändert werden.
- Protokollierung des Benutzers im Security Audit Log.
- Profilparameter login/no_automatic_user_sapstar muss auf 1 gesetzt werden.

DDIC

- Der Benutzer sollte in allen Mandanten, außer Mandant 000, abgegrenzt und gesperrt sein.
- Der Benutzer benötigt die Zuweisung des Profils SAP_ALL und ist grundsätzlich als hochprivilegierter User mit kritischen Berechtigungen zu betrachten.
- Benutzer der Benutzergruppe SUPER zuordnen und als Systembenutzer einstellen.
- Das Passwort muss geändert werden.
- Protokollierung des Benutzers im Security Audit Log.
- Mithilfe des Notallbenutzers kann DDIC auf einen Dialogbenutzer umgestellt werden.

TMSADM

- Das Passwort des Benutzers muss auf allen Mandanten gleichzeitig geändert werden. Der Report TMS_UPDATE_PWD_OF_TMSADM kann auf dem Mandanten 000 ausgeführt werden.
- Benutzer der Benutzergruppe SUPER zuordnen.
- Der Benutzer TMSADM benötigt exakt die Berechtigungen des Profils S_A.TMSADM.
- Zum Ändern des Passwortes für TMSADM siehe auch SAP-Hinweis 1414256 - Ändern des TMSADM Kennwortes ist zu komplex (siehe [SECNOTE]).
- Der Benutzer sollte nur im Mandanten 000 angelegt sein. Wenn er über Mandantenkopien oder andere Verfahren in andere Mandanten gebracht wurde, sollte er dort gelöscht werden.

WF-BATCH

- Nach der automatischen Generierung des Benutzers ist das Passwort zu ändern und die Benutzergruppe SUPER zu wählen.

Standarduser im SAP Solution Manager

Der SAP Solution Manager wird für den Betrieb einer ERP-Landschaft benötigt, um diese warten zu können. Dazu wird der Solution Manager mit der ERP-Landschaft verbunden. Hierbei werden Benutzer generiert und teilweise mit bekannten Standardpasswörtern versehen. Daher sollte

- die Solution-Manager-Installation auf solche eventuell vorhandenen Konten geprüft werden (SMD_*, SMDAGENT_*, SOLMAN_*, SAPSUPPORT) und
- die Passwörter der generierten User sollten geändert werden.

CONTENTSERV

Falls am ERP-System ein Content-Server genutzt wird, sollte das Passwort dieses generierten Standardusers geändert werden.

EARLYWATCH

Dieser Benutzer ist veraltet und wird vom SAP-Support nicht mehr verwendet. Sofern er vorhanden ist, sollte

- zunächst geprüft werden, ob er gelöscht werden kann. Dasselbe gilt für den Mandanten 066 (siehe auch SAP-Hinweise 1897372 und 1749142, [SECNOTE]).
- Falls der Benutzer noch verwendet wird, sollte beachten werden:
  - Benutzer der Benutzergruppe SUPER zuordnen und Passwort ändern.
  - Protokollierung des Benutzers im Security Audit Log.

SAPCPIC

Dieser Benutzer ist veraltet und wird überwiegend in SAP-ERP-Systemen nicht mehr verwendet. Sofern er vorhanden ist, sollte zunächst geprüft werden, ob er gelöscht werden kann.

Falls der Benutzer noch verwendet wird:

- Der Benutzer muss gesperrt werden, das Passwort ist zu ändern und es ist die Benutzergruppe SUPER zu wählen.
- Protokollierung des Benutzers im Security Audit Log.
- siehe auch SAP-Hinweis 29276 - An welchen Stellen sind Passwörter sichtbar (siehe [SECNOTE]).

Prüfung auf Passwortänderung

Der Report RSUSR003 (Ausführbar über die Transaktion SE38) enthält Informationen über die Standardbenutzer in allen Mandanten. Er überprüft die Standardbenutzer auf Existenz, Sperrstatus und Passwortänderungen. Weitere Hinweise dazu finden sich in APP.4.2.M13 *SAP-Passwortsicherheit*. Der SAP-Service Early Watch Alert kann ebenfalls die Informationen geben, ob das Standardpasswort geändert wurde oder nicht.

APP.4.2.M5 Konfiguration und Absicherung der SAP-Benutzerverwaltung

Mit der Benutzerverwaltung im SAP-ERP-System werden die Benutzerstammsätze der Mitarbeiter angelegt. Für den Mitarbeiter werden z. B. Anmeldenamen, Passwort und Berechtigungsrollen definiert und zugeordnet. Mithilfe der Berechtigungsrollen kann der Mitarbeiter Aktivitäten im SAP-ERP-System durchführen. Für die Administration der SAP-Benutzerverwaltung ist der Benutzeradministrator verantwortlich. Benutzerstammsätze sind mandantenabhängig und müssten in jedem Mandanten separat gepflegt werden. Es gibt jedoch verschiedene Möglichkeiten eine Benutzerverwaltung im SAP-ERP-System zu nutzen. Diese werden im Folgenden kurz vorgestellt.

Zentrale Benutzerverwaltung (ZBV)

Die Benutzerstammsätze werden über ein zentrales System (Zentralsystem) gepflegt und Änderungen automatisch an die angeschlossenen Tochtersysteme übertragen. Daten werden als asynchrone Kommunikation über eine Application-Link-Enabling-Landschaft (ALE-Landschaft) verteilt. Werkzeuge dafür sind die Transaktionen: PFCG, SM59, SU01, SCUA, SCUM, SCUG, SUGR, SCUL, SUIM.

Benutzerverwaltung ohne ZBV

Aufgrund der Mandantenabhängigkeit muss jedes System separat gepflegt werden. Der Transport von Benutzerstammsätzen ist nicht möglich, aber sie können mit dem Mandantenkopierer kopiert werden. Werkzeuge dafür sind die Transaktionen: SU01, SU10, SUIM.

Benutzerverwaltung des Application Server Java (AS Java)

Die Benutzerverwaltung im AS Java wird als Service über die integrierte User Management Engine (UME) bereitgestellt. Abhängig von der Konfiguration werden folgende Benutzerspeicher unterstützt: Datenbank, LDAP Directory und AS ABAP.

Benutzerverwaltung mit SAP NetWeaver Identity Management (SAP IdM)

Benutzerstammsätze und Berechtigungen werden zentral und automatisch über das IdM verwaltet und gesteuert. SAP IdM basiert auf der AS Java Plattform und ist ein eigenständiges Produkt. Im Zusammenspiel mit SAP Access Control (SAP AC) erfolgt die Benutzeradministration und Zuweisung durch Prüfung von SAP-Berechtigungen gemäß bestehenden Compliance-Anforderungen.

Benutzerverwaltung in der SAP HANA

Die Datenbankmanagementsystem-(DBMS)-Benutzer auf SAP HANA werden über einen Mandaten des AS ABAP verwaltet.

Benutzertypen im SAP-ERP-System AS ABAP

Wenn ein neuer Benutzer im SAP-ERP-System angelegt wird, kann zwischen verschiedenen Benutzertypen ausgewählt werden. Der Benutzertyp wirkt sich auf das Anmeldeverhalten und die hinterlegten Passwortregeln aus. SAP definiert fünf verschiedene Benutzertypen:

- **Dialogbenutzer**: Der Dialogbenutzer meldet sich direkt in der SAP GUI des SAP-ERP-Systems mittels Benutzername und Kennwort an (Dialoganmeldung). Setzt der Benutzeradministrator das Passwort, hat es den Status Initial und der Benutzer setzt es durch die Passwortänderung bei Anmeldung auf Produktiv. Mehrfachanmeldungen sind nur mit bestimmten Konfigurationen möglich.
- **Systembenutzer**: Eine Dialoganmeldung ist beim Systembenutzer nicht möglich. Die Anmeldung erfolgt anonym und über den RFC-Aufruf. Systembenutzer werden für technische Abläufe, wie die Hintergrundverarbeitung und Kommunikation, innerhalb eines Systems verwendet. Lediglich der Benutzeradministrator ändert das Passwort und es hat immer den Status "Produktiv". Mehrfachanmeldungen sind immer möglich.
- **Kommunikationsbenutzer**: Kommunikationsbenutzer werden von verschiedenen Benutzern verwendet, um sich von außen über den RFC-Aufruf im SAP-ERP-System anzumelden. Der Benutzeradministrator ändert das Passwort (Status Initial), aber der Benutzer muss es beim RFC-Aufruf nicht ändern. Mehrfachanmeldungen sind immer möglich.
- **Servicebenutzer**: Servicebenutzer des Benutzertyps Service sind mehreren Personen zugeordnet. Dieser wird für anonyme Systemzugänge verwendet, z. B. für Webservices. Die Passwortregeln prüft das System nicht, aber Mehrfachanmeldungen sind immer möglich. Nur der Benutzeradministrator kann das Passwort ändern, das immer den Status "Produktiv" hat.
- **Referenzbenutzer**: Der Referenzbenutzer kann sich nicht am SAP-ERP-System anmelden. Er wird einem Dialogbenutzer zugewiesen und vererbt seine zusätzlichen Berechtigungen an ihn. So wird es ermöglicht, bestimmte Berechtigungsprüfungen durchzuführen. Das Passwort ist immer deaktiviert.

Maßnahmen für eine sichere Administration der Benutzer-IDs im SAP-ERP-System

Systemzugriffe sind nur autorisierten Personen gestattet, die sich im SAP-ERP-System mit einer Benutzer-ID und einem gültigen Passwort authentisieren müssen. Unberechtigte Systemzugriffe können durch bestimmten Sicherheitsmechanismen verhindert werden. Benutzeradministratoren sollten sich an folgende Empfehlung halten:

- Jede Benutzer-ID ist einer realen Person zugeordnet.
- Es sollten keine Sammelkonten angelegt werden.
- Aufgrund der Mandantenabhängigkeit von Benutzerstammsätzen sollte in jedem System die gleiche Benutzer-ID vergeben werden.
- Benutzer-IDs müssen eindeutig sein. Es ist eine Namenskonvention zu definieren. Oftmals besitzen Mitarbeiter eine eindeutige Identifikationsnummer, diese kann auch als Benutzer-ID übernommen werden.
- Benutzer sollten einer bestimmten Benutzergruppe wie Internen, Externen, Partnern oder technischen Benutzern zugeordnet werden (siehe SAP-Hinweis 1663177, [SECNOTE]).
- Einschränkung des Zeichenvorrats für den Benutzernamen, damit ein Name nicht nur aus "alternativen" Leerzeichen besteht (siehe SAP-Hinweis 1731549, [SECNOTE]).
- Die Zuordnung der Berechtigungsprofile SAP_ALL und SAP_NEW muss vermieden werden. SAP_ALL sollte außer Notfallbenutzerkonten keine Benutzer zugewiesen bekommen. Diese Konten sollten dann ausreichend kontrolliert und überwacht werden. SAP_NEW sollte beispielsweise nur für den technischen Teil des Release-Upgrades genutzt werden.

Vorteile numerischer Benutzer-IDs

Es ist sinnvoll numerische Benutzer-Ids zu verwenden, da sie folgende Vorteile haben:

- Groß- und Kleinschreibung werden nicht verwechselt, wenn Benutzer-IDs nur aus numerischen Zeichen bestehen.
- Numerische Benutzer-IDs reflektieren den Realnamen einer Person nicht und können auch nicht direkt zugeordnet werden.
- Keine Änderung der numerischen Benutzer-ID bei Namensänderungen.
- Anhand der Nummernkreise für Benutzerkennungen werden grobe Zuordnungen durchgeführt.

Weitere Maßnahmen in der Benutzerverwaltung

Inaktive Benutzer im SAP-ERP-System sollten gesperrt oder ungültig gesetzt werden. Mit dem Report RSUSR_LOCK_USER können Administratoren inaktive Benutzer automatisch sperren lassen. Auch sollte regelmäßig ein Benutzerabgleich durchgeführt werden. Damit wird verhindert, dass die Zuordnung der Profile zu den Benutzern veraltet ist. Das kann entweder mit der Transaktion PFUD durchgeführt werden oder mit dem Report RHAUTUPD_NEW, der den Hintergrundjob PFCG_TIME_DEPENDENCY einplant. Benutzer, die über einen längeren Zeitraum auf dem SAP-ERP-System nicht aktiv waren, sollten automatisch abgemeldet werden. Dazu muss der Profilparameter rdisp/gui_auto_logout in der Transaktion RZ10 mit der entsprechenden Zeit eingestellt werden (in Sekunden).

APP.4.2.M6 Erstellung und Umsetzung eines Benutzer- und Berechtigungskonzeptes [Entwickler, Fachabteilung, Leiter IT]

Die Funktionen eines SAP-ERP-Systems werden über Transaktionen aufgerufen, die dabei unterschiedliche Operationen oder Aktivitäten auf Daten ausführen können. Die über Transaktionen gestarteten Applikationen prüfen, ob der aufrufende Benutzer über die notwendigen Berechtigungen verfügt, die angeforderte Operation auf den durch die Applikation angesprochenen Daten auszuführen.

Prinzipien

Im ersten Schritt werden die grundlegenden Prinzipien vorgestellt, die für ein SAP-Berechtigungskonzept relevant sind:

Identitätsprinzip

Natürliche Personen, die im SAP-ERP-System einen Benutzer erhalten, müssen eindeutig zugeordnet werden. Handelt es sich um einen technischen Benutzer im SAP-ERP-System, muss nachvollziehbar sein, welche natürliche Person ihn verwendet hat. Es gilt zu vermeiden, dass eine natürliche Person im SAP-ERP-System viele unterschiedliche SAP-Benutzer erhält. Zur Vermeidung von systemübergreifenden Zugriffsrisiken sollte ein systemübergreifendes Benutzer-Mapping erstellt werden. Mit dem Identity-Management-Konzept kann im SAP-ERP-System umgesetzt werden, dass eine SAP-Benutzer-ID systemübergreifend verteilt wird.

Minimalprinzip

Es werden nur die Transaktionen und Zugriffe für einen Benutzer berechtigt, die für den Benutzer zur Erfüllung seiner Tätigkeiten wirklich notwendig sind. Das Minimalprinzip muss in Bezug auf Datenqualität (z. B. Name, Wohnsitz, E-Mail Adressen, Kontodaten, Ware) dem organisatorischen Bezug (z .B. zuständige Landesorganisation) und den zeitlichen Bezug (z. B. Bestellzeitpunkt, Jahr der Bestellung) eingehalten werden. Beispielsweise benötigen Mitarbeiter im Versand nur die Informationen über die Bestellungen und nicht Informationen über Kontodaten.

Stellenprinzip

Alle natürlichen Personen, die einen Benutzer im SAP-ERP-System erhalten, müssen einer definierten Funktion in der Organisation zugeordnet sein. Zum einen dient die Form einer Aufbauorganisation, da sich grundsätzlich alle Aufgaben in Stellen definieren lassen. Das ist aber nicht zwingend Voraussetzung für das Stellenprinzip (Zuordnung über Organisationsmanagement).

Belegprinzip der Buchhaltung

Alle zahlungsrelevanten und bilanzwirksamen Vorgänge müssen gemäß dem Prinzip der Buchhaltung (in Deutschland: GoB) nachvollziehbar sein und für jedes Berechtigungsprinzip sichergestellt werden. Es muss ersichtlich sein, wer der Erfasser und Änderer des Beleges ist. Alle Zugriffe auf die Datenbank, die einen Beleg erzeugen, und jede dazugehörige Aktion (z. B. erfassen, ändern, löschen) umfassen das Belegprinzip.

Belegprinzip der Berechtigungsverwaltung

Alle relevanten Daten von Benutzern müssen gemäß der definierten Aufbewahrungsfrist gesichert und aufbewahrt werden. Folgende Informationen müssen aufbewahrt werden: die Zuordnung des Benutzers zu einer natürlichen Person, die Zuweisung von Berechtigungen, Art, Umfang, Änderungen und Änderer der Berechtigungen.

Funktionstrennungsprinzip

Mit dem Funktionstrennungsprinzip, auch Segration of Duties (SoD) genannt, wird gewährleistet, dass Benutzer nicht alle Prozesse in einem SAP-ERP-System allein ausführen können. Das Prinzip der Funktionstrennung muss beispielsweise in der Benutzer- und Berechtigungsadministration eingehalten werden. Administratoren, die in der Benutzerverwaltung zuständig sind, sollten nicht SAP-Berechtigungsrollen erstellen. Bei kleineren Institutionen kann ein Funktionstrennungsprinzip teilweise nicht durchgeführt werden. In dem Fall sollten kompensierende Kontrollen (auch mitigation controls) eingesetzt werden. Diese Kontrollen müssen in regelmäßigen Abständen geprüft werden.

Genehmigungsprinzip

Mit dem Genehmigungsprinzip wird veranlasst, dass Berechtigungen genehmigt werden müssen, bevor die Berechtigungsrollen erstellt oder sie einem Benutzer zugeordnet werden.

Bevor Berechtigungen an Benutzer vergeben werden, müssen diese nachvollziehbar genehmigt werden. Die Genehmigung sollte durch eine definierte Stelle durchgeführt werden. Es kann zwischen einer implizierten und explizierten Genehmigung unterschieden werden. Eine implizierte Genehmigung ist die indirekte Zuordnung von Berechtigungen, d. h. Berechtigungen werden ausschließlich über ein technisch definiertes Stellenkonzept vergeben. Die explizierte Genehmigung ist die direkte Vergabe einer Berechtigung an einen Benutzer.

Die Genehmigung eines Rollenantrags für einen SAP-Dialogbenutzer sollte nach dem Vier-Augen-Prinzip erfolgen. Wer welche Genehmigung für welchen Prozess durchführt, muss von der Institution definiert werden. Im ersten Schritt kann es der Vorgesetzte des SAP-Dialogbenutzers sein und im zweiten Schritt kann es der Prozessinhaber der angeforderten Rolle sein.

Genehmiger von Rollenzuordnungen

Die Genehmiger von Rollenzuordnungen sind für die Vergabe von Benutzerrechten verantwortlich. Sie genehmigen die Freigabe und den Entzug von Benutzerrollen für einzelne Benutzer im SAP-ERP-System. Die Genehmiger sollten die folgenden Kenntnisse im SAP-ERP-System besitzen:

- Kenntnis der betroffenen SAP-Prozesse,
- Kenntnis der organisatorischen Aufbau- und Ablauforganisation,
- Kenntnis der Aufgaben und Organisationsstruktur der jeweiligen Anwender,
- Kenntnis des Inhaltes der bestehenden Benutzerrollen in ihrem Verantwortungsbereich.

Der Genehmiger legt für die Rollen seines Verantwortungsbereiches fest, welche Benutzer, einschließlich der Geschäftspartner, welche Aufgaben im SAP-ERP-System durchführen dürfen. Die eingetragenen Benutzerstämme sollten im Produktivsystem regelmäßig (z. B. einmal im Quartal) auf ihre Aktualität geprüft werden. Die Prüfunterlagen sind zehn Jahre lang aufbewahrungspflichtig.

Standardprinzip

Zur Vereinfachung des Berechtigungskonzeptes ist notwendig, dass technische Standards eingehalten werden. Lösungen und Risiken werden an Hand des Standards definiert. Wird vom Standard abgewichen, kann das weitreichende Folgen für die Sicherheit des Berechtigungskonzeptes haben. Alle Änderungen die vom Standard abweichen, müssen immer dokumentiert werden.

Schriftformprinzip

In der Institution muss das genehmigte Berechtigungskonzept schriftlich vorliegen. Des Weiteren muss das Konzept für Externe nachvollziehbar und verständlich sein. Es sollte Auskunft über die technische Realisierung, die betriebswirtschaftliche Nutzung der Berechtigungen, und der Umsetzung der normativen Grundlagen geben.

Kontrollprinzip

Die Umsetzung des Berechtigungskonzeptes muss durch Kontrollen innerhalb der Berechtigungsadministration sowie durch neutrale Prüfer überprüft werden. Die folgenden Punkte sollten mit dem Berechtigungskonzept kompatibel sein:

- technische Standards im System
- Ausprägungen der Berechtigungen
- Zuordnung der Benutzer
- Passwortregeln
- Anzahl der inaktiven Benutzer
- Anzahl der gesperrten Benutzer
- Unbekannt-Sperrungen aufgrund von Falschanmeldungen

Rahmenbedingungen

Über diese Prinzipien hinaus sollten beim Aufbau eines Berechtigungskonzeptes die folgenden Rahmenbedingungen berücksichtigt werden:

- datenschutzrechtliche Bestimmungen,
- Gesetzliche Rahmenbedingungen wie die Grundsätze ordnungsmäßiger Buchführung (GoB), das Handelsgesetzbuch (HGB), International Financial Reporting Standard (IFRS) oder Sarbanes Oxley Act (SOX),
- Konzernvorgaben,
- Anforderungen der internen Qualitätsmanagementsysteme.

Grundbegriffe

Die wichtigsten Begriffe im Zusammenhang mit dem SAP-Berechtigungskonzept sind:

- **PFCG Einzelrolle**: Die Erstellung und Änderung der Rollen erfolgt mit dem Profilgenerator (Transaktion PFCG). Mit dem Profilgenerator wird ein Berechtigungsprofil automatisch generiert.
- **Businessrolle**: Beschreibt den Arbeitsplatz eines Benutzers und beinhaltet alle dafür notwendigen (Sammel-)rollen in den Systemen, in denen der Benutzer Berechtigungen für den Arbeitsplatz benötigt.
- **Berechtigungsobjektklasse**: Logische Zusammenfassung von Berechtigungsobjekten, z. B. alle Berechtigungsobjekte der Finanzbuchhaltung beginnend mit "F_" werden zur Objektklasse FI gezählt.
- **Berechtigungsobjekt**: Im Programmcode wird zur Berechtigungsprüfung das technische Objekt aufgerufen und gegen den Benutzerpuffer geprüft. Das Berechtigungsobjekt fasst 1 bis 10 Berechtigungsfelder zusammen, die in Kombination als UND-Verknüpfung geprüft werden.
- **Berechtigungsfeld**: Ist ein Bestandteil des Berechtigungsobjekts und die kleinste Einheit mit Werten wie Lesen, Ändern, Anlegen.
- **Berechtigungsprofil**: Sobald eine Rolle generiert wurde, wird automatisch das dazugehörige Berechtigungsprofil erstellt, welches die Ausprägung der einzelnen Berechtigungsobjekte (Werte) enthält.
- **Benutzer**: Meldet sich im SAP-ERP-System an und erhält über die Zuordnung der Berechtigungsprofile Zugriff auf Funktionen und Objekte.
- **Benutzertyp**: Der klassische Endanwender ist ein Dialog-Benutzer. Im SAP-ERP-System gibt es z. B. noch Servicebenutzer, Systembenutzer und Kommunikationsbenutzer.

Umsetzung

Wenn ein Berechtigungskonzept entwickelt wird, gibt es dabei viele Herausforderungen, die von den SAP-Berechtigungsadministratoren zu lösen sind. So steigt beispielsweise die Anzahl der Rollen mit der Anforderung nach organisatorischer Trennung, aber auf der anderen Seite wird in den Geschäftsanforderungen die Abgrenzung in reine Organisationseinheiten gefordert. Gleiches gilt für die Rollen der Mitarbeiter. Es gibt viele unterschiedliche Rollen für die gleichen Arbeitsplätze aufgrund der individuellen Aufgaben der Mitarbeiter, was wieder zu einer hohen Rollenanzahl im SAP-ERP-System führt.

SAP hat daher einen Best-Practice-Ansatz für ein SAP-Berechtigungskonzept entwickelt. Die folgenden Schritte unterstützen Benutzer- und Berechtigungsadministratoren bei der Erstellung des Konzeptes:

1 Erstellen eines Projektplans
2 Erstellen eines Berechtigungsrahmenkonzepts
3 Definition der Namenskonventionen
4 Definition der Einzelrollen
5 Identifizierung kritischer Berechtigungen oder Berechtigungskombinationen
6 Definition der Orglevel-Sets
7 Definition der Sammelrollen
8 Rollen-Konsolidierung
9 Definition der Rollenverantwortlichen
10 Implementierung und Test
11 Zuordnung zu Benutzern

Grundsätzlich muss die Trennung der Verantwortlichkeiten im Berechtigungswesen eingehalten werden. Es muss einen Benutzeradministrator, einen Berechtigungsadministrator und eventuell einen Profiladministrator geben. Die Administratoren sollten Benutzergruppen zugeordnet werden, die von ihnen selbst nicht verändert werden können (Vier-Augen-Prinzip), d. h. in den Rollen der Administratoren sollte die Pflegeberechtigung für diese Gruppen nicht enthalten sein.

Folgende Punkte müssen für die Umsetzung eines Benutzer- und Berechtigungskonzept noch beachtet werden:

Profilgenerator

Mit dem Profilgenerator (Transaktion PFCG) werden die SAP-Rollen und deren Berechtigungsdaten gepflegt. Der Profilgenerator wird als Standardwerkzeug zur Rollenpflege eingesetzt. Die Funktionen des Profilgenerators erleichtern die Pflege der SAP-Rollen, indem sie verschiedene Prozesse automatisieren und der Umsetzung des Berechtigungskonzepts mehr Flexibilität verleihen. Es wird empfohlen, im Profilgenerator jede Änderung an einer SAP-Rolle im Feld Langtext der Beschreibungskarte zu dokumentieren.

Berechtigungsprüfung der Berechtigungsobjekte

Die Prüfung der Berechtigungsobjekte erfolgt im ABAP-Code über die Anweisung AUTHORITY-CHECK. Es wird überprüft, ob der Benutzer in seinem Benutzerstammsatz über die entsprechenden Berechtigungen verfügt, die im AUTHORITY-CHECK als Bedingung hinterlegt sind. Kundeneigene Berechtigungsobjekte müssen in der Transaktion SU21 und Berechtigungsfelder in der Transaktion SU20 angelegt werden. Diese kundeneigenen Berechtigungsobjekte können bis zu zehn Felder enthalten.

SU24 - Vorschlagswerte Profilgenerator

Für die Pflege der SAP-Berechtigungsrollen wird die Anwendung der Transaktion SU24 empfohlen. Innerhalb von SU24 werden Vorschlagswerte und Prüfkennzeichen (inklusive dem globalen Deaktivieren von Berechtigungsprüfungen) gepflegt. In einem Konzept muss ausführlich beschrieben werden, wie SU24 genutzt werden soll. Die Transaktion SU24 bedeutet initial zusätzlichen Aufwand, allerdings ist es dadurch deutlich einfacher, die SAP-Berechtigungsrollen zu pflegen. Weitere Vorteile sind:

- vermeidet wiederholende Berechtigungsfehler,
- SAP-Standard,
- dokumentiert benötigte Berechtigungen,
- unterstützt den Rollenentwicklungsprozess,
- erleichtert die Anpassung des Berechtigungskonzepts während eines Upgrades erheblich sowie
- Vorschlagswerte werden auch in der Risikodefinition von Access Control verwendet.

In der Transaktion SU24 werden nicht nur die Transaktionen gepflegt, sondern unter anderem auch RFC-Bausteine oder Web-Dynpro-Anwendungen. Die Vorschlagswerte können auch über Traceauswertungen bezogen werden, entweder mit dem Systemtrace oder dem Langzeittrace.

Systemtrace (ST01, STAUTHTRACE) und Langzeittraces (STUSOBTRACE, STUSERTRACE)

Mit dem Systemtrace werden alle Berechtigungsprüfungen, z. B. während eine Transaktion ausgeführt wird, mitgeschrieben und alle fehlgeschlagenen Berechtigungsprüfungen werden analysiert und angepasst. Folgendes ist zu beachten:

- Der Trace wird im Kernel aufgezeichnet und beeinflusst daher die Performance des ganzen SAP-ERP-Systems. Der Trace sollte nur für ausgewählte Benutzer oder über einen kurzen Zeitraum laufen.
- Der Trace darf nicht ohne Wissen der aufzuzeichnenden Benutzers eingeschaltet werden: Leistungs- und Verhaltenskontrolle.
- Der Trace ist applikationsserverspezifisch und muss daher auf allen Servern eingeschaltet werden.

Um Berechtigungserfordernisse zu ermitteln, die sich nicht direkt aus unmittelbaren Tests von ausführenden Dialogusern ergeben, ist der Systemtrace wenig effizient. In solchen Fällen sollten alternativ Langzeittraces verwendet werden. Folgendes ist zu beachten:

- Die Langzeittraces werden nicht, wie der Systemtrace, auf Dateisystemebene geschrieben, sondern in die Datenbank. Das beeinträchtigt die Performance mehr als der Systemtrace. Daher sollten Langzeittraces nur mit Filter eingeschaltet werden.
- STUSOBTRACE: Systemweit, mandantenübergreifend, benutzerunabhängig, jede Berechtigungsprüfung einer Programmstelle wird nur einmal erfasst. Es erfolgt also keine Erfassung von Benutzern mit Zeitstempeln.
- STUSERTRACE: Systemweit, mandanten- und benutzerabhängig, jede Berechtigungsprüfung einer Programmstelle wird pro Benutzer einmal mit dem ersten Zeitstempel erfasst.

Organisationsebenen

Die Organisationsebenen bilden die Unternehmensstruktur im SAP-ERP-System ab. Dabei bilden sie die Aufbauorganisation (z. B. Buchungskreis), die Ablauforganisation (z. B. Kontenplan) oder die technisch-organisatorischen Trennungen ab. In den Berechtigungsobjekten bilden Organisationsebenen spezielle Felder ab, die eine besondere Pflege ermöglichen. Es gibt Standard-Organisationsebenen und es ist möglich, kundeneigene Organisationsebenen zu definieren. Organisationsebenen sind komponentenspezifisch und stehen in Relation zueinander. Sie stellen Unterscheidungsmerkmale dar, nach denen Berechtigungen differenziert werden können.

Synchronisation mit dem Rollenkatalog im Fiori-Gateway und mit nativen HANA-Berechtigungen

Bei modernen S/4HANA-Systemen werden neben den Detailberechtigungen im ABAP-Backend auch Rollen für den Anwendungskatalog im Fiori-Gateway (Frontendsystem) benötigt. Diese müssen mit den Backendrollen abgestimmt sein, damit die Navigation auf dem Frontend zu den Berechtigungen auf die Businessdaten passt. In der PFCG gibt es hierzu Synchronisationsprozesse, die zu beachten sind. Darüber hinaus müssen bei der Einbettung nativer HANA-Applikationen entsprechend auch Benutzer und Berechtigungen passend zum Gesamtberechtigungskonzept auf der HANA-Datenbank erarbeitet und mit den Berechtigungen auf den Frontend- und Backendsystemen abgestimmt und synchron gehalten werden (siehe dazu auch SAP HANA Baustein).

Prozesse der Berechtigungsadministration

Die folgenden Prozesse müssen im Rahmen der Berechtigungsadministration definiert werden: Rollen anlegen, Rollen ändern, Rollen löschen, Rollen transportieren und SU24-Vorschlagswerte transportieren. SAP-Berechtigungsrollen sollten nur im Entwicklungssystem angelegt und gepflegt werden. Sie werden mithilfe des Transport-Management-Systems (TMS) durch die verschiedenen Systemstufen transportiert.

Rollen und Profile können zusammen transportiert werden. Jedoch sind diese mandantenabhängig und müssen über Transportaufträge in die anderen Mandanten verteilt werden. Nach einem Transport muss der Benutzerstammsatz aktualisiert werden (Massenabgleich). Rollen können auch heruntergeladen und lokal gespeichert werden oder in einem anderen System wieder hochgeladen werden. SU24-Vorschlagswerte können mit allen Änderungen der USOBX_C und USOBT_C transportiert werden.

Definition der Arbeitsplatzrollen

Es werden Arbeitsplätze definiert und hierfür Mitarbeiter zugeordnet. Ein Ansatz ist es für jeden Arbeitsplatz Businessrollen zu entwickelt, die alle für den Arbeitsplatz notwendigen Einzelrollen sowie Sammelrollen umfassen. Die Businessrolle wird allen Mitarbeitern eines Arbeitsplatzes zugeordnet. Kritische Funktionen, die nur von einigen Mitarbeitern eines Arbeitsplatzes ausgeführt werden sollen, sind in zusätzlichen Add-on-Sammelrollen enthalten. Beispiele für Businessrollen sind Lagermitarbeiter, Sachbearbeiter Vertrieb oder Einkaufsleiter.

Einhaltung der Funktionstrennung

Die Einhaltung der Funktionstrennung sollte mit der Berechtigungsvergabe nach dem Vier-Augen-Prinzip durchgeführt werden. Ein Benutzer darf immer nur einen Teilprozessschritt im Rahmen eines geschäftskritischen Prozesses ausführen. Um Betrug zu vermeiden, werden die Berechtigungen über verschiedene Benutzer verteilt.

Grundsätzlich sind Berechtigungen auf Stamm- und Bewegungsdaten voneinander zu trennen, z. B. Bestellungen aufgeben und Lieferantendaten ändern. Die Funktionstrennung definiert sich z. B. über Vorgaben von SOX (nicht verbindlich für Organisationen, die an der NASDAY gelistet sind). SOX fordert die Definition von Risiken und die Auswertung und Kompensation von Konflikten. Ein kontinuierliches Monitoring auf die SoD-Konfliktfreiheit von Rollen und die Vergabe von kritischen Berechtigungen an Anwender sollte mit geeigneten Werkzeugen durchgeführt werden, um Abweichungen frühzeitig erkennen zu können. Mit dem Tool SAP Access Control können SAP-spezifische Risikoanalysen von Benutzer- und Rollenzuordnungen durchgeführt, geprüft und dokumentiert werden.

Definition von Berechtigungen für technische Benutzer

Neben der Berechtigung von Endanwendern werden in SAP-ERP-Systemen auch Berechtigungen für spezielle technische Konten, etwa für den Hintergrund- oder Schnittstellenbetrieb benötigt. Dabei sollte darauf geachtet werden, solche Konten jeweils szenarienbezogen auszugestalten und (nach Minimalprinzip) zu berechtigen. Es sollte vermieden werden, einen einzigen technischen Benutzer für viele Schnittstellen und Hintergrundjobs zu verwenden, da ein solcher Benutzer zu umfangreiche Berechtigungen hat und das Risiko einer Beeinträchtigung der Verfügbarkeit erheblich erhöht ist.

Aktivierung schaltbarer Berechtigungsprüfungen

Ausgewählte Berechtigungsprüfungen (insbesondere im Schnittstellenumfeld) werden von SAP als optional zuschaltbar ausgeliefert (SACF). Im Berechtigungskonzept muss bestimmt werden, welche Prüfungen aktiv geschaltet werden müssen und welche inaktiv verbleiben sollen.

Zusammenfassung der SAP-Berechtigungsrichtlinien:

- Positives Berechtigungskonzept: Alle Zugriffe und Aktionen müssen explizit erlaubt werden.
- Minimalprinzip: Es werden nur so viele Transaktionen und Zugriffe für einen Anwender berechtigt, wie er auch wirklich benötigt.
- Rollenbasiertes Berechtigungskonzept: Berechtigungen werden in den PFCG-Rollen angelegt, gespeichert und dem Benutzer zugeordnet.
- Funktionstrennung: Es sollten keine Funktionstrennungskonflikte in einzelnen Rollen vorhanden sein.
- Das Rollenkonzept orientiert sich an der Organisationsstruktur der Institution.
- Rollen werden nach Anzeige- und Änderungsberechtigung unterschieden.
- Alle Mitarbeiter der Institution, die innerhalb der Organisation dieselben Aufgaben haben, sollen auch mit denselben Berechtigungen arbeiten.
- Die Rollen unterscheiden sich nur in der Ausprägung der jeweiligen Organisationsebenen.
- Trennung der Verantwortlichkeiten. Es muss einen extra Berechtigungsadministrator geben.
- Es muss ein Notfallkonzept erstellt werden, falls im Produktivsystem Berechtigungsprobleme auftreten oder im Customizing Änderungen durchgeführt werden müssen (siehe APP.4.2.M28 Erstellung eines Notfallkonzeptes und APP.4.2.M29 Einrichten eines Notfallbenutzers).
- Vollständigkeit: Das Rollen- und Berechtigungsdesign muss auch den Betrieb technischer Konten abdecken, also auch die Berechtigung von Hintergrund- und Schnittstellenbenutzern. Auch für diese ist das Minimalprinzip zu gewährleisten.

APP.4.2.M7 Absicherung der SAP-Datenbanken

Auf Datenbanken kann mittels SAP-Tools und Software von Drittherstellern zugegriffen werden. Generell wird empfohlen, dafür SAP-Tools zu benutzen.

Es ist notwendig, die Passwörter für die Standardbenutzer der Datenbank zu ändern, da SAP diese im Klartext ausliefert. Das Standardpasswort für die Benutzer SAPR3 oder SAP<SID> muss immer geändert werden. Zum Schutz der Standardbenutzer müssen folgende Maßnahmen umgesetzt werden:

- Standardpasswörter sollten nicht übernommen werden.
- Sicherer Passwörter sollten verwendet werden.
- Wird das DBM-Benutzerkonto vorübergehend genutzt, ist ein zweites temporäres Passwort für den DBR-Benutzer zuzuweisen.
- Um Passwörter für SAP MaxDB Standardbenutzer zu ändern, sollte das Datenbankwerkzeug Database Manager CLI oder das Computing Center Management System (CCMS) genutzt werden.

Des Weiteren muss der Zugriff auf die folgenden Tabellen für andere Datenbankbenutzer unterbunden werden:

- USR* Tabellen
- T000 Tabelle (keine Schreibrechte)
- Allgemeine Tabellen (wie SAPUSER oder RFCDES) oder anwendungsspezifische Tabellen (wie PA* oder HCL*)

Wird auf Daten in der Datenbank mittels Software von Drittherstellern zugegriffen, müssen bestimmte Sicherheitsmaßnahmen durchgeführt werden. Die Benutzer SAPR3 oder SAP<SID> sind nicht zur Verbindung zur Datenbank zu nutzen. Dafür sollten andere Benutzer erstellt werden, welche besonders zu pflegen sind:

- die Zugriffsrechte auf die erforderlichen Tabellen sind einzuschränken,
- nur lesender Zugriff sowie
- kein Benutzer sollte die Berechtigung erhalten, alle Tabellen pflegen zu können.

Ebenfalls ist darauf zu achten, dass bei Nutzung von Software von Drittherstellern keine Schäden in Bezug auf die Sicherheit der Konsistenz oder Berechtigung der Datenbank erfolgt.

Authentisierung und Verschlüsselung der Datenbanken

Nach der Installation müssen die Systemschlüssel auf individuelle Werte geändert werden (SAP HANA: Master Encryption Key ändern). Auch die Passwörter der Benutzer, die zur Authentisierung auf dem SAP-ERP-System für die Datenbank oder für ein Datenbanktool notwendig sind, müssen regelmäßig geändert werden. Um den Authentisierungsprozess sowie die Kommunikation abzusichern, gibt es die folgenden Methoden:

- Es ist der Verschlüsselungsmechanismus zu verwenden, der von den proprietären Datenbanktreibern zur Verfügung gestellt wird.
- Es sind Betriebssystemmethoden oder Anwendungsmethoden wie zum Beispiel SSH oder SSL-Tunnel zu verwenden.
- Applikations- und Datenbankserver sollten in einem separaten Hochsicherheitsnetzsegment abgelegt werden. Die Überwachung des Netzverkehrs sollte erschwert werden.
- Die Verschlüsselung in solch einem Netzsegment ist nicht zwingend erforderlich, wird aber empfohlen.
- Es sollte SSF für die ABAP-Technologie verwendet werden.

SAP MaxDB Sicherheit

Die verantwortlichen Datenbankadministratoren sollten für die Absicherung der SAP MaxDB folgende Einstellungen vornehmen:

- Die Passwörter der Datenbankbenutzer müssen entsprechend den Passwortrichtlinien der Institution gepflegt sein. Das betrifft vor allem die Standardpasswörter der Benutzer DBADMIN, DBA und DBM. Das Standardpasswort muss geändert werden.
- Es ist ein Benutzer- und Berechtigungskonzept für die Datenbankbenutzer zu definieren und zu implementieren.
- Software und Funktionen sind auf das erforderliche Minimum zu begrenzen:
  - Es ist nur Software zu installieren, die wirklich benötigt wird.
  - Die Global Listener und SAP MaxDB Server sind für die lokale Kommunikation abzuschalten.
  - Der SAP MaxDB X Server ist ohne NI Support (Unix und Linux) zu starten.
  - Demo Daten sind zu entfernen.

- Trace- und Logdateien:
  - Tracedateien sind nur zur Suche von Fehlern zu benutzen. Alle Tracedateien sind zu entfernen und das Schreiben des Traces ist zu deaktivieren, nachdem die Auswertung beendet wurde.
  - Der Zugriff auf Logdateien ist zu beschränken.
  - Der Zugriff auf Betriebssystembefehle und -funktionen ist zu beschränken.
  - Die Serverberechtigungen zum Lesen von Datenbankdateien sind bei allen DBM-Betreibern zu entziehen, um den Zugriff auf Logdateien zu unterbinden.
  - Im Datenbankmanager CLI sind die DBFileRead Serverberechtigungen zu entziehen.

Oracle DB Sicherheit

Zur Absicherung einer Oracle-Datenbank müssen die Passwörter regelmäßig und nach den Richtlinien der Passwortsicherheit geändert werden (siehe hierzu auch dem Baustein). Das betrifft vor allem die Passwörter der Benutzer SAP<SID> oder SAPR3. Deshalb muss ein Berechtigungskonzept für die Datenbankbenutzer definiert und umgesetzt werden.

Der Benutzer OPS$ ist für die Windowsbenutzer zu definieren, die für den Betrieb des SAP-ERP-Systems notwendig sind. Normalerweise sind das die Benutzer SAPService<sid> und <sid>adm. Der Name kann ebenfalls geändert werden. Im SAP-Hinweis 50088 (siehe [SECNOTE]) sind weitere Informationen zum Erstellen des OPS$-Benutzers auf Windows beschrieben.

Sofern es technisch umsetzbar ist, sollte die OPS$-Remoteverbindung durch die "Secure Storage in File System"-(SSFS)-Methode ersetzt werden. Der Zugriff auf die Datenbank ist durch die erforderlichen IP-Adressen einzuschränken.

APP.4.2.M8 Absicherung der SAP-RFC-Schnittstelle

Für die sichere Konfiguration der RFC-Schnittstelle müssen vor allem die Einstellungen der RFC-Verbindungen, der RFC-Berechtigungen und die Absicherung der RFC-Gateways betrachtet werden.

RFC-Verbindungen

RFC-Verbindungen sollten nach bestimmten Richtlinien verwaltet werden. RFC-Verbindungen können zwischen verschiedenen Systemen der gleichen Sicherheitsklassifizierung (z. B. von einem Produktivsystem zu einem anderen) oder von einem System der höheren Sicherheitsklassifizierung zu einem System mit niedrigerer (z. B. von einem Produktivsystem zu einem Testsystem) angelegt werden.

Es ist nicht erlaubt, Benutzerdaten oder eine Trusted-Systemanmeldung von einem System mit einer niedrigen Sicherheitsklassifizierung zu einem System mit einer höheren Sicherheitsklassifizierung zu nutzen. Diese Verbindungen sind nur erlaubt, um technische Verbindungskonfigurationen zu speichern und Benutzer für jeden Zugriff zu authentisieren.

Folgende Empfehlungen und Umsetzungen sind für RFC-Verbindungen zu beachten:

- Alle RFC-Verbindungen müssen einem für die Verbindungen, verantwortlichen Benutzer hinzugefügt werden. Der Verantwortliche kann Informationen zur Notwendigkeit und Verwendung der RFC-Verbindungen zur Verfügung stellen. RFC-Verbindungen, die nicht länger benötigt werden, sind zu löschen.
- RFC-Verbindungen mit gespeicherten Benutzerdaten oder solche, die eine Trusted-Systemanmeldung benutzen, müssen mit der gleichen Sicherheitsklassifizierung oder von einer höheren zu einer niedrigen Sicherheitsklassifizierung genutzt werden.
- Beim Betrieb des SAP-ERP-Systems werden von den von außen aufrufbaren Funktionsbausteinen (remote enabled) typischerweise weniger als zehn Prozent wirklich benötigt. Bei allen anderen Funktionsbausteinen sollte die Remote-Fähigkeit abgeschaltet werden. Ab Release 740 steht hierfür eine Standardfunktion zur Verfügung, mit der die RFC-Funktionsbausteinnutzung gemessen und ungenutzte Bausteine für den Remote-Zugriff deaktiviert werden können (UCON). Dies sollte umgesetzt werden.

RFC-Berechtigungen

Der Zugriff auf Trusting-Systeme wird durch das Berechtigungsobjekt S_RFCACL gesteuert und muss streng kontrolliert werden. Des Weiteren muss die Vergabe von Wildcard-Berechtigungen (*) für das Objekt vermieden werden. Es muss sichergestellt werden, dass der Profilparameter auth/rfc_authority_check aktiviert ist. Alle RFC-Verbindungen mit gespeicherten Anmeldeinformationen sollten dokumentiert werden. Ebenfalls muss sichergestellt werden, dass diesen RFC-Benutzerkonten auf dem Zielsystem nur die Mindestberechtigungen (vor allem nicht SAP_ALL) und die Benutzergruppe SYSTEM zugewiesen werden. Innerhalb des SAP Solution Manager hat SAP dafür eine Diagnosefunktion implementiert.

Zusammenfassend sind die folgenden Maßnahmen umzusetzen:

- Die RFC-Berechtigungsprüfung wird mit dem Profilparameter auth/rfc_authority_check = 1 aktiviert.
- Der Benutzertyp für die RFC-Verbindungen ist SYSTEM.
- Eine Namenskonvention für die RFC-Serverbenutzer sollte entwickelt werden.
- Die Berechtigungen auf dem Zielsystem sind stark einzuschränken. Kein SAP_ALL!
- Keine Wildcard-Berechtigung für das Berechtigungsobjekt S_RFCACL.

Absicherung des RFC-Gateways

RFC-Gateways sind Teil jeder ABAP-Instanz, sie sollten aber unabhängig von dieser Instanz installiert werden. Ein Gateway-Betrieb ist zum Beispiel für bestimmte Java-Anwendungen notwendig. In beiden Fällen werden die gleichen Profiparameter eingestellt. Die RFC-Gateways sind für jede Art der Kommunikation erforderlich, die RFC- oder CPI-C- Protokolle verwenden und müssen deshalb die neuste verfügbare RFC-Bibliothek nutzen. Als Applikationsserver-Schnittstelle zu anderen Systemen (z. B. zu anderen SAP-ERP-Systemen, zu externen Programmen) müssen angemessene Sicherheitsbedingungen geschaffen werden. Speziell für externe Programme, die über die Gateways gestartet werden, müssen die folgenden Sicherheitseinstellungen benutzt werden:

- Es ist eine sichere Verbindung zwischen Gateway und verschiedenen SAP-ERP-Systemen herzustellen. Das kann mit der Einrichtung von SNC oder der Verwendung des SAProuters zwischen den Gateways durchgeführt werden.
- Die Protokollierung des Gateways ist zu aktivieren. Das Gateway muss so konfiguriert werden, dass vom Gateway ausgeführte Aktionen und erhaltene Anfragen in die Protokolldatei aufgenommen werden, um die Sicherheitseinstellungen für ein externes Programm zu definieren.
- Jeder unberechtigte Start eines externen Programmes muss durch die Instandhaltung der Datei secinfo im Datenverzeichnis der Gatewayinstanz (gw/sec_info) verhindert werden. Eine allgemeine Freigabe mit * auf allen Nutzungsspezifikationen ist nicht erlaubt.
- Die nicht autorisierte Registrierung von Programmen muss verhindert werden, indem die Datei reginfo in das Datenverzeichnis der Gatewaysinstanz (gw/reg_info) aufgenommen wird. Eine allgemeine Freigabe mit * auf allen Nutzungsspezifikationen ist nicht erlaubt.

Für den RFC-Gateway gibt es vier verschiedene Anwendungsfälle. Jeder einzelne muss im Kontext der Sicherheit analysiert werden:

1. Anwendungsfall: Überwachung – gwmon

Die Serverapplikation gwmon kann ohne Berechtigungen remote aufgerufen werden. Die folgenden Aktionen können unter anderem ausgeführt werden:

- Anzeige von Profilparametern
- Änderung der Gatewayparameter
- Anzeige von secinfo und erneutes Lesen von reginfo (reread)
- Anzeige der Verbindungstabellen
- hartes Herunterfahren des Gatewayservers

Zur Konformität muss der Parameter gw/monitor auf 1 gesetzt werden. Der Parameter definiert, ob das Gateway lokal (=0) und/oder remote (=1) mit einem Monitor kommuniziert.

2. Anwendungsfall: RFC-Verbindung zu einem ABAP-Stack → fehlt – wird noch nachgeliefert

Dieser Anwendungsfall ist nur mit einem integrierten RFC-Gateway möglich. Funktionsbausteine werden innerhalb des AS ABAP auf diesen Weg aufgerufen und mit Hilfe des AS ABAP wird die Authentifizierung und Autorisierung durchgeführt. Die folgenden Aktionen dürfen von Clientes ausgeführt werden:

- Aufruf eines beliebigen Funktionsbausteines innerhalb der AS ABAP Berechtigungen.
- Das Berechtigungsobjekt S_RFC wird für den Funktionsaufruf benötigt. Aus diesem Grund muss dieses Berechtigungsobjekt nur dem Benutzer zugeordnet werden, der dieses benötigt und die erforderlichen Funktionsbausteine müssen im Berechtigungsobjekt gepflegt werden.

Für Remote Aufrufe wird zusätzlich das Berechtigungsobjekt S-RFC benötigt. Des Weiteren sind Berechtigungsprüfungen für Remote Aufruf die gleichen wie für interne Aufrufe.

Zur Gewährleistung einer starken Authentifizierung und Verschlüsselung zum AS ABAP und einer Ende-zu-Ende-Verschlüsselung sollte SNC verwendet werden. Der Parameter snc/permit_insecure_com definiert, ob vom RFC-Gateway Verbindungen akzeptiert werden, die nicht über SNC abgesichert sind. Ein weiterer Parameter snc/permit_insecure_start definiert, ob Programm (z.B. AS ABAP) Verbindungen ohne SNC herstellen dürfen.

3. Anwendungsfall: Starten von RFC-Serverprogrammen

Das Programm ist auf dem Server selbst ausführbar, ohne die Sicherheitsmechanismen des AS ABAP zu nutzen. Die primäre Authentisierung wird durch das RFC-Gateway selbst ausgeführt. Dazu wird die Datei secinfo, die einen ACL enthält, verwendet. Die folgenden Aktionen können vom RFC-Client ausgeführt werden:

- Starten des Serverprogramms auf dem Server

Die Datei secinfo ist mit den entsprechenden ACL für die RFC-Clients zu verwalten. Empfohlen wird Secure Network Communication (SNC) einzusetzen, um eine starke Authentisierung zum RFC-Gateway und eine Ende-zu-Ende-Verschlüsselung zu erreichen. Der Profilparameter snc/permit_insecure_com definiert, ob das RFC-Gateway Verbindungen akzeptiert, die nicht SNC geschützt sind.

4. Anwendungsfall: Registrierung von RFC-Serverprogrammen

Das externe RFC-Serverprogramm registriert sich selbst durch Benutzung der Programm-ID, ohne die Sicherheitsmechanismen des AS ABAP zu nutzen. Das RFC-Serverprogramm akzeptiert alle Aufrufe der RFC-Clients durch Nutzung des RFC-Gateways (ähnlich wie Anwendungsfall 3). Die folgenden Aktionen können vom RFC-Server ausgeführt werden:

- Ein beliebiges RFC-Serverprogramm kann sich durch Verwendung der Programm-ID registrieren.
- Ein beliebiger RFC-Client kann jedes der registrierten Serverprogramme aufrufen.
- Berechtigungen, die ACLs für ihre IP-Adressen oder Hostnamen nutzen:
- Verwalte die Datei reginfo mit angemessenen ACLs für die registrierten RFC- Serverprogramme.
- Verwalte die Datei secinfo mit angemessenen ACLs für die RFC-Clients.

Protokollierung am Gateway

Es gibt bestimmte Systemvoraussetzungen, um die Protokollierung am Gateway mit der Transaktion SMGW zu nutzen. Die Protokollierung ist für die Kernel-Releases größer 640 zu implementieren. Zur Protokollierung der Gateway-Ereignisse sollte die folgende Parametereinstellung gesetzt werden (siehe auch SAP-Hinweis 910919 – Gateway-Logging einrichten, [SECNOTE]):

- Empfohlene Einstellung des Profilparameters mit Aktionen: gw/logging: ACTION=SPXMZR

Härtung des RFC-Gateways

Für die Systemsicherheit ist es notwendig, dass die Zugriffssteuerungslisten (ACL) des Gateways erstellt und gewartet werden. Dazu sollten die folgenden Schritte durchgeführt werden.

1. Mit der Transaktion RZ11 wird der Parameter gw/reg_no_conn_info geprüft. Die SAP-Empfehlung ist, dass alle Sicherheitsbits gesetzt werden. Der Parameter sollte demnach auf 255 stehen. Falls das noch nicht umgesetzt wurde, muss DEFAULT.PFL auf Betriebssystemebene eingestellt oder mit der Transaktion RZ10 den Parameter gw/reg_no_conn_inf auf 255 gesetzt werden.
2. Der Inhalt der ACL-Dateien soll für alle Einträge geprüft werden, die als Variable ein * haben (z. B. TP=* USER=* HOST=*). Dazu die Transaktion SMGW aufrufen, Menüpunkt Springen wählen, unter Expertenfunktionen Externe Sicherheit und Anzeige ACL wählen.
3. Ist das der Fall, müssen die ACL zentral verwaltet und überwacht werden.

Zusammenfassung der Gatewayeinstellungen

Die RFC-Gateway Sicherheitsdateien secinfo, reginfo und pxyinfo müssen bearbeitet und aktiviert werden. secinfo verhindert, dass externe Programme unberechtigt gestartet werden. reginfo stellt sicher, dass sich externe Programmen am Gateway registrieren.

Der Profilparameter gw/reg_no_conn_info muss gemäß SAP-Hinweis 1444282 (siehe [SECNOTE]) – gw/reg_no_conn_info Einstellung eingespielt werden. In jedem Fall sollte der Parameter auf 255 gesetzt werden. Für den Profilparameter muss ein ungerader Wert gesetzt werden.

Der Profilparameter gw/acl_mode definiert, wie sich das Gateway verhält, falls eine ACL-Datei (gw/sec_info oder gw/reg_info) nicht existiert. Die empfohlene Standardeinstellung für den Parameter ist gw/acl_mode = 1. Externe und registrierte Server werden so nur innerhalb des Systems erlaubt.

Der Profilparameter gw/monitor definiert, ob das Gateway lokal und/oder remote mit einem Monitor kommuniziert. Die empfohlene Einstellung ist gw/monitor = 1.

APP.4.2.M9 Absicherung und Überwachung des Message-Servers

Der Message-Server wird pro SAP-ERP-System nur einmal konfiguriert. Seine Aufgaben sind:

- Zentraler Kommunikationskanal zwischen den einzelnen Applikationsservern (Instanzen) des Systems.
- Lastverteilung bei Anmeldungen über SAP GUI und RFC mit Logongruppen (Transaktion SMLG).
- Informationsstelle für den Web Dispatcher und die Applikationsserver. Jeder Applikationsserver des Systems meldet sich zuerst beim Message-Server an.

Die Sicherheitseinstellungen für den Message-Server sind über Profilparameter durchzuführen. Die empfohlenen Werte zur Einstellung der Profiparameter sind in der folgenden Tabelle aufgeführt:

Profilparameter	**Beschreibung**	**Wert**
ms/monitor	Nur der Applikationsserver darf den internen Speicher des Message-Servers ändern und die Monitorfunktion ausführen. Das externe Überwachungstool msmom hat nur noch eingeschränkten Zugriff.Wert 1 bedeutet, dass auch externe Überwachungsprogramme den internen Speicher des Message-Servers überwachen dürfen.	0Die externe Überwachung des Message-Servers wird unterbunden.
ms/acl_info	Bestimmung einer Datei mit Zugriffsberechtigungen auf die Zugriffskontrollliste (ACL) für den Message-Server.	<Dateiname>
rdisp/msserv_internal	Die Message-Server Ports müssen in interne Ports (Kommunikation mit dem Applikationsserver) und externe (Kommunikation mit Client/Server) Ports getrennt werden. Für den internen Port kann der Profiparameter rdisp/msserv_internal genutzt werden. Der Parameter bestimmt einen Port, der vom Applikationsserver zur internen Kommunikation genutzt wird. Der Wert 0 bedeutet, dass kein eigener Port für die interne Kommunikation verwendet wird.	<Interne Port Nummer>Sollte sich vom externen Message Port unterscheiden.
ms/admin_port	Der Parameter spezifiziert einen Port, der für die remote-Administration des Message-Servers genutzt werden kann. Ist der Wert auf 0 gesetzt, ist die remote-Administration deaktiviert.	0

Profilparameter	Beschreibung	Wert
icm/http_admin	Der interne Kommunikations-manager kann remote als Web-Interfacemkonfiguriert werden.	Sollte nicht verwendet werden.

Zum verbesserten Schutz des Message-Servers und zum Genehmigen von Ports müssen die folgenden Einstellungen festgelegt werden:

1 Ist es externen Überwachungsprogrammen wie dem Überwachungstool msmon erlaubt, sich mit dem Message-Server zu verbinden?
2 Wird die interne von der externen Kommunikation getrennt?
3 Werden ACL (Zugriffskontrollliste) für den Message-Server genutzt?

Überwachung des Message-Servers

Fällt der Message-Server auf dem SAP-ERP-System aus, muss dieser schnellstmöglich neu gestartet werden. Wird eine Instanz gestartet, kontaktiert der Dispatcher-Prozess den Message-Server und stellt die verfügbaren Dienste dem Message-Server vor (DIA, BTC, SPO, UPD etc.). Kann der Verbindungsaufbau zum Message-Server nicht hergestellt werden, werden diese Daten im Systemprotokoll (Syslog) eingetragen. Es gibt verschiedene Möglichkeiten, den Message-Server zu überwachen und zu testen:

- Überwachung des Message-Servers im SAP-ERP-System: Mit der Transaktion SMMS – Message-Server-Monitor können alle Einstellungen im SAP-ERP-System geprüft und geändert werden sowie Trace-Dateien erzeugt und angeschaut und Statistiken gelesen werden.
- Überwachung des Message-Servers über den Browser: Damit Details über Server und Logon-Gruppen im Web-Browser angezeigt werden, muss in der URL der Host des Message-Servers und der http-Port des Message-Servers angeben werden. Dazu muss der Profilparameter ms/server_port_<xx> gesetzt werden.
- Überwachung und Test des Message-Servers auf Betriebssystemebene: Dafür stehen die folgenden Programme zur Verfügung:
  - msmon – hat die gleichen Funktionen wie die Transaktion SMMS.
  - msprot – übermittelt einen kontinuierlichen Status über die Applikationsserver, die an den Message-Server angeschlossenen sind.

Zum Testen stehen die folgenden Programme zur Verfügung:

- Im Executable-Verzeichnis das Programm /usr/sap/<SID>/SYS/exe/run.
- igtst, zur Prüfung der Verbindung zum Message-Server und zum Anzeigen der aktiven Instanzen und Logon-Gruppen.

APP.4.2.M10 Regelmäßige Implementierung von Sicherheitskorrekturen [Fachabteilung]

SAP hat den Prozess "Product Security Response Prozess" zur Verbesserung der Produktsicherheit definiert: Sobald eine Schwachstelle identifiziert wurde, gibt das Unternehmen einen SAP-Sicherheitshinweis heraus. Die Hinweise werden typischerweise an jedem zweiten Dienstag eines Monats veröffentlicht (SAP Security Patch Day) und in dringenden Fällen auch außerhalb des Patch-Day-Zyklus.

Die Sicherheitshinweise haben verschiedene Prioritätsstufen:

- HotNews (1)
- Korrekturen mit einer hohen Priorität (2)
- Korrekturen mit einer mittleren Priorität (3)
- Korrekturen mit einer niedrigen Priorität (4)
- Empfehlungen / zusätzliche Informationen (5)

Die erste und zweite Stufe müssen zeitnah eingespielt werden, während die dritte bis fünfte Stufe auch mit dem nächsten Support-Package eingespielt werden können. Die fünfte Stufe der SAP-Hinweise beinhaltet lediglich Informationen und keine Software-Patches. Der zentrale Zugangspunkt mit den neuen Informationen zu SAP-Hinweisen ist der SAP Service Marketplace (siehe [SECNOTE]).

SAP HotNews

In dem SAP HotNews ist beschrieben, wie Probleme behoben oder verhindert werden (z. B. wie das SAP-ERP-System heruntergefahren wird oder keine Daten verlorengehen). Es sollte ein Verfahren eingerichtet werden, mit dem regelmäßig die SAP HotNews geprüft werden. Dafür sollte ein Verantwortlicher benannt werden, der die Änderungsanforderung (Change Request) erstellen darf. Diese Änderungsanforderungen werden den verantwortlichen Personen des Prozesses weitergeleitet.

SAP Security Patch Day

Der SAP Security Patch Day findet jeden zweiten Dienstag im Monat statt. Eine aktuelle Liste der Sicherheitshinweise befindet sich unter [SECNOTE]. Darüber hinaus können in der Media Library (siehe [SAP-SOS]) weiterführende Informationen zu verschiedenen Applikationen und Hinweisen nachgelesen werden, die im Folgenden kurz erläutert werden und in einem eigenen Abschnitt noch detaillierter beschrieben werden.

Mit der Applikation-Systemempfehlung (System Recommendations) wird geprüft, welche Sicherheitshinweise für die verschiedenen Systeme der SAP-Landschaft relevant sind. Dafür kann ein regelmäßiger Hintergrundjob eingeplant werden, der die Sicherheitshinweise für das System auswertet. Eine Änderungsanforderung (change request) kann direkt aus der Applikation gestartet werden.

Die Risikobewertung (Risk Assessment) gibt an, wie kritisch die Sicherheitslücke ist, aber auch wie hoch das Risiko für die produktiven Geschäftsprozesse durch das Einspielen ist. Entsprechend dieser Bewertung wird entschieden, welche Sicherheitshinweise im Rahmen eines monatlichen Patch-Zyklus angewandt werden und welche ein Teil des nächsten Wartungszyklus sind.

Die Applikation-Validierung der Konfiguration ("Configuration Validation") bietet die Möglichkeit, einen Report auszuführen, der prüft, welches System den Sicherheitsrichtlinien entspricht. Demzufolge werden alle zu installierenden Sicherheitshinweise für das Zielsystem der Validierung der Konfiguration (Configuration Validation) hinzugefügt.

Innerhalb des aktuellen Monats erfolgt die Anwendung der ausgewählten Sicherheitshinweise (Security Notes). Falls notwendig, wird ein Regressionstest durchgeführt, um sicherzustellen, dass die produktiven Geschäftsprozesse ordnungsgemäß funktionieren.

Im Rahmen des Wartungszyklus wird der Kernel aktualisiert. Das gilt für Java Patches und ABAP-Support-Packages. Dazu zählt ebenfalls, dass die Korrekturen der Sicherheitshinweise mitgeliefert werden. Ein Teil der Sicherheitshinweise beschreibt Konfigurationsänderungen, die sofort angewendet werden können. Während der Aktualisierung kann es sein, dass neue Sicherheitshinweise von neueren Patch-Days eintreffen. Diese sollten mit einbezogen werden. Am Ende der Aktualisierung ist ein vollständiger Test für alle Geschäftsprozesse durchzuführen.

SAP-Sicherheitshinweise mit der Transaktion SNOTE implementieren

Die Transaktion SNOTE wird dazu verwendet, die mit den SAP-Sicherheitshinweisen gelieferten Korrekturen einzuspielen. Es ist notwendig, alle dazugehörigen SAP-Hinweise und Beschreibungen sorgfältig zu lesen und diese nicht zu ignorieren.

SAP-Sicherheitshinweise transportieren

Das Einspielen eines SAP-Sicherheitshinweises sollte mit den dazugehörigen SAP-Sicherheitshinweisen in einem Transportauftrag angelegt werden. SAP-Sicherheitshinweise, die unabhängig voneinander sind, dürfen nicht in einen gemeinsamenTransportauftrag aufgenommen werden.

Java-Systeme

Neben Korrekturen, die über Java-Support-Packages ausgeliefert werden, sollte unbedingt beachtet werden, dass die verwendete JVM selbst ebenfalls Schwachstellen aufweisen kann und aktuell gehalten werden muss. Das gilt sowohl für die JVM von Oracle als auch die von SAP. Die regelmäßigen Updates zu den JVM enthalten oft wichtige Sicherheitskorrekturen, die mitunter nicht detailliert beschrieben sind. Daher sollten JVM-Updates auch ohne konkreten Sicherheitshinweis regelmäßig angewendet werden.

Grundsätzlich gilt, dass die SAP-Sicherheitshinweise der Priorität 1 (HotNews) und 2 (High) teilweise schwerwiegende Fehler in der Programmierung der SAP-Standardsoftware beheben und deswegen zeitnah bewertet und angewendet werden müssen. Hinweise mit geringerer Priorität können auch über Support-Packages implementiert werden. Da die ausgelieferten Korrekturen oft Abhängigkeiten zum Softwarestand haben und deswegen eine verspätete Umsetzung komplexer wird, sollte mindestens einmal im Jahr ein Support-Package eingespielt werden. SAP garantiert den Downport von Einzelkorrekturen nur für Releases und Support-Package-Stände der zurückliegenden 18 Monate.

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich APP.4.2 *SAP-ERP-System*.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "SAP-ERP-System".

APP.4.2.M11 Sichere Installation eines SAP-ERP-Systems

Bevor ein SAP-ERP-System sicher konfiguriert wird, müssen bestimmte Schritte während der Installation durchgeführt werden. Im folgenden Kapitel werden einige der wichtigsten Punkte zur sicheren Installation eines SAP-ERP-Systems (ABAP) beschrieben.

Aktuelle SAP-Sicherheitsleitfäden und SAP-Dokumentationen berücksichtigen

SAP stellt zahlreiche Dokumente und Informationen zur Verfügung. Diese sollten die Administratoren kennen und sie sollten regelmäßig prüfen, ob Aktualisierungen vorliegen. Details zu Sicherheitseinstellungen können auf dem SAP-Hinweis 2253549 - The SAP Security Baseline Template entnommen (siehe [SECNOTE]) werden. Dieser SAP-Hinweis beinhaltet Informationen und Dokumente zu den Themen:

- **SAP Security Baseline Template** [SAPSBAS]
- **SAP Secure Operations Map** [SAPSOPM]
- **SAP Security White Papers** [SAPSWP]
- **Security Optimization Services** [SAPSOS]
- **Security Guides zu SAP-Lösungen** [SAPSG]
- **SAP HANA Security Checklists and Recommendations** [SAPHSCR]

Absicherung der Betriebssysteme

Die Komponenten eines SAP-ERP-Systems werden als Programme auf einem IT-System installiert und in Form von Prozessen ausgeführt. Damit ist die Sicherheit des genutzten Betriebssystems auch wichtig für das SAP-ERP-System. Folgende Maßnahmen sind hierbei zu beachten:

- APP.4.2.M16 *Umsetzung von Sicherheitsanforderungen für das Betriebssystem Windows*
- APP.4.2.M17 *Umsetzung von Sicherheitsanforderungen für das Betriebssystems Unix*

Mithilfe geeigneter Schutzmaßnahmen sollte der Applikationsserver Betriebssystemkommandos und Dateizugriffe so selten wie möglich und immer nur kontrolliert ausführen können. Hierzu sollten entsprechende Berechtigungen gesetzt und die Dateischnittstelle geschützt werden (Transaktionen FILE und SFILE, Tabelle SPTH).

Nur benötigte Komponenten installieren

Ein SAP-ERP-System besteht potenziell aus vielen unterschiedlichen Komponenten. Ungenutzte Komponenten bergen jedoch Sicherheitsrisiken, da diese oft vergessen werden und daher ohne angepasste Konfiguration betrieben werden. Aus diesem Grund sollten nur Komponenten installiert werden, die tatsächlich benötigt werden.

Für ein SAP-ERP-System muss insbesondere entschieden werden, ob nur ein oder beide Stacks nötig sind, sofern die eingesetzte Systemversion die separate Installation noch unterstützt. Ist das nicht der Fall, muss der nicht benötigte Stack so abgesichert werden, dass dessen Funktionen nicht unberechtigt genutzt werden können.

Wahl von sicheren Passwörtern

Während der Installation müssen wichtige Authentisierungsdaten eingegeben werden. Dies sind beispielsweise Passwörter für technische Benutzer, die von den SAP-ERP-Systemkomponenten zur Authentisierung bei internen Kommunikationsverbindungen genutzt werden. Weitere Informationen sind in der Maßnahme APP.4.2.M13 *SAP-Passwortsicherheit* beschrieben.

Installationsquellen absichern

In der Regel werden SAP-ERP-Systeme nicht direkt von CD oder DVD installiert. Vielmehr wird eine Verzeichnisstruktur lokal oder im Netz genutzt, um die Daten anzubieten, die zur Installation benötigten werden. Die Daten der CD- bzw. DVD-Medien werden dann dorthin kopiert. Es wird empfohlen, die Daten nicht lokal auf dem Rechner zu halten, auf dem das SAP-ERP-System installiert wird, sondern auf einem Server. Auf die Daten kann dann über das Netz zugegriffen werden. In großen Institutionen kann dieses Verzeichnis genutzt werden, um zusätzliche SAP-ERP-Systeme zu installieren. Werden die Systeme nicht in einem separaten und abgeschirmten Netzsegment installiert, sollte der Installationsrechner vom Netz genommen werden, solange er nicht benötigt wird.

Es wird empfohlen, den Zugriff auf die Installationsquellen mit Mitteln des Betriebssystems abzusichern, sodass nur berechtigte Administratoren darauf zugreifen können. Unberechtigte Benutzer dürfen insbesondere keine schreibenden Rechte auf die Installationsquellen besitzen, damit die enthaltenen Daten nicht verändert werden können.

Werden die Installationsquellen lokal auf den Rechnern des SAP-ERP-Systems vorgehalten, sollten sie nach der Installation gelöscht werden.

SAP-Hinweise für die Installation umsetzen

Die Installationsanleitung eines SAP-ERP-Systems enthält in der Regel viele Verweise auf SAP-Hinweise, in denen wichtige Informationen für eine reibungslose Installation oder zur Problemlösung enthalten sind. Häufig verweisen die SAP-Hinweise auch wieder auf weitere SAP-Hinweise, sodass eine beträchtliche Informationsmenge zusammenkommen kann. Die Hinweise sind vor der Installation zu besorgen. Es ist aber zunächst ausreichend, die in der Installationsdokumentation angegebenen Hinweise zu lesen und einen weiteren Iterationsschritt durchzuführen. Oft wird bei Referenzen auf weitere Informationen explizit angegeben, ob diese verpflichtend abzuarbeiten sind oder nur unter bestimmten Bedingungen angewandt werden sollen.

Es wird dringend empfohlen, alle relevanten Informationen abzuarbeiten, da es sonst leicht zu Fehlern kommen kann. Fehlermeldungen dürfen nur dann ignoriert werden, wenn dies explizit durch die Installationsanleitung oder SAP-Hinweise angegeben wird. Weitere Informationen sind in der Maßnahme APP.4.2.M30 *Implementierung eines kontinuierlichen Monitorings auf die Sicherheitseinstellungen* beschrieben.

Sichere Installation und Konfiguration der Datenbank

Die SAP-Datenbank ist eine kritische Komponente, die vor unberechtigtem Zugriff geschützt werden muss. Neben den allgemeinen Aspekten einer sicheren Datenbank-Installation sind die spezifischen Empfehlungen in der Maßnahme APP.4.2.M7 *Absicherung der SAP Datenbanken* zusammengefasst. Die Sicherheit von Datenbanken wird auch im Baustein APP.4.3 *Relationale Datenbanksysteme* behandelt.

APP.4.2.M12 SAP-Berechtigungsentwicklung [Entwickler, Fachabteilung, Leiter IT]

Die klassische SAP-ERP-Systemlandschaft besteht aus drei Stufen: Entwicklung, Qualitätssicherung/Test und Produktion (D-Q-P). In SAP-ERP-Systemen werden Entwicklungen durchgeführt und Änderungen vorgenommen. Die Entwicklungen werden nach einem festgelegten Zyklus freigegeben und entsprechend ausgerollt. Berechtigungsrollen, die neu entwickelt oder geändert wurden, sollten mithilfe des SAP-Transportsystems durch die SAP-Transportstufen D-Q-P transportiert werden.

Entwicklungssysteme

Berechtigungen in Entwicklungssystemen sind grundsätzlich nicht so stark eingeschränkt wie in einem Qualitätssicherungs- und Produktivsystem. Dennoch sollten Berechtigungen in den folgenden Funktionsbereichen gewissen Einschränkungen unterliegen: Berechtigungsadministration, Benutzeradministration, Systemadministration, Customizing, Transportverwaltung und Entwicklung. Im Entwicklungssystem können neue Funktionen erstellt und geändert werden sowie weitere Rollenanpassungen vorgenommen werden. Schaltbare Berechtigungsprüfungen (SACF) werden im Entwicklungssystem aufgenommen und in den Loggingmodus oder Aktiv gesetzt und danach in die Folgesysteme transportiert.

Qualitätssicherung/Test

Die SAP-ERP-Systeme für die Qualitätssicherung sowie Tests unterliegen den gleichen Berechtigungseinschränkungen wie Produktivsysteme. Die Qualitätssicherungssysteme für Tests und Trainings simulieren eine reale Systemumgebung. Tests werden auf dem Qualitätssicherungssystem von sogenannten Key-Usern durchgeführt. Dadurch wird vermieden, dass sich Endanwender auf dem System befinden.

Produktivsysteme

Die Berechtigungsvergabe unterliegt im Produktivsystem bestimmten Einschränkungen, die in einem Berechtigungskonzept definiert werden sollten. Berechtigungen für das Replacing im Debugging (elektronisches Radieren) und die Berechtigung für das Editieren von Änderungsbelegen sollten im Produktivsystem ausschließlich Notfallbenutzer erhalten. Berechtigungen, mit denen sich Massenpflegeaktivitäten (z. B. über CATT, SAPGUI-Skripting usw.) durchführen lassen, sollten in Produktivsystemen sehr restriktiv vergeben werden. Das Notfallkonzept regelt die Ausnahmefälle kritischer Berechtigungen im Produktivsystem.

APP.4.2.M13 SAP-Passwortsicherheit

SAP liefert viele Profilparameter mit Standard-Passwort- und -Anmelderegeln aus. Es müssen jedoch nicht nur diese Standardeinstellungen geändert werden, sondern auch Passwortrichtlinien definiert, interne oder externe Vorgaben umgesetzt und Sicherheitsrichtlinien für Benutzer erstellt werden.

SAP-ABAP-Stack

Passwortregeln im SAP-ERP-System können durch Profilparameter (RZ10), Customizing-Schalter (Tabelle PRGN_CUST), pflegen verbotener Passwörter (Tabelle USR40) oder durch erstellte Sicherheitsrichtlinien (SECPOL) definiert werden.

Einstellungen der Passwortregeln über Profilparameter (Login-Parameter)

Die Login-Parameter definieren die Mindestanforderungen für Passwörter. SAP liefert eine Reihe von Standardwerten aus. Alle Standardregeln der Profilparameter für Passwort- und Anmelderegeln sind auf der SAP-Help Webseite unter [SAPLOPA] detailliert beschrieben.

Die Einstellungen der Profilparameter in der folgenden Tabelle werden empfohlen, um eine höhere Absicherung zu erreichen (die Pflege der Profilparameter erfolgt über die Transaktion RZ10):

Profilparameter	Empfohlener Wert	Standard-wert	Beschreibung
login/min_password_lng	8	6	Minimallänge des Passworts
Mindestens zwei der fünf Zeichenkategorieparameter sollten gesetzt werden:			
login/min_password_digits	1	0	minimale Anzahl von Ziffern
login/min_password_letters	1	0	minimale Anzahl von Buchstaben

Profilparameter	Empfohlener Wert	Standard-wert	Beschreibung
login/min_password_lowercase	1	0	minimale Anzahl von Kleinbuchstaben
login/min_password_uppercase	1	0	minimale Anzahl von Großbuchstaben
login/min_password_specials	1	0	minimale Anzahl von Sonderzeichen
login/password_max_idle_initial	3	0	Gültigkeit des ungenutzten Initialpasswortes
login/password_downwards_compatibility	0	1	Grad der Abwärtskompatibilität

Hinweis: Schutz vor Passwort-Attacken

Es wird empfohlen, das SAP-ERP-System vor Passwort-Attacken zu schützen, indem nach einer bestimmten Anzahl erfolgloser Anmeldeversuche die Verbindung unterbrochen wird. Die Anzahl wird durch den Profilparameter login/fails_to_session_end konfiguriert.

Generierung von Passwörtern

Werden Kennwörter neu angelegt oder zurückgesetzt, sollten die neuen Kennwörter vom SAP-ERP-System generiert und nicht manuell gesetzt werden. So wird vermieden, dass dieselben Initialpasswörter an verschiedene Benutzer ausgeliefert werden.

Customizing-Schalter für die Generierung von Passwörtern

Mithilfe der Customizing-Schalter wird die Obergrenze der Werte definiert. Die Mindestanforderungen werden durch Profilparameter gesetzt. In der folgenden Tabelle sind die korrespondieren Customizing-Schalter und Profilparameter dargestellt.

Customizing-Schalter	Profilparameter (Login-Parameter)	Empfohl-ener Wert	Beschreibung
GEN_PSW_MAX_LETTERS	login/min_password_letters	40	maximale Anzahl an Buchstaben im generierten Kennwort
GEN_PSW_MAX_DIGITS	login/min_password_digits	2	maximale Anzahl an Zahlen im generierten Kennwort
GEN_PSW_MAX_SPECIALS	login/min_password_specials	1	maximale Anzahl an Sonderzeichen im generierten Kennwort
GEN_PSW_MAX_LENGTH	login/min_password_lng	10	maximale Länge des generierten Kennworts

Ist der Wert des Customizing-Schalters nicht mit dem Wert des Profilparameters identisch, wird der Standardwert des Profilparameters gezogen. Die Pflege erfolgt über die Tabelle PRGN_CUST mit der Transaktion SM30.

Komplexitätsregeln und verbotene Passwörter

Passwörter können über Komplexitätsregeln oder mittels einer Liste verbotener Passwörter definiert werden. Die Komplexität der Passwörter lässt sich durch die folgenden Profilparameter definieren:

- login/min_password_specials
- login/min_password_uppercase
- login/min_password_lowercase

Durch die Pflege der Tabelle USR40 (Transaktion SM30/SM31) ist es möglich, bestimmte Passwörter auszuschließen. Es können ebenfalls generische Werte (mit der Wildcard *) und Platzhalter (wie ?) als Einzelwerte oder Muster verboten werden.

Definieren von Sicherheitsrichtlinien

Falls die Anforderung besteht, dass die Passwortregeln und Anmeldebestimmungen nicht für jeden Benutzer gleich sind, müssen Sicherheitsrichtlinien definiert werden (siehe dazu APP.4.2.M19 *Definition der Sicherheitsrichtlinien für Benutzer*).

Passwörter mit dem Hash-Algorithmus schützen

Passwörter in einem SAP-ERP-System werden verschlüsselt und als Hash-Wert abgelegt. Dieser Wert wird verwendet, wenn das Passwort übertragen wird. Deshalb muss der eingesetzte Hash-Algorithmus den aktuellen Sicherheitsstandards entsprechen.

Es muss zudem darauf geachtet werden, dass der neueste Hash-Algorithmus auch aktiviert wird (Codeversion). In der nachfolgenden Tabelle sind die entsprechenden Codeversionen für die einzelnen Releases mit den empfohlenen Profilparametern aufgeführt.

Release	Empfohlener Profilparameter	Codeversion
Bis 4.5	Keine bestimmten Profilparameter werden benötigt	B
4.6 – 6.40	login/password_charset = 2	E
7.00 – 7.01	login/password_downwards_compatibility = 0	F
7.02 und höher	login/password_downwards_compatibility = 0	H

Zur Sicherung des Passwortes muss die Berechtigungsgruppe von Tabellen, in denen Hash-Werte abgelegt sind, auf SPWD geändert werden. Das betrifft die Tabellen: USR02, USH02, USRPWDHISTORY, VUSR001, USH02_ARC_TMP und VUSR02_PW. Kein Benutzer darf auf die Berechtigungsgruppe SPWD über die Berechtigungsobjekte S_TABU_DIS zugreifen. Dedizierte Benutzer könnten die Berechtigung über die Tabelle USR02 durch das Berechtigungsobjekt S_TABU_NAM erhalten.

Der Report CLEANUP_PASSWORD_HASH_VALUES unterstützt dabei redundante, alte und abwärtskompatible Passwörtern zu entfernen (über die Transaktion SA38). Alte Passwort-Hashes können auch über die Tabelle USR02 (über die Transaktion SE16) in den Spalten BCODE und PASSCODE angezeigt werden.

Hinweis: Wird die zentrale Benutzerverwaltung (ZBV) eingesetzt, müssen die Basisrelease der angebundenen Systeme (Tochtersysteme) gleich oder ein Release höher sein.

Weitere Empfehlungen für die sichere Einstellung des Passwort-Hashes im ABSP-System sind in den SAP-Hinweisen "1458262 - ABAP: Empfohlene Einstellung für Kennwort-Hash-Algorithmen" und „1484692 - Lesezugriff für Tabellen können mit Kennwort-Hash-Werten geschützt werden“ [SECNOTE] beschrieben.

Hinweis: Benutzer-IDs und Passwörter werden während der Anmeldung unverschlüsselt am Client des Anwendungsservers übertragen. Deshalb müssen weitere Sicherheitsmaßnahmen ergriffen werden, z.B. verschlüsselte Kommunikation (siehe APP.4.2.M18 *Abschaltung von unsicherer Kommunikation*).

SAP-JAVA-Stack

Mit den folgenden Parametern sollten die Sicherheitsrichtlinien für Anmelde-IDs und Passwörter definiert werden.

Hinweis: Wird die ABAP-Benutzerverwaltung als Datenquelle verwendet, wird das System diese Werte in den meisten Fällen ignorieren.

UME-Parameter	Wert	Beschreibung
ume.logon.security_policy.auto_unlock_time	Default wert = 600 = deaktiviert diese Option.	Sperre eines Benutzers in Minuten nach mehrfachen fehlerhaften Loginversuchen.
ume.logon.security_policy.enforce_policy_at_logon	Default wert = FALSE	Das Passwort wird während der Anmeldung gegen die Sicherheitsliste überprüft. Falls diese nicht mehr reicht, muss der Benutzer ein neues Passwort setzen.
ume.logon.security_policy.lock_after_invalid_attempts	Default wert = 6 Mögliche Werte = 0 bis 99990 = erlaubt eine unbegrenzte Anzahl an fehlgeschlagener Anmeldeversuche.	Anzahl fehlerhafter Login-Versuche, bevor der Benutzer gesperrt wird.
ume.logon.security_policy.log_client_address	Default wert = TRUE	Die IP-Adresse des Benutzers wird mitprotokolliert.
ume.logon.security_policy.log_client_name	Default wert = FALSE	Der Benutzername wird mitprotokolliert.
ume.logon.security_policy.oldpass_in_newpass_allowed	Default wert = FALSE	Definiert, ob das neue Passwort Bestandteile des alten Passworts enthalten darf.
ume.logon.security_policy.password_alpha_numeric_required	Default wert = 1	Mindestanzahl von Buchstaben und Zahlen (Beispielsweise muss das Passwort mindestens 3 Buchstaben und 3 Zahlen enthalten, wenn der Wert = 3)
ume.logon.security_policy.password_change_allowed	Default wert = TRUE	Definiert, ob Benutzerpasswörter geändert werden können.
ume.logon.security_policy.password_expire_days	Default value = 90	Gültigkeit des Passworts in Tagen.
ume.logon.security_policy.password_history	Default value = 0	Verhindert das Benutzer alte Passwörter wiederverwenden (Größe der Passworthistorie).
ume.logon.security_policy.password_impermissible		Eine Liste, die durch Kommata getrennt ist, mit Ausdrücken und Zeichen, die nicht als Passwort verwendet werden dürfen. Variablen sind Stern (*) = eine Reihe von Zeichen (aaa*= alle Passwörter, die mit „aaa“ beginnen, werden abgelehnt) und Fragezeichen (?) = ein Einzelausdruck.
ume.logon.security_policy.password_last_change_date_default	Datum im Format = MM/DD/YYYY Default wert = 12/31/9999	Das Datum wird als Datum der letzten Änderung gezählt, wenn der Benutzer sein Passwort nie-

UME-Parameter	Wert	Beschreibung
		mals verändert hat.siehe auch: ume.logon.security_policy. password_expire_days
ume.logon.security_policy.password_max_idle_time	Default value = 0	Weitere mögliche Werte: 0 bis 2147483647; Wert = 0 deaktiviert Tage bis zur Sperrung des Passwortes seit dem letzten Login.
ume.logon.security_policy.password_max_length	Default value = 14	Maximale Passwortlänge
ume.logon.security_policy.password_min_length	Default value = 1	Minimale Passwortlänge
ume.logon.security_policy.password_mixed_case_required	Default value = 0	Minimale Anzahl von Groß- und Kleinbuchstaben in einem Passwort.
ume.logon.security_policy.password_special_char_required	Default value = 0	Minimale Anzahl an Sonderzeichen in einem Passwort.
ume.logon.security_policy.password_successful_check_date_format	Date in format MM/DD/YYYY	Default value = MM/DD/YYYYDefaultwert = 12/31/9999 Definiert das Standarddatum für die letzte erfolgreiche Anmeldung mit Benutzer-ID und Passwort, wenn ein Benutzer keine erfolgreiche Anmeldung mit Benutzer-ID und Passwort aufgezeichnet hat oder die letzte Anmeldung vor dem Standarddatum stattgefunden hat.
ume.logon.security_policy.userid_digits	Default value = 0	Wert < 0 => Zahlen sind nicht erlaubtWert = 0 => Zahlen sind erlaubtWert > 0 = > Zahlen sind erforderlich Minimale Anzahl an Zahlen in einer Benutzer-Login-ID.
ume.logon.security_policy.userid_in_password	Default value = FALSE	Definiert, ob das Passwort Teile der Benutzer-ID enthalten darf.
ume.logon.security_policy.userid_lowercase	Default value =	
ume.logon.security_policy.userid_special_char_required	Default value = 0	Wert < 0 => Sonderzeichen sind verbotenWert = 0 => Sonderzeichen sind erlaubtWert > 0 => Sonderzeichen sind erforderlich Minimale Anzahl an Sonderzeichen in einer Benutzer-Login-ID.
ume.logon.security_policy.useridmaxlength	Default value = 20	Maximale Länge der Benutzer-ID.Dieser Wert wird automatisch auf 12 gesetzt, wenn die Kombination AS Java und AS fürABAP installiert ist. Wenn eine Datenbank als Quelle für Benutzerdaten verwendet wird, muss dieser Wert kleiner bzw. gleich 200 sein.
ume.logon.security_policy.useridminlength	Default value = 5	Minimale Länge der Benutzer-ID.

APP.4.2.M14 Identifizierung kritischer SAP-Berechtigungen [Fachabteilung]

Kritische Berechtigungen sollten nur restriktiv vergeben werden und auch nur dann, wenn organisatorische und technische Sicherheitsmaßnahmen dafür definiert wurden. Mithilfe von Tools, wie SAP Access Control Emergency Access Management, können kritische Berechtigungen vergeben und überwacht werden.

Kritische Berechtigungen werden meistens Notfallbenutzern zugeordnet. Tritt ein Notfall ein, meldet sich der Benutzer mit dem Notfallbenutzer an und seine Tätigkeiten werden protokolliert.

Was sind kritische Berechtigungen?

Vereinfacht kann eine kritische Berechtigung damit beschrieben werden, dass sie auf Konfigurationen im SAP-ERP-System zugreifen kann, die sicherheitskritische Aktivitäten beinhalten. Dazu zählen die SAP-Basisberechtigungen oder auch der Zugriff auf personenbezogene Daten. SAP gibt keine generellen Anweisungen für den Umgang mit kritischen Berechtigungen vor, da jede Institution andere Sicherheitsbestimmungen und individuelle Vorgaben im Umgang mit kritischen Berechtigungen hat.

Kritische Berechtigungen identifizieren

Mithilfe eines Berechtigungsreviews oder mit Tools wie SAP Access Control Access Risk Analysis lassen sich kritische Berechtigungen in Benutzerrollen analysieren. Nachdem sie in den Rollen identifiziert wurden, müssen die Berechtigungsadministratoren diese Objekte im Detail betrachten:

- Sind diese wirklich für die Institution kritisch?
- Ist die Transaktion allein kritisch oder vor allem die Ausprägung der Werte des Berechtigungsobjektes?
- Welche Maßnahmen können durchgeführt werden?
- Kann die Institution das Risiko tragen oder müssen Kontrollen zur Minderung eingesetzt werden?

Die Liste der kritischen Berechtigungen und Kombinationen wäre insgesamt jedoch sehr lang und könnte nicht vollständig abgebildet werden. Deshalb werden allgemeine Beschreibungen für kritische Berechtigungen definiert und im Folgenden nur einige Beispiele vorgestellt.

Allgemein können die Berechtigungen der SAP-ERP-Systemadministration als kritisch eingestuft werden. Die Berechtigungsobjekte beginnen mit dem Präfix S_ wie beispielsweise:

- uneingeschränkte Tabellenpflege = S_TABU_DIS oder S_TABU_NAM mit * und ACTVT <> 3
- Entwicklungsobjekte anlegen, ändern oder löschen: S_DEVLOP mit ACTVT = 01, 02 oder 06
- Security Audit Log löschen = S_ADMI_FCD mit A_ADMI_FCD = AUDA
- Benutzer pflegen = S_USER_GRP mit ACTVT = 01, 02, 05 oder 06
- In diesem Zusammenhang gelten insbesondere die Berechtigungen zum Debugging mit Replace (S_DEVELOP|OBJ_TYPE = DEBUG; ACTVT = 02) und zur Löschung von Änderungsbelegen (S_SCD0, S_SCD0_OBJ jeweils mit ACTVT=06) als hochkritisch.

Kritische Rollen und kritische Profile

Neben den kritischen Berechtigungen gibt es auch kritische Rollen und Profile. Kritische Profile lassen sich durch die Endung _ALL identifizieren und kritische Rollen durch die Zeichenkette ADM.

Kritische Berechtigungen durch Risikoanalyse identifizieren und bewerten

Folgende Instrumente sind für eine Risikoanalyse verfügbar:

- Report RSUSR008_009_NEW: Der Report wird über die Transaktion SA38 aufgerufen oder über das Benutzerinformationssystem SUIM (Benutzer und dann mit kritischen Berechtigungen (Neue Version) wählen). Mit dem Report können Benutzer mit kritische Berechtigungen und Benutzer mit kritischen Berechtigungskombinationen analysiert werden. Es empfiehlt sich zunächst die Hauptgeschäftsprozesse und -funktionen zu definieren, damit Risiken besser zugeordnet werden können. Kritischen Berechtigungen werden unter dem Punkt kritische Berechtigungen gepflegt. Die ID der Berechtigung ist frei wählbar. Es sollte jedoch eine Namenskonvention dafür definiert werden. Nachdem die ID definiert wurde, kann unter dem Punkt Berechtigungsdaten das Berechtigungsobjekt mit den Werten erstellt werden. Danach muss noch eine Variante erstellt werden, die dann zur Risikoanalyse genutzt wird. Im Einstiegsbild des Reports kann die Risikoanalyse durchgeführt werden (Variante für kritische Kombinationen oder für kritische Berechtigungen). Es können noch weitere Kriterien gewählt werden, z. B. Benutzer, Benutzergruppe, Rollen. Der Report kann insgesamt jedoch keine ausführliche Risikoanalyse ersetzen und dient als Übersicht des SAP-ERP-Systems.
- SAP Access Control: Mit dem Tool SAP Access Control ist es möglich, SAP-spezifische Risikoanalysen auf Benutzer-, Rollen- und Profilebene durchzuführen sowie für HR-Objekte. Es kann für eine schnelle und umfassende Erstbereinigung eingesetzt werden. Auch lassen sich bestehende Zugriffs- und Berechtigungsrisiken identifizieren und elimenieren.

APP.4.2.M15 Sichere Konfiguration des SAP-Routers

Der SARouter ist ein SAP-Programm und schützt das SAP-Netz. Er ergänzt bestehende Firewall-Architektur und sollte immer zusammen mit ihm eingesetzt werden. Der SARouter sollte als Gateway für eine klassische ABAP-Verbindung benutzt werden.

Es sollten folgende Punkte berücksichtigt werden:

- Der SARouter muss die Verbindungen zu den SAP-ERP-Systemen überwachen und protokollieren.
- Es muss eine indirekte Verbindung aufgesetzt werden, falls eine direkte Verbindung aufgrund der Netzkonfiguration nicht möglich ist.
- Verbesserung der Netzsicherheit durch Umsetzung der folgenden Einstellungen:
    - SARouter Passwörter setzen
    - genehmigt Zugang nur zu bestimmten Hosts,
    - genehmigt Zugang nur zu bestimmten Dienstleistungen und Hosts,
    - akzeptiert nur SNC gesicherte Verbindungen und
    - Benutzung eines SARouters als SNC-Tunnel.

Darüber hinaus kann es erforderlich sein, die Leistung und Stabilität des lokalen Netzes zu steigern, um die Last des SAP-ERP-Systems zu kompensieren.

Es muss geprüft werden, dass die Richtlinien für den SARouter eingehalten werden. Vor allem die SAProuter Routetabelle (bestehend aus Verbindungseinträgen) und die SARouter excecutable müssen durch folgende Maßnahmen geschützt werden:

- Die Routetabelle darf nicht unberechtigt geändert werden. Hierfür bietet das Betriebssystem unterstützende Einstellungen an. Der Standardname der Routetabelle ist saprouttab.
- Der SARouter muss für spezielle Verbindungen mit einem Passwort geschützt werden.
- Das Passwort wird in der Routetabelle eingetragen und wird unverschlüsselt gespeichert. Deshalb ist es zwingend erforderlich, ein Passwort zu benutzen, das in keinem persönlichen Bezug steht.
- Verbindungen, die ein Passwort für die SARouter-Verbindung verwenden, müssen verschlüsselt werden. SNC-Einträge fangen immer mit dem Buchstaben K (wie key) an. Verbindungen, die nicht SNC verwenden, sind in dem Fall zu blockieren.
- Es dürfen keine Wildcard-Verbindungen konfiguriert sein, also Verbindungen bei denen Quelle und Ziel nur mit * spezifiziert sind.
- Sofern kein nativer TCP/IP-Zugriff gewünscht ist, sondern SAP-Kommunikation (DIAG/SAPGUI, RFC, eventuell mit SNC) eingesetzt wird, sollten Verbindungseinträge statt mit D mit S erlaubt werden.

Die ausführbare Datei des SAProuters muss geschützt werden (SAProuter auf Unix/Linux oder saprouter.exe unter Windows).

APP.4.2.M16 Umsetzung von Sicherheitsanforderungen für das Betriebssystem Windows

Die SAP-spezifischen kritischen Benutzer <sid>adm, SAPService<sid> müssen jedoch genauso sicher wie andere administrative Benutzer verwaltet werden. Zudem muss der Zugriff auf die Ressourcen und die Administrationsrechte auf die erforderlichen Benutzer beschränkt werden.

Der Benutzer SAPService<sid> führt die für das SAP-ERP-System benötigten Windowsdienste aus. Dafür sind auf dem lokalen Rechner entsprechende Berechtigungen notwendig. Allerdings sollte eine interaktive Anmeldung nicht erlaubt sein. Darüber hinaus muss der Benutzer nicht in der lokalen Windowsadministratorengruppe enthalten sein. In Bezug auf diese Berechtigungen müssen die dazugehörigen Systemressourcen des SAP-ERP-Systems geschützt werden. Das beinhaltet Dateien, Prozesse und gemeinsam genutzten Speicher zu schützen.

Windowsgruppen und -Benutzer in einer SAP-ERP-Systemumgebung

Windows unterscheidet zwischen Domaingruppen und lokalen Gruppen. In der Windowsdomain gibt es lokale, globale und allgemeine Domains. Domaingruppen sind innerhalb einer Windowsdomain gültig und nicht nur auf einem Server. Es ist notwendig, die Domainbenutzer, abhängig von ihren Aufgaben, in unterschiedlichen Aktivitätsgruppen zu bündeln. Der Domainadministrator kann die Aktivitätsgruppen auf andere Bereiche exportieren, sodass der jeweilige Benutzer auf alle Ressourcen zugreifen kann, die er benötigt, um das SAP-ERP-System zu verwalten. Der Name der globalen Standarddomaingruppe für SAP-ERP-Systemadministratoren ist definiert als SAP_<SID>_GlobalAdmin.

Lokale Benutzergruppen sowie lokale Benutzer existieren auf einem Server nur lokal. Während der Installation eines SAP-ERP-Systems werden die Benutzerrechte an lokale Benutzer zugewiesen. Zum Beispiel erhält der Benutzer <sid>adm die Benutzerberechtigung, sich direkt als Dienst anzumelden. Allerdings sollten für eine einfachere Benutzeradministration und für eine bessere Ressourcennutzung des Servers die Benutzerberechtigungen zu lokalen Gruppen zugeordnet werden. Danach werden diese den entsprechenden Domainbenutzern und Domaingruppen der lokalen Gruppe zugewiesen.

Hinweis: Wenn lokale Benutzergruppen oder ein einzelner lokaler Benutzer auf einem Domaincontroller definiert wurden, ist die Gruppe oder der Benutzer auf allen Domaincontrollern innerhalb der Domain bekannt. Deshalb muss es vermieden werden, SAP-ERP-Systeme auf Domaincontrollern zu installieren.

Die folgenden drei Beziehungen können zwischen dem Benutzer, der lokalen Gruppe und der Domaingruppe bestehen:

- Ein lokaler Benutzer kann nur ein Mitglied einer lokalen Gruppe sein.
- Ein Domainbenutzer kann Mitglied einer lokalen Gruppe und einer Domaingruppe sein.
- Eine Domaingruppe kann in eine lokale Gruppe eingeschlossen werden. Es können auch Domaingruppen zu anderen Windowsdomains exportiert werden.

SAP-ERP-Systeme in einem Windowsdomainkonzept

Es sollten zwei getrennte Domains erstellt werden: Eine Domain für die Institution und eine für das SAP-ERP-System. Zwischen den beiden Domains sollte eine vertrauensvolle Beziehung (trusted relationship) eingerichtet werden, damit ein Single-Sign-On (SSO) möglich ist. In der Institutionsdomain sind die Domainbenutzer (einschließlich der SAP-ERP-Systembenutzer) und die Domainadministratoren einzurichten. In der SAP-Domain sind die SAP-ERP-Systemserver, Dienste und Administratoren einzurichten, einschließlich:

- SAP-ERP-Systemapplikation und Datenbankserver,
- SAP-ERP-System und Datenbankdienste,
- SAP-ERP-Systemadministratoren,
- Windowsadministratoren sowie
- SAP-Domainadministratoren.

Es wird empfohlen, auch separate Domains für die Institutionsdaten und das SAP-ERP-System zu etablieren. Des Weiteren sollte das vertrauenswürdige Windowsdomainkonzept für bestimmte SAP-spezifische Funktionen und spezielle Windowsdienste verwendet werden, die für eine vertrauenswürdige Beziehung zwischen den Domains nötig sind.

Sicherung der relevanten Daten in einem SAP-ERP-System

Unabhängig davon, ob das SAP-ERP-System zentral installiert ist oder als verteiltes System besteht, sollte eine Domain eingerichtet werden, die die SAP-ERP-System-Applikation und den Datenbankserver enthält. Der SAP-ERP-System-Server sollte in einer Windowsdomain installiert werden. Für kurzfristige Testinstallationen oder Demonstrationszwecke könnte das zentrale SAP-ERP-System installiert werden, das sich nicht in einer Windowsdomain befindet. Das ist jedoch nur für ein begrenztes Szenario zu empfehlen. Es ist schwierig, ein Domainkonzept auf einem System einzuführen, das bereits genutzt wird. In der zentralen Installation auf dem Server in einer Domain sind alle SAP-ERP-Systemadministratoren Mitglieder der lokalen Gruppe SAP_<SAPSID>_LocalAdmin. Bei einer verteilten Installation mit mehreren Servern in der Domain ist die globale Gruppe für das SAP-ERP-System einzurichten (SAP_<SAPSID>_GlobalAdmin). Diese Gruppe ist Mitglied der lokalen Gruppen des Servers und beinhaltet die SAP-ERP-Systemadministratoren. Das vereinfacht die Administration der Client- oder Serverumgebung, da neue Benutzer, die SAP-ERP-Systemadministrationsrechte benötigen, nur Mitglieder der lokalen Gruppe werden.

APP.4.2.M17 Umsetzung von Sicherheitsanforderungen für das Betriebssystem Unix

Es sollten Sicherheitsmaßnahmen realisiert werden, wenn die folgenden Objekte, Dateien oder Services genutzt werden:

- **SUID/SGID-Programme:** Es sollten nur die SENDMAIL-Versionen genutzt werden, in dem bekannte Fehler korrigiert wurden (oder ähnliche SUID-Programme).
- **Passwortdatei (passwd):** Es ist nur eine Shadow-Passwortdatei zu verwenden, die nur dem Benutzer Root-Zugriff auf die Passwortinformationen genehmigt.
- **Network Information System (NIS)**: Es sollten sichere Alternativen wie LDAP (mit SSL/TLS) oder Kerberos genutzt werden.
- **Network File System (NFS):** Es bestehen Sicherheitsrisiken, wenn dieser Service verwendet wird. Es sollten daher keine Verzeichnisse exportiert werden, die SAP-Daten zu beliebigen Empfängern enthalten und NFS nutzen. Es sollte nur zu bekannten und vertrauenswürdigen Systemen exportiert werden. Schreibberechtigungen müssen für NFS-Pfade sehr sorgfältig zugewiesen werden und es sollte vermieden werden, dass die Home-Verzeichnisse der Benutzer über NFS verteilt werden.

Insgesamt müssen folgende Punkte berücksichtigt werden:

- Alle nicht genutzten Dienste müssen deaktiviert werden.
- Es sollte keine direkte Anmeldung mit der Administrator-UserID root erlaubt sein. Alle Benutzeranmeldungen sollten personalisiert erfolgen. Tätigkeiten mit root-Rechten sollten über sudo entsprechend protokolliert werden.
- Es dürfen keine Verzeichnisse, die SAP-Daten an beliebige Empfänger mit NFS enthalten, exportiert werden. Der Transport sollte nur an vertrauenswürdige Systeme erfolgen.
- Schutz der folgenden Benutzer: root, <sid>adm und <db><sid>. Diese Benutzer sollten die einzigen Benutzer sein, die auf dem Applikationsserver und auf der Hauptinstanz existieren. Nach der Installation ist der Benutzer <db><sid> auf dem Applikationsserver zu sperren.
- Für kritische Benutzer ist die .rhosts-Datei zu leeren und die Berechtigung 000 zuzuweisen.
- Entweder ist die Datei /etc/hosts.equiv zu löschen oder es ist sicherzustellen, dass sie leer ist.
- Das Betriebssystem muss mit den entsprechenden sicherheitsrelevanten Patches auf dem aktuellen Stand gehalten werden.

Unter Unix/Linux müssen die Zugriffsberechtigungen für SAP-ERP-Systemverzeichnisse festgelegt werden. Es wird empfohlen, die Datei- und Verzeichniszugriffsrechte entsprechend der folgenden Tabelle zu setzen:

SAP-Verzeichnis oder Dateien	Zugriffsrechte in Oktalform	Eigentümer	Gruppe
/<sapmnt>/<SAP-SID>/exe	755	<sapsid>adm	sapsys
/<sapmnt>/<SAP-SID>/exe/saposcol	755	root	sapsys
/<sapmnt>/<SAP-SID>/global	700	<sapsid>adm	sapsys
/<sapmnt>/<SAP-SID>/profile	755		
/usr/sap/<SAPSID>	751		
/usr/sap/<SAPSID>/<instance ID>	755		
/usr/sap/<SAPSID>	750	<sapsid>adm	sapsys
/usr/sap/<SAPSID>/<instance ID>/sec	700	<sapsid>adm	sapsys
/usr/sap/<SAPSID>/SYS	755	<sapsid>adm	sapsys
/usr/sap/<SAP-SID>/SYS/*	755	<sapsid>adm	sapsys
/usr/sap/trans	775	<sapsid>adm	sapsys
/usr/sap/trans/*	770	<sapsid>adm	sapsys
/usr/sap/trans/.sapconf	775	<sapsid>adm	sapsys
<home directory of <sapsid>adm>	700	<sapsid>adm	sapsys
<home directory of <sapsid>adm>/*	700	<sapsid>adm	sapsys

APP.4.2.M18 Abschaltung von unsicherer Kommunikation

Jede Information, die als vertraulich klassifiziert ist, sollte verschlüsselt übertragen werden. Hierzu zählen beispielsweise Passwörter, die grundsätzlich nie unverschlüsselt übertragen werden dürfen. Die sichere Datenübertragung erfolgt über eine verschlüsselte Kommunikation, z. B. über aktuelle Implementierungen von SSL/TLS oder SNC.

Secure Network Communication (SNC)

SNC schützt die Datenkommunikationspfade zwischen verschiedenen Clients- und Serverkomponenten des SAP-ERP-Systems, die das SAP-Protokoll RFC oder DIAG verwenden. SNC bietet durch eine Ende-zu-Ende-Verschlüsselung Sicherheit auf der Anwendungsebene. Die gesamte Kommunikation zwischen zwei mit SNC geschützten Komponenten wird gesichert, z. B. zwischen dem SAP GUI for Windows und dem Anwendungsserver. SNC bietet drei Schutzstufen an:

- Authentisierung (geringer Schutz): Das System verifiziert die Identität der Kommunikationspartner
- Integrität (mittlerer Schutz): Das System bemerkt, wenn Daten geändert oder manipuliert wurden.
- Vertraulichkeit (hoher Schutz): Die übertragenen Daten werden vom System verschlüsselt.

Das Sicherheitsprodukt von SNC ist die SAP Cryptographic Library, die SNC-Verbindungen zwischen Systemkomponenten (RFC-Verbindungen) schützt.

Secure-Sockets-Layer (SSL)

Mit SSL erfolgt die Absicherung der HTTP-Verbindungen zum und vom AS ABAP. Die Daten zwischen den beiden Partnern (Client und Server) werden verschlüsselt übertragen und sie können sich gegenseitig authentisieren. Die SSL-Informationen werden über diese Funktionen gepflegt:

- Profilparameterpflege (Transaktion RZ10)
- Trust-Manager (Transaktion STRUST)
- Pflege der RFC-Destinationen (Transaktion SM59)
- ICM Monitor (Transaktion SMICM)

Das SSL-Protokoll verwendet das Public-Key-Verfahren. Daher muss der Server ein Public-Key-Schlüsselpaar sowie ein entsprechendes Public-Key-Zertifikat besitzen. Ein Schlüsselpaar und ein Zertifikat benötigt er, um sich als Serverkomponente auszuweisen. Das weitere Schlüsselpaar und Zertifikat wird gebraucht, um sich gegebenenfalls als Client-Komponente auszuweisen. Diese Schlüsselpaare und Zertifikate sind in den eigenen persönlichen Sicherheitsumgebungen (Personal Security Environments; PSEs) des Servers abgelegt, in der SSL-Server-PSE bzw. der SSL-Client-PSE.

Transport Layer Security (TLS)

TLS sichert die Transportschicht von Verbindungen zwischen den SAP-NetWeaver-Systemkomponenten ab. Mithilfe von TLS wird die Datenübertragung verschlüsselt und die Kommunikationspartner können sich gegenseitig authentisieren. Bei Verbindungen, die Internetprotokolle wie HTTP verwenden, wird das SSL-Protokoll benutzt. Bei SAP-Protokollen wie RFC oder Dialog wird SNC eingesetzt. TLS bietet drei Schutzstufen an:

- Authentisierung: Die Kommunikationspartner können authentisiert werden. Bei SSL können die Verbindungen so eingerichtet werden, dass nur die Serverkomponente der Verbindung authentisiert wird oder dass beide Partner authentisiert werden. Bei SNC werden immer beide Partner authentisiert
- Datenintegrität: Die zwischen dem Client und dem Server übertragenen Daten sind geschützt, sodass jede Manipulation der Daten aufgedeckt wird.
- Vertraulichkeit der Daten: Die zwischen dem Client und dem Server übertragenen Daten sind auch verschlüsselt, wodurch der Schutz der Vertraulichkeit erreicht wird.

APP.4.2.M19 Definition der Sicherheitsrichtlinien für Benutzer

Für unterschiedliche Benutzer können spezifische Sicherheitsrichtlinien für Passworte und Anmelderestriktionen eingestellt werden. Zum Beispiel sind für technische Benutzer im Gegensatz zu Dialogbenutzern abwärtskompatible Passwörter erforderlich und Benutzer mit kritischen Berechtigungen müssen durch starke Passwortregeln höher abgesichert werden. Die Zuordnung der Sicherheitsrichtlinien kann benutzer- und mandantenspezifisch erfolgen.

Die Sicherheitsrichtlinien lösen die Steuerung der Passwortregeln, Passwortänderungen und Anmelderestriktionen durch Profilparameter ab. Wird einem Benutzer keine Sicherheitsrichtlinie explizit zugeordnet, gelten für ihn die Richtlinien nach den gesetzten Profilparametern. Jedoch können auch nicht alle Profilparameter als Sicherheitsrichtlinie abgebildet werden.

Die Sicherheitsrichtlinien können mit SAP NetWeaver 7.31 umgesetzt werden. Weitere Informationen dazu finden sich im SAP-Hinweis 2018918 – Benutzerspezifische Einstellungen zu Kennwortregeln, Kennwortänderungen und Anmelderestriktionen (siehe [SECNOTE]).

Sicherheitsrichtlinien definieren

Sicherheitsrichtlinienattribute und die zugehörigen Vorschlagswerte sind in den Sicherheitsrichtlinien definiert und können wie folgt angepasst werden.

Vorgehen über SECPOL:

- Transaktion SECPOL ausführen.
- Bearbeitungsmodus aktivieren und neue Einträge wählen.
- Im Feld Sicherheitsrichtlinie einen Namen definieren und im Feld Kurztext eine Beschreibung eintragen.
- Für die neue Sicherheitsrichtlinie müssen Attribute definiert werden: Neue Einträge wählen.
- In der Tabelle werden die Richtlinienattribute und Attributwerte gepflegt.
  - Button Effektiv: Alle tatsächlich aktiven Attribute werden angezeigt.
  - Button Verzichtbare Einträge: Anzeige der Attributwerte, die sich nicht von den globalen Einträgen unterscheiden.
- Eine Übersicht der Sicherheitsrichtlinienattribute für die Steuerung der Kennwortregeln, Kennwortänderungen und Anmelderestriktionen findet sich im SAP Help Portal [SAPSECPO].

Sicherheitsrichtlinien Benutzern zuordnen

Die Zuordnung der definierten Sicherheitsrichtlinien zu Benutzern erfolgt über die Benutzerpflege (SU01) oder die Massenbenutzerpflege (SU10).

Vorgehen über die SU01:

- Transaktion SU01 ausführen.
- Ausgewählten Benutzer im Änderungsmodus öffnen.
- Registerkarte Logondaten auswählen.
- Im Feld Sich.-Richtlinie eine definierte Sicherheitsrichtlinie für den Benutzer auswählen.
- Eingaben sichern.

Vorgehen über die SU10:

- Transaktion SU10 ausführen.
- Alle Benutzer in der Spalte Benutzer eintragen.
- (Alle) Benutzer ändern wählen.
- Im Feld Sich.-Richtlinie eine definierte Sicherheitsrichtlinie für alle Benutzer auswählen.
- Eingabe sichern.

Verwendungsnachweis von Sicherheitsrichtlinien

Mit dem Report RSUSR_SECPOL_USAGE (über SA38) werden die Benutzer und ihre zugeordneten Sicherheitsrichtlinien dargestellt. Der Report lässt sich ebenfalls über das Benutzerinformationssystem (SUIM) öffnen. Hier muss die Struktur unter Benutzerinformationssystem bis Benutzer nach komplexen Selektionskriterien geöffnet werden. Weitere Informationen dazu finden sich im SAP-Hinweis 1611173 – SUIM| Auswertung von Sicherheitsrichtlinien für Benutzer (siehe [SECNOTE]).

APP.4.2.M20 Sichere SAP-GUI-Einstellungen

Folgenden Maßnahmen müssen eingestellt werden, um die Sicherheit der SAP-GUI-Nutzung zu erhöhen:

- Es ist immer die neueste verfügbare SAP-GUI-Version auf allen Endbenutzer-Arbeitsstationen einzusetzen.
- Die SAP-GUI-Sicherheitseinstellungen sind als customized und Standardaktionen als ask einzustellen.

Es wird empfohlen, die dazugehörigen Administratorregeln beizubehalten und zu verteilen. So ist es möglich, homogene Sicherheitseinstellungen auf allen Arbeitsstationen zu erreichen und den Benutzer von unnötigen Pop-ups zu befreien. Des Weiteren sollten die folgenden Einstellungen umgesetzt und implementiert werden:

- kein Zugriff auf die Registry
- eingeschränkte Konfigurationsoptionen der lokalen SAP-GUI-Installation wie über diese SAP-Hinweise (siehe [SECNOTE]):
  - SAP-Hinweis 762661 - SAP Logon: Registerkarten/Bearb.funktion anzeigen/ausblenden
  - SAP-Hinweis 867260 - Scripting: Plattenzugriff über Registry-Schlüssel deaktiv.
  - SAP-Hinweis 1669256 - SAP GUI 7.30: Registry-Werte und Optionsdialog schreibgeschützt

APP.4.2.M21 Konfiguration des Security Audit Logs

Mit der Transaktion SM19 (Security-Audit: Audit-Profil verwalten) werden die Filter des Security Audit Logs (SAL) konfiguriert. Für jeden Filter lässt sich definieren, ob Mandanten und Benutzer aufgezeichnet werden (abhängig von der Kategorisierung und Auditklasse). Die Ergebnisse können nach den drei Kategorien unkritisch, schwerwiegend und kritisch eingestuft werden. Diese müssen den Auditklassen Dialoganmeldung, RFC-/CPIC-Anmeldung, RFC-Funktionsaufruf, Transaktionsstart, Reportstart, Benutzerstammänderung, System und sonstige Ereignisse zugeordnet werden.

Das Security Audit Log kann als statische oder dynamische Konfiguration eingestellt werden. Bei der statischen Konfiguration werden die Filtereinstellungen persistent in der Datenbank gespeichert und bei jedem Systemstart verwendet. Bei der dynamischen Konfiguration können dagegen die Filtereinstellungen im laufenden Betrieb geändert werden. Allerdings ist die Anzahl der vorhandenen Filter nicht änderbar. Die Einstellungen sind bei dieser Konfiguration nur bis zum nächsten Systemstart aktiv.

Damit die Ereignisse im System protokolliert werden, muss zusätzlich der Profilparameter für das Security Audit Log aktiviert werden (Transaktion RZ11). Das Security Audit Log wird durch die folgenden drei Einstellungen aktiviert:

- **rsau/enable = 1**Dieser Parameter bestimmt, ob das Log eingeschaltet ist oder nicht (1 = eingeschaltet, 0 = ausgeschaltet (Standardwert)).
- **rsau/selection_slots = 10**Dieser Parameter zeigt die Anzahl der Filter, die in der Transaktion SM19 konfiguriert und dann geprüft werden.
- **rsau/user_selection = 1**Dieser Parameter bestimmt, ob eine generische Selektion von Benutzern möglich ist (0 = generische Selektion ist nicht möglich, 1 = generische Selektion ist möglich (z. B. SAP_*))

Die folgende Tabelle zeigt weitere Profilparameter, die zu setzen sind:

Profilparameter	Standardwert	Empfohlener Wert	Beschreibung
DIR_AUDIT			Verzeichnis, in dem die SAL-Dateien angelegt werden
FN_AUDIT			definiert den Namen der SAL-Dateien
Rsau/ip_only	0 = Terminal-Name wird protokolliert	1 = IP-Adresse wird protokolliert	Protokollierung des Terminal-Namens oder der IP-Adresse
rsau/max_diskspace/local		2 GB	maximale Größe der SAL-Dateien, Wertebereich von 100 MB bis 2 GB
rsau/max_diskspace/per_file		2 GB	maximale Größe der SAL-Dateien. Ist die maximale Größe der Datei erreicht, wird eine neue erstellt. Wertebereich von 1 GB bis 2 GB

Profilparameter	Standardwert	Empfohlener Wert	Beschreibung
rsaus/max_diskspace/ per_day		1.024 GB	Bestimmt maximalen Speicherplatz für alle SAL-Dateien. Der Wert des Parameters rsaus/max_diskspace/ per_file muss größer als sein. Wertebereich von 3* bis 1.024 GB

Mindestens eine der folgenden Protokollierungen sollte definiert und aktiviert werden:

- Die Protokollierung aller Ereignisse für kritische Benutzer wie SAP* (Verwendung des Filters SAP#*), Notfallbenutzer (wie FF*) oder Supportbenutzer (wie SAPSUPPORT*).
- Die Protokollierung aller kritischen Ereignisse für Benutzer.

Hinweis: Das Security Audit Log wurde in den letzten Jahren erweitert. Im Folgenden wird ein Auszug der neuen Funktionen mittels SAP-Hinweise vorgestellt (siehe [SECNOTE]):

- 1411741 - Auswertung von Debuggingereignissen im Audit Log
- 1465495 - ABAP Debugger: Sicherheitsprüf.prot. für Debugger-Aktivität. 1465495 - ABAP Debugger: Sicherheitsprüf.prot. für Debugger-Aktivität
- 1539105 - Protokollierung generischer Tabellenzugriffe per RFC
- 1810913 - Performanceverbesserung beim Auslesen des Security Audit Log
- 1963882 - SAL|Probleme bei der Auswertung von AuditLog-Dateien
- 1941568 - SAL|FAQ für Nutzung kundenindividueller Ereignisse
- 1819317 - Erweiterung des Security Audit Log
- 539404 - FAQ: Antworten auf Fragen zum Security Auditlog

APP.4.2.M22 Schutz des Spools im SAP-ERP-System [Entwickler]

Der Spool-Administrator ermöglicht einen reibungslosen Betrieb der SAP-Ausgabe-Landschaft. Zu den Aufgaben des Spool-Administrators gehören:

- administrieren von Ausgabegeräten,
- definieren einer ausfallsicheren Spool-Server-Landschaft,
- überwachen des korrekten Ausgabebetriebes.

Die Spool-Administration der Ausgabegeräte erfolgt mit der Transaktion SPAD. Schützenswerte Spool-Einträge sind zum Beispiel Einträge aus dem Bereich Finanzwesen.

Vergabe von Spool-Berechtigungen

Will ein Benutzer im SAP-ERP-System etwas ausdrucken, braucht er dazu die entsprechenden Berechtigungen. Diese werden über das Berechtigungsobjekt S_SPO_DEV gesteuert. Wird S_SPO_DEV mit den Gesamtberechtigungen (*) erteilt, hat der Benutzer Zugriff auf alle Drucker im SAP-ERP-System. Weitere Einstellungen von Spool-Berechtigungen erfolgen über die Aktivitäten und Wertezuweisungen der Berechtigungsobjekte S_ADMI_FCF und S_SPO_ACT. Auszuführende Aktionen werden mit dem Berechtigungsfeld SPOACTION festgelegt. Das Berechtigungsfeld SPOAUTH ordnet die Spool-Einträge zu. Eine Übersicht über benutzereigenen Spool-Aufträge kann jeder Benutzer mit der Transaktion SP02 aufrufen.

Es ist zu vermeiden, dass Benutzer dazu berechtigt sind, (geschützte) Spool-Aufträge von anderen Benutzern aufzurufen (Transaktion SP01 oder SP01O). Die folgenden Beispiele für Spool-Berechtigungen sollten im Regelbetrieb nur dem Spool-Administrator zugeordnet werden.

Berechtigungen zur Änderung des Inhabers einer Spool-Anfrage:

- Berechtigungsobjekt 1: S_TCODE mit TCD = SP01
- Berechtigungsobjekt 2: S_ADMI_FCD mit S_ADMI_FCD = SP01 or SP0R
- Berechtigungsobjekt 3: S_SPO_ACT mit SPOACTION = USER

Berechtigungen zum Umleiten des Druckauftrages zu einem anderen Drucker:

- Berechtigungsobjekt 1: S_TCODE mit TCD = SP01
- Berechtigungsobjekt 2: S_ADMI_FCD mit S_ADMI_FCD = SP01or SP0R
- Berechtigungsobjekt 3: S_SPO_ACT mit SPOACTION = REDI

Berechtigungen zum Exportieren eines Druckauftrages:

- Berechtigungsobjekt 1: S_TCODE mit TCD = SP01
- Berechtigungsobjekt 2: S_ADMI_FCD mit S_ADMI_FCD = SP01oder SP0R
- Berechtigungsobjekt 3: S_SPO_ACT mit SPOACTION = DOWN

Schritte zur benutzerübergreifenden Vergabe von Spool-Berechtigungen

Für den Fall, dass Benutzer in Spool-Aufträgen auf andere Benutzer zugreifen sollen, müssen bestimmte Einstellungen in der SP01 durch den Spool-Administrator durchgeführt werden. Voraussetzung dafür ist, dass dem Benutzer, der die Spoolaufträge eines anderen Benutzers bearbeiten soll, drei Berechtigungsobjekte mit der entsprechenden Ausprägung zugewiesen werden:

1. Das Berechtigungsobjekt S_ADMI_FCD mit dem Wert SPOR (= Benutzerübergreifende Verwaltung von Spool-Aufträgen).
2. Das Berechtigungsobjekt S_SPO_ACT für die Aktion mit BASE mit dem entsprechenden Wert, z. B. Name des anderen Benutzers.
3. Das Berechtigungsobjekt S_SPO_ACT mit der Ausprägung, die der Benutzer erhalten soll: DISP (Anzeigen des Inhaltes), DELE (Löschen des Spoolauftrages), PRNT (einmaliges Drucken eines bisher nicht gedruckten Auftrages), PEPR (Nachdrucken eines Auftrages)

Der Benutzer kann somit alle Druckaufträge des anderen Benutzers bearbeiten. Der andere Benutzer kann die Druckaufträge jedoch schützen, indem das Feld Berechtigung in der SP01 mit dem Wert GEHEIM gepflegt wird. Das geht nicht, wenn der andere Benutzer über die Berechtigung GEHEIM verfügt.

Schutz des TemSe-Inhaltes

Die Datenablage TemSe wird vom SAP-Spoolsystem genutzt, um Datenausgaben und Zwischenergebnisse von Hintergrundjobs zwischenzuspeichern. Die folgenden Berechtigungen sollten geprüft und entsprechend zugewiesen werden, damit unbefugte Benutzer nicht zu viele Berechtigungen haben.

Berechtigungen zur Anzeige von TemSe-Inhalten:

- Berechtigungsobjekt 1: S_TCODE mit TCD = SP11 oder TCD = SP12
- Berechtigungsobjekt 2: S_TMS_ACT mit STMSACTION = REA und (STMSOWNER = GRP oder OCL) und STMSOBJECT = SPOOL*

Das Druckerkonzept sollte durch eine Namenskonvention vereinheitlich werden.

APP.4.2.M23 Schutz der SAP-Hintergrundverarbeitung [Entwickler]

Für die Verwaltung der Batch-Jobs (Hintergrundjobs) ist der Batch-Job-Administrator verantwortlich. Hintergrundjobs können über die Transaktionen SM36, SA38 und über weitere Anwendungstransaktionen eingeplant werden. Batch-Jobs können nach folgenden Kriterien eingeteilt werden:

- Art des Jobs (technisch, funktional),
- periodische Nutzung (stündlich, täglich, wöchentlich, monatlich),
- sporadische Nutzung (ja/nein),
- Kurzbeschreibung des Jobs,
- Zuordnung zu Rolle, Benutzer oder Position.

Benutzer benötigen keine speziellen Berechtigungen, um ihre eigenen Hintergrundjobs anlegen oder ändern zu können. Die Freigabe von eigenen oder anderen Hintergrundjobs wird über ein spezielles Berechtigungsobjekt (S_BTCH_JOB) geschützt. Der generelle Zugriff auf Hintergrundjobs von anderen Benutzern benötigt ebenfalls spezielle Berechtigungen. Die drei wichtigsten Berechtigungsobjekte für Hintergrundjobs sind:

- **S_BTCH_JOB**Steuerung der Zugriffsrechte von Hintergrundjobs für den eigenen und für andere Benutzer. Alle kritischen Operationen für die Verwaltung der Hintergrundverarbeitung werden über dieses Objekt geprüft. Mit dem Objekt können keine Hintergrundjobs eingeplant werden. Spezielle Berechtigungen:
  - Freigabe von eigenen Hintergrundjobs oder von anderen Benutzern:
    Berechtigung: S_BTCH_JOB mit JOBACTION = RELE
  - Ändern der Hintergrundjobs von anderen Benutzern:
    Berechtigung: S_BTCH_JOB mit JOBACTION = MODI
  - Löschen der Hintergrundjobs von anderen Benutzern:
    Berechtigung: S_BTCH_JOB mit JOBACTION = DELE
  - Anzeigen der Hintergrundjobdefinitionen von anderen Benutzern:
    Berechtigung: S_BTCH_JOB mit JOBACTION = SHOW
- **S_BTCH_NAM**Das Berechtigungsobjekt berechtigt dazu, einen Hintergrundjob im Namen eines anderen Benutzers zu vergeben. Diese Benutzer müssen in den Berechtigungen (Feld BTCUNAME) eingetragen werden. Batch-Administratoren können somit die Hintergrundjobs unter einem technischen Benutzer laufen lassen. Spezielle Berechtigung:
  - Job-Steps unter einem anderen Benutzer einplanen:
    Berechtigung: S_BTCH_ADM mit BTCUNAME = <Benutzererkennung>
- **S_BTCH__ADM**Umfassende Berechtigungen für den Batch-Job-Administrator. Das ermöglicht unter anderem die systemweite Übersicht aller Hintergrundjobs, das Durchführen aller Funktionen für Hintergrundjobs und den Zugriff auf Hintergrundjobs in allen Mandanten. Spezielle Berechtigung:
  - Administratorberechtigung: S_BTCH_ADM mit BTCADMIN = Y

Einplanen von Hintergrundjobs

Alle Schritte für zeitgesteuerte wiederkehrende Hintergrundjobs sind an Hintergrundbenutzer zu binden. Hintergrundjobs sollten durch Systembenutzer (Typ System) nach ihren Funktionsbereichen eingeplant werden. Die verwendete Benutzer-ID wird als Benutzertyp SYSTEM angelegt. Hintergrundbenutzer sind durch die Namenskonvention von anderen Benutzern zu unterscheiden.

Der Benutzer, der Jobs für einen Systembenutzer einplant, muss diese Berechtigungen erhalten: Berechtigungsobjekt S_BTCH_NAM und im Feld BTCUNNAME = Name des auszuführenden Benutzers (z. B. Systembenutzers). Ein Risiko für kontinuierlichen und störungsfreien Betrieb besteht, wenn Hintergrundbenutzer versehentlich gesperrt werden oder die Kennwörter ablaufen.

Empfehlungen:

- Die Berechtigungsobjekte S_BATCH_ADM und S_BATCH_JOB mit dem Wert RELE sollten beim Endbenutzer nicht mehr berechtigt werden.
- Batch-Administratoren sind berechtigungstechnisch auf die entsprechenden Systemuser einzuschränken. Das geschieht über das oben beschriebene Berechtigungsobjekt S_BATCH_NAM, in das der Batch-Benutzername hinterlegt werden kann.

- Technische Benutzer sollten nicht das SAP-Profil SAP_ALL zugewiesen bekommen.
- Eine Anzeigeberechtigung für die Transaktion SM37 "Übersicht über Hintergrundjobs" ohne Jobfreigabe ist bei den entsprechenden Benutzern als nicht kritisch anzusehen.

APP.4.2.M24 Aktivierung und Absicherung des Internet Communication Frameworks (ICF)

Mit dem Internet Communication Framework (ICF) ist es möglich, von einem SAP-ERP-System über http, https und SMTP-Anfragen mit anderen Systemen zu kommunizieren. Auf die webbasierten Anwendungen eines ABAP-System kann vom Webbrowser aus zugegriffen werden. Dieser Inhalt wird durch die Dienste des ICFs gepflegt und kann über die Transaktion SICF verwaltet werden. Die Dienste sind in einer dateisystemähnlichen Baumstruktur hierarchisch angeordnet.

Um unautorisierte Zugriffe zu vermeiden, müssen die folgenden Einstellungen für ICF-Dienste umgesetzt werden:

- Es sind nur die ICF-Dienste zu aktivieren, die für die Geschäftsprozesse wirklich notwendig sind. Vor allem auf produktiven SAP-ERP-Systemen sollten nicht alle ICF-Dienste aktiviert werden.
- Alle ICF-Dienste müssen überprüft werden, für die keine Benutzerauthentisierung erforderlich ist. Einschließlich der ICF-Dienste /sap/public mit gespeicherten Anmeldedaten.

In der folgenden Tabelle sind alle ICF-Dienste aufgeführt, die zu deaktivieren sind. Falls diese im aktuellen Release vorhanden sind und nicht für einen Geschäftsprozess verwendet werden:

ICF-Dienst	**SAP-Hinweis (siehe [SECNOTE])**
/sap/bc/soap/rfc	1394100 - Sicherheitshinweis:Zugriff auf RFC-fähige Bausteine via SOAP
/sap/bc/echo	626073 - Nicht freigegebene Internet Communication Framework Services
/sap/bc/FormToRfc	
/sap/bc/report	
/sap/bc/xrfc	
/sap/bc/xrfc_test	
/sap/bc/error	
/sap/bc/xrfc	
/sap/bc/xrfc_test	
/sap/bc/error	
/sap/bc/webrfc	865853 - WebReporting/WebRFC ab NW2004s veraltet
/sap/bc/bsp/sap/certreq	1417568 - Unautorisierte Änderung von Inhalten in CERTREQ und CERTMAP
/sap/bc/bsp/sap/certmap	
/sap/bc/gui/sap/its/CERTREQ	
/sap/bc/gui/sap/its/CERTMAP	
/sap/bc/bsp/sap/bsp_veri	1422273 Unautorisierte Modifikation von angezeigtem Inhalt in BSP
/sap/bc/bsp/sap/icf	
/sap/bc/IDoc_XML	IDoceingang via HTTP/SOAP
/sap/bc/srt/IDoc	

ICF-Kommunikation über SSL

Es wird empfohlen für die ICF-Kommunikation SSL für alle ICF-Dienste zu verwenden. SSL kann auch nur für einzelne ICF-Dienste konfiguriert werden (siehe APP.4.2.M18 Abschaltung von unsicherer Kommunikation).

ICF-Berechtigungen

Wenn Berechtigungen für ICF-Dienste vergeben werden, muss dabei auf die Funktionstrennung geachtet werden. Benutzer, die auf ICF-Dienste Zugriff haben, sollten nicht über die Dialogschnittstelle (SAP-GUI) auf das SAP-ERP-System zugreifen können. Für das Berechtigungsobjekt S_ICF sollten die folgenden Werte gesetzt sein:

- Feld: ICF_Field = SERVICE
- Feld: ICF_VALUE = muss die Zeichenkette genutzt werden, die im betroffenen ICF-Dienst unter Service-Daten/Service Optionen/SAP-Berechtigung eingetragen ist.

Berechtigungen für die Transaktion SICF können über das Berechtigungsobjekt S_ADMI_FCD mit dem Feldwert S_ADMI_FCD = ICFA gesteuert werden. Über die Transaktion SICF kann der Administrator die Funktionen für SICF aktivieren oder deaktivieren:

- Recording-Funktion nicht erlauben,
- Trace-Funktion nicht erlauben,
- Debugging-Funktion nicht erlauben,
- Laufzeitanalyse-Funktion nicht erlauben.

Folgenden Sicherheitsmaßnahmen sind zusammenfassend für die Aktivierung der ICF-Dienste zu beachten:

- Nur die ICF-Dienste aktivieren, die wirklich benötigt werden.
- Authentisierungsmethoden und Anmeldefolgen für Benutzer von Services definieren.
- Für die ICF-Kommunikation ist SSL zu verwenden.
- ICF-Berechtigungen sind nur restriktiv zu vergeben.
- Fehlerseiten sollten für ICF-Dienste so konfiguriert werden, dass keine internen Informationen ersichtlich sind.

Session Management

Das Secure-Session-Management (Transaktion SICF_SESSIONS) muss für alle Mandanten aktiviert werden. Als Fallback sollte der Parameter icf/user_recheck=1 gesetzt werden. Allerdings wird dann bei jeder neuen http(s)-Anfrage eine neue Anmeldung (eventuell per SAP-Logon-Ticket) durchgeführt, was zu Leistungseinbußen führen kann. icf/user_recheck=1 ist aber unwirksam, solange das Secure-Session-Management aktiv ist.

APP.4.2.M25 Sichere Konfiguration des SAP Web Dispatchers

Der SAP Web Dispatcher sollte nicht der erste Einstiegspunkt aus dem Internet sein. Außerdem sollten folgende Einstellungen vorgenommen werden:

- Der Web-Dispatcher muss immer auf dem aktuellen Stand sein (siehe SAP-Hinweis 538404: Sammelhinweis SAP Web Dispatcher, siehe [SECNOTE]).
- Es sollte eine eigene Fehlerseite konfiguriert werden, damit Informationen (technischer Grund der Fehlermeldung) für potenzielle Angreifer nicht unnötig offengelegt werden. Dazu muss der Parameter icm/HTTP/error_templ_path = /usr/sap/<SID>/<Instance>/data/icmerror gesetzt werden. Alternativ kann auch der Parameter is/HTTP/show_detailed_errors to FALSE benutzt werden (an den Client werden keine Informationen weitergegeben).
- Der Web Dispatcher kann als URL-Filter mit Positivlisten verwendet werden. In jedem Fall müssen die folgenden URLs gefiltert werden, da sie Informationen über die Infrastruktur und Konfiguration zurückgeben:

-
  - D /sap/public/icman/*
  - D /SAP/public/ping
  - D /sap/public/icf_info/*

Der Zugriff auf Informationsseiten wird mit dem Parameter blockiert: D /sap/wdisp/info

Die Webadmin-Oberfläche wird mit den folgenden Parametern sicher konfiguriert:

- Die Verwendung des HTTPS-Ports verhindert es, dass Passwörter abgefangen werden. Die HTTPS-Port-Einstellungen sollten mit dem Parameter icm/server_port_<num> in der URL eingerichtet werden.
- Die Administration des Web Dispatchers sollte nur auf Ports erlaubt sein, die ein sicheres Protokoll (HTTPS) verwenden. In der URL ist ein HTTPS-Port zu benutzen. Für den Parameter icm/HTTP/admin_<num> muss die Option PORT gesetzt werden.
- Der Admin-Port konfiguriert einen Port, der nur im internen Netz erreichbar ist mittels des Parameters icm/HTTP/admin_<num> mit der Option PORT.
- Die Administration sollte nur unter einem bestimmten Hostnamen oder mit einer IP-Adresse aus dem internen Netz erlaubt werden. Dazu wird die Option HOST für den Parameter icm/HTTP/admin_<num> verwendet.
- Die Administration von Clients aus dem internen Netz muss eingeschränkt werden. Dazu wird die Option PORT für den Parameter icm/HTTP/admin_<num> benutzt.

Alle aktuellen Sicherheitseinstellungen für den SAP Web Dispatcher sind im SAP-Hinweis 87017 (siehe [SECNOTE]) zusammengefasst.

APP.4.2.M26 Schutz des kundeneigenen Codes im SAP-ERP-System

SAP und andere Anbieten haben verschiedene Tools entwickelt, die kundeneigenen Code unter den Aspekten Qualität, Sicherheit und Quantität prüfen.

Die folgende Tabelle stellt die SAP-Prüftools für kundeneigenen Code vor:

Tools	Prüfung	Beschreibung
ABAP Test Cockpit (ATC)	Qualität des Codes	• • • • •
Code Vulnerability Analyzer (CVA)	Sicherheit des Codes	• • • •
Usage & Procedure Logging (UPL)	Quantität des Codes	• • •
SAP Solution Manager	Custom Code Lifecycle Management	• • •

Custom Code Lifecycle Management

Das Custom Code Lifecycle Management (CCLM) sowie ergänzende Tools sind seit dem SAP Solution Manager mit der Version 7.1 verfügbar. CCLM wurde entwickelt, um ABAP-Erweiterungen und Neuentwicklungen während des gesamten Lebenszyklus zu begleiten. Der Lebenszyklus startet, wenn ein Objekt (z. B. ein Programm, eine Transaktion oder eine Tabelle) entwickelt wird, geht über die Verwendung im Produktivsystem und erstreckt sich bis hin zur Nichtanwendung oder Neuausrichtung des Objektes. Der Kern des CCLM ist eine generische Bibliothek, die kundeneigene Codes klassifiziert und grundlegende Informationen enthält. Die generische Bibliothek mit allen Informationen ist über eine XML-Datei verfügbar (siehe SAP-Hinweis 1547237 – Technische Konfiguration des CCLM, [SECNOTE]). Der Datensammler erhält die Eigenschaften der kundeneigenen Codes automatisch von den angeschlossenen Systemen. Das kann über einen periodisch angelegten Hintergrundjob gesteuert werden.

Berechtigungen für das CCLM

Da der SAP Solution Manager die Informationen über die zu überwachenden Systeme in internen Tabellen speichert, kann auf sie schnell zugegriffen werden. Es sind jedoch bestimmte Berechtigungen notwendig, um den SAP Solution Manager mit CCLM benutzen zu können. Falls SAP-Standardrollen für CCLM genutzt werden, müssen diese in den kundeneigenen Namensraum kopiert werden:

- SAP_CCLM_DIS: die SAP-Standardrolle enthält die Berechtigung CCLM im Anzeigemodus zu nutzen (keine Änderungen in der Konfiguration möglich).
- SAP_CCLM_ALL: die SAP-Standardrolle enthält das Berechtigungsobjekt SM_CC_AUTH mit dem Berechtigungsfeld SM_CC_LIB (Änderungen in der Konfiguration sind möglich).
- SAP_SMWORK_BASIC_CCLM: die SAP-Standardrolle enthält die Berechtigung auf das Workcenter zuzugreifen und die Basisberechtigung für das Berechtigungsobjekt CCLM.
- SAP_SMWORK_BASIC_CCLM: die SAP-Standardrolle enthält die Berechtigung auf das Workcenter Custom Code Lifecycle Management zuzugreifen.

Der kundeneigene Code sollte durch spezialisierte Prüfwerkzeuge auf Schwachstellen untersucht werden. Das Transportwesen sollte so konfiguriert werden, dass ungeprüfte Entwicklungen oder Programme mit identifizierten Schwachstellen nicht weitertransportiert werden.

APP.4.2.M27 Audit des SAP-ERP-Systems [Fachabteilung]

SAP-ERP-Systeme sollten regelmäßig auditiert werden. Die folgenden Empfehlungen sollten zur Vorbereitung für ein internes und externes Audit eingehalten werden:

- Es sollten aus den relevanten Vorschriften wie ITIL, BASEL II, SOX, FDA oder Datenschutzalle notwendigen Maßnahmen identifiziert werden.
- Die Revisionssicherheit der Systeme wird durch angemessene und effektive Sicherheitsmaßnahmen gewährleistet, insbesondere durch die Zuweisung von Berechtigungen. So sollten beispielsweise nicht uneingeschränkte Berechtigungen durch die Zuweisung des Profils SAP_ALL oder die Zuweisung von Debug- und Änderungsberechtigungen auf dem Produktivsystem vergeben werden.
- Protokolle und Traces sollten definiert und erfasst werden, z. B. die Prüfung der Datenschutzgesetze oder Einschränkungen der Produktionsumgebung. Das Protokollieren der Daten und der Zugriff auf Protokollierungsmöglichkeiten muss eingeschränkt werden.

Für das in der Institution bestehende Risikomanagementrahmenwerk muss ein Plan entwickelt werden, der allen relevanten regulatorischen Anforderungen entspricht. Demzufolge ist es für das Auditmanagement entscheidend, sich die Risikoinformationen anzeigen zu lassen, die von der Institution erfasst und dokumentiert wurden. Darüber hinaus müssen die folgenden Schritte durchgeführt werden:

- alle relevanten regulatorischen Anforderungen identifizieren,
- benötigte Protokolle und Traces definieren, den Security Audit Log (SAL) aktivieren und konfigurieren,
- Protokolle mit geeigneten Tools analysieren,
- Sicherheitsüberprüfungen wie Penetrationstests und Schwachstellenscans durchführen,
- Prüfung der verschiedenen Secure Operation Tracks:
    - Infrastruktureinstellungen und Kommunikationsschnittstellen (Firewall, Dispatcher und Reserve-Proxy, Betriebssystem, RFC-Verbindungen, ALE, ICF, WS usw.),
    - Benutzer und Berechtigungen überprüfen (Stichproben, SAP Access Control usw.).

Ist in einer Institution kein Rahmenwerk für das Risikomanagement definiert, muss das Auditmanagement seine eigene Bewertung über die Risikoeinträge anwenden und diese mit der Geschäftsleitung absprechen.

Der Leiter der internen Revision muss in der Lage sein, die risikobasierenden Pläne und die dafür erforderlichen Ressourcen zusammenzufassen. Der Vorstand und die leitenden Angestellten der Institution haben die Befugnis, die Arbeit der internen Revision zu überwachen.

APP.4.2.M28 Erstellung eines Notfallkonzeptes [Notfallbeauftragter]

Die folgenden Schritte sind zur Vorbereitung und für den Einsatz des Notfallkonzepts für SAP-ERP-Systeme notwendig.

Vorbereitungen auf einen Zwischenfall

- Definition von Prozessen und Verantwortlichen,
- Durchführung von regelmäßigen Notfallübungen und Anpassung der Prozesse,
- Erstellen und Bearbeiten von Notfallbenutzern (siehe APP.4.2.M29 *Einrichten eines Notfallbenutzers*) für alle relevanten Systeme,
- Sammlung von notwendigen Protokollen und Daten,
- Definition von Regeln und Auslösern zur Identifizierung und Klassifizierung von Vorfällen,
- Vorbereitung für technische und nichttechnische (z. B. gesetzliche Vorschriften) Folgeaktivitäten und Verbesserungen.

Etablierung eines Datensicherungs- und Wiederherstellungskonzeptes

Ein wesentlicher Punkt der Notfallvorsorge ist die Datensicherung der SAP-ERP-Systeme. Demzufolge müssen Verantwortlichkeiten und Prozessabläufe in einem Konzept definiert werden. Das Datensicherungskonzept muss ständige verfügbar sein, damit es im Notfall auch schnell umgesetzt werden kann. Die folgenden Informationen und Maßnahmen sind in dem Konzept festzuhalten:

- Wann werden welche Komponenten und Daten gesichert?
- Wer besitzt die Berechtigung dazu?
- Wer besitzt die Berechtigung, Daten wiederherzustellen?
- Wer besitzt Zugriff auf die archivierten Backup-Daten?
- Wo werden die Backup-Daten sicher gelagert? Hier ist besonders darauf zu achten, dass Daten räumlich getrennt von Produktivdaten aufbewahrt werden.

Weiterhin müssen die Verfahren definiert werden, mit denen ein SAP-ERP-System wiederhergestellt werden soll. Da die Verfügbarkeit von SAP-ERP-Systemen und der damit verbundenen Prozesse, Anwendungen und Dienste die Voraussetzung für einen sicheren Betrieb sind, sollten Ausweichsysteme vorgehalten oder hochverfügbare Architekturen für Server benutzt werden (Cold-Stand-by, Hot-Stand-by, Cluster oder Cloud). Vor allem kleinere Unternehmen und Behörden betreiben oftmals eine Single-Server-Installation. In dem Fall wird empfohlen, auf einem Ausweichsystem (z. B. als Cold-Stand-by-System) die letzte Datensicherung einzuspielen. Beide Konzepte sollten jedoch keine Aspekte der allgemeinen Sicherheitsstandards beinhalten, sondern für den Notfall definiert werden.

Konzept der Notfall-Administration erstellen

Sollte mit den normalen Administrator-Benutzerkennungen nicht mehr auf ein SAP-ERP-System zugegriffen werden können, wird ein Notfall-Administrator-Konto benötigt. Der ABAP- und Java-Stack verfügt jeweils über eine Benutzerverwaltung und es muss in jedem Stack ein solches Konto definiert werden. Weitere Informationen zum Notfallbenutzer siehe APP.4.2.M5 *Konfiguration und Absicherung der SAP-Benutzerverwaltung*.

APP.4.2.M29 Einrichten eines Notfallbenutzers

Aufgrund der weitreichenden Berechtigungen ist es notwendig, dass Notfallbenutzer stark kontrolliert werden:

- Notfallbenutzer-IDs unterscheiden sich von normalen Benutzer-IDs.
- Für Notfallbenutzer, die nicht im Einsatz sind, werden Gültigkeitseinschränkungen im System deaktiviert.
- Beim Einsatz der Notfallbenutzer ist der Security Audit Log zu aktivieren.
- Die Nutzung der Notfallbenutzer ist protokollarisch festzuhalten.
- Nach Beendigung des Notfalleinsatzes ist die ID wieder zu sperren und das Kennwort neu zu initialisieren.

Mit dem Produkt SAP Access Control (SAP AC) und der Komponente Emergency Access Management (EAM) lassen sich sogenannte FireFighter als Notfalladministratoren erstellen. Werden die FireFighter eingesetzt, wird das automatisch protokolliert. Das Prinzip des Firefighters besteht darin, dass ein Benutzer (z. B. ein Benutzeradministrator) sich mit der FireFighter-ID in dem jeweiligen SAP-ERP-System anmelden kann. Der Vorteil ist, dass die Notfallmaßnahmen außerhalb seiner eigentlichen Tätigkeit in einer kontrollierten und für den Audit transparenten Umgebung durchgeführt werden.

APP.4.2.M30 Implementierung eines kontinuierlichen Monitorings der Sicherheitseinstellungen

Mit dem Solution Manager ab Version 7.1 ist es möglich, systematische und automatisierte Überwachungsprozesse einzurichten.

Konfigurationsvalidierung

Die Konfigurationsvalidierung dient dazu, die Sicherheitskonfiguration der SAP-ERP-Systeme und den Implementierungsstatus von SAP-Sicherheitshinweisen und Patches zu überwachen. Eine Option der Konfigurationsvalidierung ist es, die Ist-Werte der Konfigurationselemente mit definierten Sicherheitsstandards zu vergleichen. Des Weiteren können Benutzer auf kritische Berechtigungen analysiert werden. Die Konfigurationsvalidierung basiert auf der Änderungsauswertung und der Änderungsdatenbank (CCDB). Die CCDB speichert die Konfigurationsdaten der Systeme, die mit dem SAP Solution Manager verbunden sind.

Funktionen/Sichten der Konfigurationsvalidierung:

- Vorlagen für AuswertungenReports
  - Es gibt verschiedene Auswertungsvorlagen, basierend auf Ad-hoc-Reports.
  - Die Auswertungen sind nach Kategorien unterteilt: Operatorvalidierung, Konsistenzvalidierung, Konfigurations-Reporting und gewichtete Validierung
- Transport-Reporte
  - Bietet schnellen Zugriff auf eine Reihe vordefinierter Reports, damit Transporte geprüft und validiert werden können.
- Lesezeichen
  - Für den späteren Zugriff lässt sich die URL einer Reportvariante sichern.
- Zielsysteme
  - Enthalten benutzerdefinierte Zielkonfigurationsdaten und sind virtuelle Systeme.
- Vergleichslisten
  - Es können Vergleichslisten definiert werden, um ähnliche Systeme, die regelmäßig validiert werden sollen, zu Gruppen zusammenzufassen. Systeme müssen nicht jedes Mal beim Ausführen erneut ausgewählt werden.
- Trendanalyse
  - Reports können regelmäßig in Tages- oder Wochenintervallen eingeplant werden, um Analysen über einen bestimmten Zeitraum zu erhalten. Daraus können dann Trendanalysen erstellt werden.

Weitere Informationen über die Konfigurationsvalidierung sind im SAP-Hinweis 1483508 (siehe [SECNOTE]) beschrieben.

System Recommendations (Systemempfehlungen)

Das Tool System Recommendations liefert passende Empfehlungen zu wichtigen SAP-Hinweisen und Patches für ABAP- und Java-basierte SAP-ERP-Systeme. Abhängig vom aktuellen Systemstatus und bereits implementierten Hinweisen empfiehlt das Tool weitere SAP-Hinweise bezüglich Sicherheit, Performance oder gesetzlichen Änderungen (Java-Patches, HotNews mit hoher Priorität oder allgemeine SAP-Hinweise).

Integration der System Recommendations:

- Im SAP-Support-Portal werden die Hinweise für die ausgewählten Systeme abgefragt und die Informationen werden zum SAP Solution Manager übertragen.
- System Recommendations werden als Änderungsanträge eingebunden.
- Die SAP-Hinweise werden dann heruntergeladen und könnten mit dem Note Assistant implementiert werden.

Funktionen der System Recommendations:

- Anzeigen und Herunterladen von Hinweisen, um sie anschließend zu implementieren.
- Darstellen der Ergebnisse nach Anwendungskomponente, Softwarekomponente oder als Liste. In der Listendarstellung können die Ergebnisse gefiltert und sortiert werden.
- Zuweisen eines Status zu einem Eintrag und Anzeigen von Hinweisinformationen eines bestimmten Status.
- Analysieren, wie sich die Implementierung eines Hinweises auf das System und die Geschäftsprozesse auswirkt.
- Anlegen eines Änderungsantrags bzw. Auswahl eines Java-Patches und Anlegen eines Wartungsvorgangs.
- Definieren eines Hintergrunddienstes zur automatischen Aktualisierung der Hinweisinformationen.

APP.4.2.M31 Konfiguration von SAP Single-Sign-On

SAP Single-Sign-On (SSO) ermöglicht es, die Risiken von ungesicherten Login-Informationen zu senken, Help-Desk-Anrufe zu reduzieren und die Vertraulichkeit und Sicherheit von persönlichen und geschäftlichen Daten sicherzustellen. Folgende sicherheitsrelevante Aspekte sind zu bedenken, wenn SAP Single-Sign-On eingesetzt wird:

- Single-Sign-On sollte nur zwischen vertrauenswürdigen Systemen konfiguriert werden. Insbesondere SSO-Szenarien über Unternehmens- oder Behördengrenzen hinweg sind unter Sicherheitsgesichtspunkten zu vermeiden.
- Es empfiehlt sich, pro Szenario nur ein System für die zentrale Anmeldung einzusetzen, das SSO-Tickets ausstellt. Alle anderen Systeme sollten SSO-Tickets nur akzeptieren.
- Besonders wichtig ist, dass die Kommunikation zwischen dem Browser des Benutzers und dem SAP-ERP-System verschlüsselt wird. Ansonsten besteht die Gefahr, dass Angreifer das SSO-Ticket abhören und damit ohne Anmeldung auf das SAP-ERP-System zugreifen können.

Folgende Profilparameter regeln die SSO-Konfiguration für ein SAP-ERP-System:

- login/accept_sso2_ticket: System akzeptiert SSO-Tickets.
- login/create_sso2_ticket: System stellt SSO-Tickets aus.
- login/ticket_expiration_time: Gültigkeitsdauer der ausgestellten SSO-Tickets in Stunden
- login/ticket_only_by_https: SSO-Tickets werden nur beim Zugriff über HTTPS ausgestellt.
- login/ticket_only_to_host: SSO Tickets werden nur bei Zugriffen auf das ausstellende System verwendet.

Für die Konfiguration von SAP SSO sind zusätzliche administrative Tätigkeiten durchzuführen, die über die Transaktionen SSO2, SSO2_ADMIN (SSO2_ACL) und STRUSTSSO2 gemanagt werden können. SAP empfiehlt, die Transaktion SSO2 zu nutzen.

Neben dem SAP-SSO-Mechanismus über Tickets können auch externe Systeme für SSO genutzt werden. Diese müssen dann jedoch über die SNC-Schnittstelle eingebunden sein.

Für Windows-Umgebungen (ab Windows 2000) wird darauf hingewiesen, Single-Sign-On über Kerberos zu nutzen. In diesem Fall erfolgt die Anmeldung nur am Windows-System. Beim Zugriff auf das SAP-ERP-System ist es dann nicht mehr notwendig, Benutzername und Passwort einzugeben. Der verwendete Windows-Kerberos-SNC-Provider ist standardmäßig und ohne Mehrkosten verfügbar. Es muss jedoch bedacht werden, dass der Windows-Kerberos-SNC-Provider die Kommunikation nicht verschlüsselt. Daher ist nur eine SNC-basierte Authentisierung verfügbar. Ab Windows 2000 ist es jedoch möglich, IPSec zwischen Rechnern einzusetzen und so die Kommunikation zu verschlüsseln. Ob das eine mögliche Variante ist, um Single-Sign-On in einer Institution umzusetzen, muss diese jeweils selbst entscheiden.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

APP.4.2.M32 Echtzeiterfassung und Alarmierung von irregulären Vorgängen (CIA)

Mithilfe von Security-Information-and-Event-Management-(SIEM)-Systemen können Betrugs- und Sicherheitsvorfälle identifiziert werden. Die Systeme sammeln die Logdaten aus verschiedenen Quellen (Netzen, Servern und Datenbanken) und bringen sie mit vordefinierten Regelwerken in Beziehung. Ein Alarm wird ausgelöst, sobald ein Angriffsmuster erkannt wurde.

Für SAP-ERP-Systeme sind Standard SIEM-Produkte nur bedingt geeignet. Die Enterprise Threat Detection (ETD) ist eine Lösung von SAP, die SAP-Protokolle und Logdateien interpretieren und analysieren kann. Es gibt noch viele weitere Lösungen auf dem Markt, die für SAP-ERP-Systeme eingesetzt werden können. Diese Produkte müssen Angriffe aufzeigen, sobald Veränderungen am ABAP-Quellcode durchgeführt, unbefugte Sicherheitseinstellungen erkannt oder Berechtigungen manipuliert wurden.

3 Weiterführende Informationen

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "SAP-ERP-System" finden sich unter anderem in folgenden Veröffentlichungen:

[BVASJ] Benutzerverwaltung mit AS Java

SAP SE, https://help.sap.com/saphelp_nw73/helpdata/de/45/b90177cf2252f8e10000000a1553f7/content.htm?no_cache=true , zuletzt abgerufen am 05.10.2018

[DSAPERP] Prüfleitfaden SAP ERP 6.0

Best Practice - Epfehlungen, Deutschsprachige SAP Anwendergruppe e.V. (DSAG), 2015, https://www.dsag.de/go/leitfaeden , zuletzt abgerufen am 21.03.2018

[SAPAUD] SAP Audit Management

SAP SE, https://help.sap.com/saphelp_fra110/helpdata/de/ab/ce1b52bd543c3ae10000000a441470/frameset.htm und https://help.sap.com/saphel_erp60_sp/helpdata/de/f9/558f40f3b19920e10000000a1550b0/content.htm , zuletzt abgerufen am 21.03.2018

[SAPBAS] SAP Security Baseline Template

SAP SE, https://support.sap.com/support-programs-service/services-optimization-service/media-library.html , zuletzt abgerufen am 20.04.2018

[SAPHELP] SAP Help Portal

SAP SE, https://www.help.sap.com/viewer/index , zuletzt abgerufen am 21.03.2018

[SAPHSCR] SAP HANA Security Checklists and Recommendations

SAP SE, https://help.sap.com/hana/SAP_HANA_Security_Checklists_and_Recommendations_en.pdf , zuletzt abgerufen am 20.04.2018

[SAPLOPA] Standardregeln der Profilparameter für Passwort- und Anmelderegeln

SAP SE, https://help.sap.com/saphelp_nw70ehp2/helpdata/de/4a/c3f18f8c352470e10000000a42189c/content.htm , zuletzt abgerufen am 20.04.2018

[SAPSECPO] Übersicht der Sicherheitsrichtlinienattribute für die Steuerung der Kennwortregeln

Kennwortänderung und Anmelderestriktionen, SAP SE, https://help.sap.com/saphelp_nw74/helpdata/de/e9/c15fb4c06340558898fda99d98cb0d/content.htm?no_cache=true , zuletzt abgerufen am 20.04.2018

[SAPSG] Security Guides zu SAP-Lösungen

SAP SE, https://service.sap.com/securityguide , zuletzt abgerufen am 20.04.2018

[SAPSOPM] SAP Secure Operations Map

SAP SE, https://support.sap,com/en/offeringsprograms/support-service/security-optimization-service-portfolio.html , zuletzt abgerufen am 20.04.2018

[SAPSOS] SAP Security Optimization Services Portfolio

SAP SE, https://support.sap.com/sos , zuletzt abgerufen am 20.04.2018

[SAPSUPP] SAP Support Portal

SAP SE, https://support.sap.com/ , zuletzt abgerufen am 20.04.2018

[SAPSWP] SAP Security White Paper

SAP SE, https://support.sap.com/securitywp , zuletzt abgerufen am 20.04.2018

[SECNOTE] Sicherheitshinweis

SAP SE, https://support.sap.com/securitynotes , zuletzt abgerufen am 20.04.2018

[ZVB] Zentrale Benutzerverwaltung

SAP SE, https://help.sap.com/doc/erp2005_ehp_07/6.07/de-DE/8d/270bea613d2443bad6ce0524f08ca0/frameset.htm , zuletzt abgerufen am 21.03.2018

Umsetzungshinweise zum Baustein APP.4.6 SAP ABAP-Programmierung

1 Beschreibung

1.1 Einleitung

Häufig werden in SAP-Systemen Eigenentwicklungen programmiert. Die Gründe hierfür sind vielfältig, so können Geschäftsprozesse oder Anforderungen an das Reporting mithilfe von Eigenentwicklungen individuell auf die Institution angepasst oder spezielle Funktionen erstellt werden, die in der Standard-Auslieferung nicht vorhanden sind.

Eigenentwicklungen werden von Entwicklern der Institution oder von beauftragten Entwicklern programmiert. Im SAP-Umfeld wird dazu häufig ABAP (Advanced Business Application Programming) verwendet. Dabei handelt es sich um eine proprietäre, plattformunabhängige Programmiersprache der Firma SAP. Sie wurde für die Programmierung kommerzieller Anwendungen im SAP-Umfeld entwickelt und ähnelt in ihrer Grundstruktur entfernt der Sprache COBOL. Wichtige Merkmale sind:

- Integration eines Authentisierungs-, Rollen- und Berechtigungskonzepts,
- Verwendung eines proprietären, datenbankunabhängigen SQL-Derivats (Open SQL),
- Unterstützung der Kommunikation zwischen verschiedenen SAP-Systemen sowie
- Integration von Auditoptionen

1.2 Lebenszyklus

Planung und Konzeption

Es sollten Programmierrichtlinien festgelegt werden, die genau definierte Regeln beinhalten, mit denen sich sicherheitsrelevante Schwachstellen vermeiden lassen (siehe APP.4.6.M5 *Erstellung einer Richtlinie für die ABAP-Entwicklung*). Außerdem müssen Entwickler und Abnahmetester geschult und für mögliche Bedrohungen und Schwachstellen sensibilisiert werden.

Umsetzung und Betrieb

Grundsätzlich müssen Reports und Transaktionen mithilfe von Berechtigungsprüfungen abgesichert werden (siehe APP.4.6.M1 *Absicherung von Report mit Berechtigungsprüfungen* und APP.4.6.M3 *Berechtigungsprüfung vor dem Start einer Transaktion*). Auf proprietäre Berechtigungsprüfungen ist zu verzichten (siehe APP.4.6.M4 *Verzicht auf proprietäre Berechtigungsprüfungen*). Alle Prüfungen sind korrekt auszuwerten und müssen vollständig sein (siehe APP.4.6.M2 *Formal korrekte Auswertung von Berechtigungsprüfungen* und APP.4.6.M6 *Vollständige Ausführung von Berechtigungsprüfungen*). Es darf nicht vorkommen, dass ein Mandant auf die Daten eines anderen Mandanten zugreifen kann (siehe APP.4.6.M20 *Keine Zugriffe auf Daten eines anderen Mandanten*).

Es sollten außerdem Maßnahmen ergriffen werden, die beispielsweise vor unberechtigt ausgeführten Betriebssystemkommandos, eingeschleustem Schadcode, Datenlecks und Open SQL-Injection-Schwachstellen schützen (siehe APP.4.6.M10 *Verhinderung der Ausführung von Betriebssystemkommandos*, APP.4.6.M11 *Vermeidung von eingeschleustem Schadcode*, APP.4.6.M15 *Vermeidung von Datenlecks* und APP.4.6.M18 V*ermeidung von Open SQL-Injection-Schwachstellen*). Auch müssen generische Zugriffe auf Tabelleninhalte und die generische Modulausführung vermieden werden (siehe APP.4.6.M12 *Vermeidung von generischer Modulausführung* und APP.4.6.M13 *Vermeidung von generischem Zugriff auf Tabelleninhalte).*

Zudem empfiehlt es sich, Tools einzusetzen, die vorhandenen ABAP-Quelltext auf bestehende Schwachstellen untersuchen, sie bewerten und dann priorisieren (siehe APP.4.6.M22 *Einsatz von ABAP-Codeanalyse Werkzeugen*). Auf Basis dieser Priorisierung können dann die gefundenen Schwachstellen schrittweise bereinigt werden. ABAP-Quelltext von Drittanbietern sollte im optimalen Fall bereits auf Schwachstellen überprüft werden, bevor er in das eigene Entwicklungssystem eingespielt wird. Gerade hier können Schwachstellen auch ganz bewusst implementiert worden sein, um das Kundensystem gezielt auszuspähen oder anzugreifen.

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "SAP ABAP-Programmierung" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

APP.4.6.M1 Absicherung von Reports mit Berechtigungsprüfungen [Entwickler]

Es gibt viele Möglichkeiten, Reports mit SAP-Standardmitteln oder selbst geschriebenen Programmen zu starten. Hierzu zählen neben den bekannten Transaktionen SE38 und SA38 auch

- Transaktion SE80,
- Transaktion START_REPORT und
- kundeneigene Module.

Ebenso können mit dem Kommando SUBMIT REPORT aus eigenen ABAP-Programmen weitere ABAP-Programme aufgerufen werden.

Nicht bei allen möglichen Startmethoden findet jedoch eine implizite Berechtigungsprüfung seitens SAP statt. Um sich nicht darauf verlassen zu müssen, dass jeder Aufrufer eines Programms zuvor eine passende Berechtigungsprüfung durchführt, sollte jedes Programm selbst eine explizite, zum Kontext des Programms passende Berechtigungsprüfung durchführen.

APP.4.6.M2 Formal korrekte Auswertung von Berechtigungsprüfungen [Entwickler]

Eine Berechtigungsprüfung schützt in einem ABAP-Programm nur dann vor unberechtigtem Zugriff auf Daten, wenn das Ergebnis einer Berechtigungsanfrage auch ausgewertet wird und dieses Ergebnis den weiteren Programmablauf beeinflusst. Deshalb muss nach jeder Berechtigungsprüfung durch das Kommando AUTHORITY-CHECK der Erfolg der Anfrage über die Systemvariable SY-SUBRC abgefragt werden.

Beispiel: Vor der Anzeige von Änderungsbelegen soll geprüft werden, ob der aktuelle Benutzer das Recht hat, diese Belege zu lesen:

AUTHORITY-CHECK OBJECT 'S_SCD0'

ID 'ACTVT' FIELD '08'.

IF SY-SUBRC NE 0.

“Nachricht wegen fehlender Berechtigung und Programmende

ELSE.

“Programmlogik zur Anzeige der Änderungsbelege

ENDIF.

APP.4.6.M3 Berechtigungsprüfung vor dem Start einer Transaktion [Entwickler]

ABAP-Programme können SAP-Transaktionen starten, indem sie die Befehle CALL TRANSACTION oder LEAVE TO TRANSACTION aufrufen. Während LEAVE TO TRANSACTION eine implizite Berechtigungsprüfung für den aktuell angemeldeten Benutzer durchführt, erfolgt dies bei CALL TRANSACTION in der Regel nicht (siehe unten Parameter auth/check/call-transaction). Daher sollten Entwickler immer eine explizite Startberechtigungsprüfung erzwingen, wenn sie den Befehl CALL TRANSACTION verwenden. Ohne diese Prüfung könnten unberechtigte Benutzer an kritische Daten gelangen.

Zwar kann für CALL TRANSACTION über den Profilparameter auth/check/calltransaction auch eine implizite Berechtigungsprüfung erzwungen werden, jedoch sollte der Schutz von Transaktionsaufrufen generell nicht von Konfigurationseinstellungen eines Systems abhängig sein. Außerdem kann die hierdurch erzwungene implizite Prüfung auf das Berechtigungsobjekt S_TCODE in einigen Fällen unzureichend oder aber auch zu einschränkend sein.

Eine unzureichende Prüfung kann dann vorliegen, wenn eine Transaktion mit zusätzlichen Parametern aufgerufen wird. So kann z. B. das erste Bild übersprungen werden und die Transaktion wird im daraufhin eingeblendeten Bild fortgesetzt, wie es durch den aufgerufenen ABAP-Code definiert wird. Je nach Transaktion kann dieses Verhalten eventuell zusätzliche, detailliertere Berechtigungsprüfungen erfordern.

Es existieren jedoch auch Fälle, in denen eine Berechtigungsprüfung auf die gesamte Transaktion mittels S_TCODE kontraproduktiv wäre. Wenn durch das ausgewählte Programm (mittels MODE oder OPTIONS FROM) nur besondere Unterfunktionen einer Transaktion im Hintergrund aufgerufen werden, sollte es nicht erforderlich sein, dem Benutzer eine Genehmigung zum Starten der gesamten Transaktion zu gewähren.

Hinweis: Seit der SAP Netweaver Version 7.40 wird CALL TRANSACTION als obsolet betrachtet, wenn es die neuen Optionen WITH AUTHORITY-CHECK / WITHOUT AUTHORITY-CHECK nicht verwendet. Daher sollten ab dann CALL TRANSACTION-bezogene Berechtigungsprüfungen mittels der Option WITH AUTHORITY-CHECK ausgeführt werden. Diese prüft die S_TCODE-Berechtigung, berücksichtigt aber auch Ausnahmen von Transaktionspaaren, die über Transaktion SE97 konfiguriert werden können. Besitzt der Benutzer unzureichende Zugriffsrechte, wird eine Ausnahme vom Typ cx_sy_authorization_error ausgelöst.

APP.4.6.M4 Verzicht auf proprietäre Berechtigungsprüfungen [Entwickler]

Das Berechtigungswesen in SAP ist ein mächtiges und komplexes Werkzeug. Um es korrekt in ABAP-Programme zu integrieren, muss entweder ein geeignetes SAP-Standard-Berechtigungsobjekt gefunden oder ein neues Berechtigungsobjekt angelegt werden. Anschließend muss definiert werden, welche Ausprägungen die darauf basierenden Berechtigungen haben können, z. B. Anzeigen, Ändern, Einfügen und Löschen eines betriebswirtschaftlichen Objekts. Im nächsten Schritt sind entsprechende Rollen zu definieren oder bestehende Rollen zu ergänzen. Danach müssen die Rollen noch den berechtigten Benutzern zugewiesen werden.

Da in diese Prozesskette zahlreiche Abteilungen involviert sind (Entwicklung, Berechtigungs- und Rollenarchitekten, Berechtigungsadministration), werden in einigen Fällen proprietäre Berechtigungsprüfungen implementiert. Diese fragen oft nur einen bestimmten Benutzernamen (IF SY-UNAME = ‚MUELLER‘.) oder andere Eigenschaften des Benutzers (Abteilung, Organisationseinheit etc.) ab. Allerdings können solche Berechtigungsprüfungen auch dazu benutzt werden, das Standardberechtigungskonzept ganz bewusst zu umgehen, um unrechtmäßigen Zugriff auf Daten zu erhalten oder andere Angriffe durchzuführen. Werden proprietäre Prüfungen im Quelltext von Drittanbietern (Outsourcing, Add-on-Produkte von externen Anbietern) gefunden, ist besondere Vorsicht angebracht.

Deswegen sollte jede Berechtigungsprüfung in ABAP-Programmen technisch ausschließlich durch den Befehl AUTHORITY-CHECK <OBJECT> erfolgen. (Der Befehl kann dabei auch indirekt verwendet werden, zum Beispiel durch den Aufruf von SAP-Modulen, die ihn verwenden.)

Durch die Entwicklungsrichtlinie muss verboten sein, Geschäftslogik basierend auf dem Namen oder anderen Eigenschaften des Benutzers auszuführen.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "SAP ABAP-Programmierung".

APP.4.6.M5 Erstellung einer Richtlinie für die ABAP-Entwicklung

Es sollte eine Richtlinie für die ABAP-Entwicklung erstellt werden, die genau definierte Regeln beinhaltet, wie sicherheitsrelevante Schwachstellen zu vermeiden sind. Die Anforderungen aus dem Baustein APP.4.6 *SAP ABAP-Programmierung* sollten in die Richtlinie aufgenommen werden. Diese Regeln müssen stets zeitnah aktualisiert werden. Gründe hierfür sind z. B. die kontinuierliche Erweiterung des Sprachumfangs der Programmiersprache ABAP selbst oder Erweiterungen, die zusammen mit dem Kern des SAP-Systems (SAP Netweaver Stack) zur Verfügung gestellt werden.

APP.4.6.M6 Vollständige Ausführung von Berechtigungsprüfungen [Entwickler]

Berechtigungsprüfungen werden innerhalb von ABAP-Programmen durch den Befehl AUTHORITY-CHECK <OBJECT> realisiert. Dabei wird geprüft, ob der aktuell angemeldete Benutzer über die passenden Zugriffsrechte für das mit übergebene Berechtigungsobjekt OBJECT verfügt. Das geschieht, indem eine festgelegte Liste von Feldern für das Berechtigungsobjekt überprüft wird.

Die Anweisung AUTHORITY-CHECK sollte immer alle Felder des entsprechenden Berechtigungsobjekts auswerten. Wird ein Feld bei der Berechtigungsprüfung weggelassen, dann werden die Rechte des Benutzers in Bezug auf dieses Feld nicht geprüft. Damit ist die Prüfung unvollständig und kann zu unberechtigtem Zugang führen.

Dazu ein Beispiel:

AUTHORITY-CHECK OBJECT 'S_DEVELOP'

ID 'DEVCLASS' FIELD 'ZPROGS'

ID 'OBJTYPE' FIELD 'FUNC'

ID 'OBJNAME' FIELD 'ZFT'

ID 'ACTVT' FIELD '02'.

IF sy-subrc = 0.

"Benutzer für Aktion berechtigt

ENDIF.

Obwohl hier das Objekt S_DEVELOP auch das Berechtigungsfeld P_GROUP beinhaltet, fehlt es im ABAP-Code und wird folglich nicht geprüft. Hat der Entwickler es vergessen oder absichtlich weggelassen und falls ja, warum? Über die Gründe kann insgesamt nur spekuliert werden.

Wenn bei einer Berechtigungsprüfung ein Feld tatsächlich nicht erforderlich ist, sollte es als DUMMY deklariert und somit ausdrücklich übergangen werden. Der Beispielcode sieht dann wie folgt aus:

AUTHORITY-CHECK OBJECT 'S_DEVELOP'

ID 'DEVCLASS' FIELD 'ZPROGS'

ID 'OBJTYPE' FIELD 'FUNC'

```
ID 'OBJNAME' FIELD 'ZFT'

ID 'P_GROUP' DUMMY "Not required for type 'FUNC'

ID 'ACTVT' FIELD '02'.

IF sy-subrc = 0.

"Benutzer für Aktion berechtigt

ENDIF.
```

Dabei sollten folgende Regeln befolgt werden:

- Eine Prüfung auf alle Felder des Objekts mit DUMMY sollte verboten sein.
- Eine DUMMY-Prüfung auf Felder, die eine Aktivität beschreiben (z. B. ACTVT, AUTHC, CO_ACTION) sollte verboten sein.

Zusammenfassend gilt also: Bei einer Berechtigungsprüfung in ABAP-Programmen sollten alle Felder des relevanten Berechtigungsobjekts explizit einbezogen werden. Werden einzelne Felder tatsächlich nicht benötigt, so sollten diese aus Gründen der Transparenz und Nachvollziehbarkeit als DUMMY gekennzeichnet werden. Zusätzlich sollte am Feld der Grund für die Ausnahme genannt werden. Eine Prüfung aller Felder eines Berechtigungsobjekts auf DUMMY oder eines Feldes, das eine Aktivität beschreibt, bietet keinen hinreichenden Schutz.

APP.4.6.M7 Berechtigungsprüfung während der Eingabeverarbeitung [Entwickler]

In ABAP-Dynpro-Anwendungen werden Menüeinträge und Bildschirmelemente oft basierend auf den Berechtigungen des Benutzers ein- oder ausgeblendet. Dadurch wird zwar verhindert, dass die entsprechende Funktion in der Dynpro-Oberfläche selbst ausgelöst werden kann, jedoch ist es weiterhin möglich, den zugehörigen Funktionscode durch Eingabe in das Kommandofeld der SAP GUI auszulösen. Dadurch kann der Benutzer eine Funktion ausführen, für die er eigentlich nicht berechtigt ist.

Wenn bestimmte Einträge eines Dynpro-Menüs ausgeblendet oder einzelne Schaltflächen deaktiviert werden sollen, dann muss also die Behandlung der zugehörigen Funktionscodes ebenfalls im Quellcode verhindert werden.

Andersherum sollten auch keine Funktionscodes existieren, die keinem Dynpro-Element zugeordnet sind.

APP.4.6.M8 Schutz vor unberechtigten oder manipulierenden Zugriffen auf das Dateisystem [Entwickler]

Aus ABAP-Programmen wird häufig lesend oder schreibend auf Dateien des SAP-Servers zugegriffen. Dabei kann es sich um Daten der Anwendung, aber auch um Konfigurations- oder Log-Informationen handeln.

Erlaubt ein Programm, die zu bearbeitende Datei über eine Benutzereingabe frei zu wählen, so besteht potenziell die Gefahr, dass beliebige Dateien des Servers gelesen, verändert oder gelöscht werden. Somit können Daten nicht nur ausspioniert oder manipuliert werden, sondern sogar das gesamte System kompromittiert werden.

Muss ein Teil des Pfades oder des Dateinamens durch Benutzereingaben bestimmbar sein, dann sollte die Eingabe vor dem Dateizugriff validiert werden.

Der SAP-Hinweis 1497003 "Mögliche Directory Traversals in Anwendungen" (siehe [[1497003]]) beschreibt gleichfalls eine Validierungsfunktion (Funktionsbaustein FILE_VALIDATE_NAME), die genutzt werden sollte, falls keine Whitelist gepflegt werden kann. Über diesen Funktionsbaustein kann der konkrete Dateiname des jeweiligen Aufrufs gegen eine vorher definierte Konfiguration (Transaction FILE) geprüft werden.

APP.4.6.M9 Berechtigungsprüfung in remote-fähigen Funktionsbausteinen [Entwickler]

ABAP-Programme können über SAP-Systemgrenzen hinweg mittels remote-fähiger Funktionsbausteine kommunizieren. Dabei handelt es sich um Funktionsbausteine, die mit dem Attribut remote-fähig gekennzeichnet sind. Die hierzu bereitgestellte Remote-Function-(RFC)-Schnittstelle kann jedoch nicht nur von ABAP-Programmen genutzt werden, sondern auch von allen anderen Systemen, die mit dem jeweiligen SAP-System verbunden sind.

Voraussetzung für die Ausführung remote-fähiger Funktionsbausteine ist lediglich eine erfolgreiche Authentifizierung über das RFC-Protokoll.

SAP prüft dabei implizit über das Berechtigungsobjekt S_RFC die Aufrufberechtigung auf Basis einzelner Funktionsbausteine. Viele Institutionen scheuen jedoch die zusätzliche Komplexität einer Berechtigungsvergabe, die neben der Businesslogik auch noch architektonische Aspekte der Codemodularisierung berücksichtigen soll. Hinzu kommt, dass diese Granularität der Prüfung erst in aktuelleren SAP-Netweaver-Versionen vorhanden ist. Vorher wurde nur auf Basis ganzer Funktionsgruppen geprüft. Entsprechend sind viele RFC-Berechtigungen in Rollen auch noch auf Basis dieser Funktionsgruppen definiert. Aus diesen Gründen sind RFC-Berechtigungen oftmals sehr großzügig vergeben oder überhaupt nicht eingeschränkt.

Alle remote-fähigen Funktionsbausteine sollten deshalb selbst im Code explizit prüfen, ob der Aufrufer berechtigt ist, die zugehörige Businesslogik auszuführen. Die zu prüfenden Berechtigungen sollten hierzu zusammen mit den Fachverantwortlichen oder mit Sicherheitsexperten bestimmt werden.

APP.4.6.M10 Verhinderung der Ausführung von Betriebssystemkommandos [Entwickler]

Es existieren verschiedene Methoden, aus ABAP-Programmen Kommandos an das Betriebssystem zu senden. Zwar haben Administratoren die Möglichkeit, alle erlaubten Betriebssystemkommandos mit den Transaktionen SM49 und SM69 zu definieren, jedoch werden diese nur dann validiert, wenn der Aufruf des Betriebssystemkommandos über die dafür vorgesehenen SAP-Funktionsbausteine erfolgt.

Besonders kritisch sind Betriebssystemaufrufe, wenn Benutzereingaben als Teil des Kommandos verwendet werden (die definierten, erlaubten Kommandos also Parameter beinhalten) oder wenn der Entwickler andere Methoden als die Standardfunktionsbausteine benutzt.

In der Entwicklungsrichtlinie sollte deshalb festgelegt werden, dass Betriebssystemaufrufe ausschließlich über die SAP-Funktionsbausteine SXPG_CALL_SYSTEM oder SXPG_COMMAND_EXECUTE erfolgen. Sind parametrisierte Kommandos in SM49 oder SM69 definiert, ist sicherzustellen, dass die Werte hierfür in ABAP-Programmen nicht von Benutzereingaben bereitgestellt werden. Sollten die Parameter der Kommandos dennoch ganz oder teilweise durch Benutzereingaben befüllt werden, so muss eine Eingabevalidierung vorgenommen werden.

Jedem Aufruf eines erlaubten Betriebssystemkommandos muss außerdem eine entsprechende Berechtigungsprüfung (Berechtigungsobjekt S_LOG_COM) vorangestellt werden.

APP.4.6.M11 Vermeidung von eingeschleustem Schadcode [Entwickler]

Mithilfe der ABAP-Befehle INSERT REPORT und GENERATE SUBROUTINE POOL können aus einem ABAP-Programm heraus weitere ABAP-Programme dynamisch generiert und nachfolgend auch gestartet werden. Werden Programme aber erst zur Laufzeit erzeugt, entziehen sie sich damit einer vorherigen Überprüfung (Codeanalyse). Das stellt ein sehr hohes Sicherheitsrisiko dar.

So ist es zum Beispiel ohne weiteres möglich, einen SAP-Standard-Report mittels READ REPORT in eine interne Tabelle einzulesen, die Sätze der Tabelle nachfolgend zu bearbeiten, um dann das so geänderte Coding wieder mit INSERT REPORT unter dem alten Programmnamen im System abzulegen. Diese Änderungen werden weder vom SAP-Änderungs- und -Transportwesen aufgezeichnet, noch wird das betroffene Programm vor der Änderung versioniert.

Noch gefährlicher ist es, wenn der Inhalt des dynamisch erzeugten Programms von Benutzereingaben abhängt. Werden solche Eingaben nicht sorgfältig im Code validiert, können Angreifer auf diesem Weg Schadcode in das System einschleusen.

Beispiel:

TYPES: line(255) TYPE c.DATA: lt_tab TYPE STANDARD TABLE OF line.DATA: lv_input TYPE string.DATA: lv_code TYPE string.lv_input = me->request->get_form_field('lv_input').CONCATENATE 'WRITE '"lv_input"'.INTO lv_code.APPEND 'report ZTF_REPORT.'TO lt_tab.APPEND 'write: ''Anzahl Kilometer: '.TO lt_tab.APPEND lv_code TO lt_tab.INSERT REPORT 'ZTF_REPORT' FROM lt_tab.SUBMIT ('ZTF_REPORT').

Der Code generiert ein ABAP-Programm, in dem die Kilometeranzahl ausgegeben werden soll, die zuvor vom Benutzer eingegeben wurde. Gibt der Benutzer "100" ein, erscheint die Ausgabe "Anzahl Kilometer: 100". Die gleiche Ausgabe erscheint, wenn der Benutzer

"100'. DELETE FROM MARA. DELETE FROM KNA1. WRITE '"

eingibt. Allerdings hat er so auch noch sämtliche Material- und Kundenstammdaten gelöscht.

Auch wenn das genannte Beispiel durch eine einfache Validierung der Eingabe auf numerische Zeichen behoben werden kann, so sollte aus Gründen der Transparenz und Testbarkeit auf dynamischen Code verzichtet werden.

Die Verwendung von Techniken, die ABAP-Quelltext zur Laufzeit erzeugen, sollte generell durch die Enwicklungsrichtlinie verboten sein. Sollten trotzdem dynamisch generierte Programme benötigt werden, so müssen diese Funktionen genehmigt und dokumentiert werden. Weiterhin ist darauf zu achten, dass möglichst keine direkten Benutzereingaben in den generierten Quellcode übertragen werden, sondern der Quellcode z. B. aus konstanten Textliteralen zusammengesetzt wird.

Wird der generierte Quellcode dennoch aus externen Parametern versorgt, so ist zwingend eine Eingabevalidierung vorzunehmen, z. B. mithilfe einer vordefinierte Liste erlaubter Werte oder einer Suche nach nicht erlaubten Zeichen.

APP.4.6.M12 Vermeidung von generischer Modulausführung [Entwickler]

Die Ausführung von ABAP-Modulen über die entsprechenden SAP-Standardtransaktionen ist durch eine implizite Berechtigungsprüfung geschützt.

Technisch gesehen werden ABAP-Module durch ABAP-Befehle aufgerufen. Diese Befehle erlauben es auch, den Namen des aufgerufenen Moduls dynamisch zur Laufzeit anzugeben. Ist dieser Name durch Benutzereingaben beeinflussbar, können hierüber potenziell beliebige Module des aufgerufenen Modultyps (Transaktionen, Reports, Methoden, Funktionsbausteine) ausgeführt werden.

Beispiel:

DATA: request TYPE REF TO if_http_request.

DATA: my_report TYPE string.

DATA: event TYPE string.

my_report = request->get_form_field('myreport').

TRY.

SUBMIT my_report.

RETURN.

ENDTRY.

Die generische Ausführung von ABAP-Modulen muss deshalb durch die Entwicklungsrichtlinie verboten sein.

Sollte es jedoch wichtige Gründe für eine generische Ausführung geben, muss detailliert dokumentiert werden, wo und warum das geschieht. Zusätzlich sollte dann eine Whitelist definiert werden, die alle erlaubten Module enthält. Bevor ein Modul aufgerufen wird, sollte die Benutzereingabe mit der Whitelist abgeglichen werden. Eine weitere benutzerbezogene Differenzierung kann durch eine passende vorangestellte Berechtigungsprüfung (AUTHORITY-CHECK) erfolgen.

APP.4.6.M13 Vermeidung von generischem Zugriff auf Tabelleninhalte [Entwickler]

Für den Zugriff auf Tabelleninhalte stellt der SAP-Standard verschiedene Transaktionen zur Verfügung, z. B. SM30, SE16 und SE16N. Diese Transaktionen sollten durch eine gezielte Berechtigungsvergabe vor unberechtigten Zugriffen geschützt werden.

Die SAP-Standardtransaktionen, mit denen sich Datenbanktabellen auslesen lassen, basieren auf dem Befehl SELECT. Er erlaubt es, den Namen der zu lesenden Tabelle dynamisch zur Laufzeit anzugeben. Wird ein solcher generischer SELECT-Befehl in Eigenentwicklungen benutzt und ist der Tabellenname durch Benutzereingaben beeinflussbar, kann hierüber potenziell jede dem SAP Data Dictionary bekannte Tabelle aus der Datenbank gelesen werden. Damit besteht das Risiko, dass durch Eigenentwicklungen die Absicherung von Transaktionen (z. B. SM30, SE16 und SE16N) ausgehebelt wird.

Beispiel:

DATA: lv_tab TYPE string.

DATA: lv_year TYPE string.

DATA: lv_ccvar TYPE string.

DATA: request TYPE REF TO IF_HTTP_REQUEST.

lv_tab = request->get_form_field('reference').

lv_year = '2010'.

SELECT ccdata FROM (lv_tab) INTO lv_ccvar WHERE lyear = lv_year.

Enthält der Parameter "reference" den Namen einer Tabelle mit einer Spaltenbezeichnung "ccdata" und einer Spaltenbezeichnung "lyear" können die selektierten Spalten ohne Berechtigung gelesen werden.

Das generische Auslesen von Tabelleninhalten sollte deshalb durch die Entwicklungsrichtlinie verboten sein.

Sollte es wichtige Gründe für einen generischen Zugriff geben, muss detailliert dokumentiert werden, wo und warum das geschieht. Außerdem sollte dann gewährleistet sein, dass sich der dynamische Tabellenname auf eine kontrollierbare Liste von Werten beschränkt. Eine dynamische OSQL-Abfrage muss in diesem Fall mindestens eine Präfix-Zeichenkette mit statischen Daten verwenden. Zusätzlich können die statischen Methoden CHECK_TABLE_NAME_STR und CHECK_TABLE_NAME_TAB der Klasse CL_ABAP_DYN_PRG benutzt werden, um zu prüfen, ob eine gültige (vorhandene) Tabelle übergeben wurde und ob diese Tabelle zu einer definierten Liste gehört.

Beispiel:

DATA: lv_tab TYPE string.

DATA: lv_year TYPE string.

DATA: lv_ccvar TYPE string.

DATA: request TYPE REF TO IF_HTTP_REQUEST.

lv_tab = request->get_form_field('reference').

```
lv_year = '2010'.

*Es sind nur Tabellen erlaubt, die mit 'ZFINT' beginnen.

CONCATENATE 'ZFINT' lv_tab INTO lv_tab.

SELECT ccdata FROM (lv_tab) INTO lv_ccvar WHERE lyear = lv_year.
```

APP.4.6.M14 Vermeidung von nativen SQL-Anweisungen [Entwickler]

Der Sprachumfang von ABAP umfasst mit OPEN SQL ein proprietäres SQL-Derivat, dessen Anweisungen portabel, also vom darunterliegenden Datenbankmanagementsystem unabhängig sind. Open SQL-Anweisungen arbeiten standardmäßig mit einer automatischen Mandantenbehandlung. Anweisungen, die auf mandantenabhängige Anwendungstabellen zugreifen, lesen und bearbeiten nur die Daten des aktuellen Mandanten.

Durch direkte Verwendung der ABAP-Anweisung EXEC SQL oder durch Verwendung der Klassen der ABAP Database Connectivity (ADBC) lassen sich zusätzlich auch native, datenbankspezifische SQL-Kommandos ausführen. Derartige spezielle Befehle gehen weit über den Sprachumfang von OPEN SQL hinaus und können schwerwiegende Sicherheitsprobleme hervorrufen, wenn zum Beispiel Befehle auf dem Betriebssystem ausgeführt werden.

Des Weiteren ist zu beachten, dass mit EXEC SQL ausgeführte SQL-Befehle nicht in den SAP-Prüfprotokollen erscheinen. Zudem führt EXEC SQL keine automatische Mandantenbeschränkung aus, wie es bei Open SQL der Fall ist (siehe auch APP.4.6.M20 Keine Zugriffe auf Daten eines anderen Mandanten). Aus diesem Grund stellt jeder Zugriff auf eine SAP-Datenbank mit einer mandantenabhängigen Tabelle unter Umständen einen Compliance-Verstoß dar.

Native SQL-Nutzung ist eventuell akzeptabel, wenn Daten in einer externen Datenbank verarbeitet werden, d. h. nicht in der SAP-Datenbank. Das primäre Sicherheitsrisiko von EXEC SQL liegt in der Umgehung des Open SQL Layer und darin, dass potenziell schädliche SQL-Anweisungen in der SAP-Datenbank ausgeführt werden. Werden die EXEC-SQL-Befehle an eine externe Datenbank gesendet, hängt das Risiko von den Schutzanforderungen dieser externen Datenbank ab. Falls die externe Datenbank keine kritischen Daten enthält, sind die durch EXEC SQL ausgeführten Befehle nicht gefährlich, und eine solche Verwendung kann als annehmbar betrachtet werden.

Die Verwendung von EXEC SQL oder ADBC sollte über die Entwicklungsrichtlinie verboten sein. In keinem Fall darf eine Benutzereingabe Teil von ADBC-Befehlen sein.

APP.4.6.M15 Vermeidung von Datenlecks [Entwickler]

SAP-Systeme verwalten oft geschäftskritische Daten. Ein Risiko liegt insbesondere dann vor, wenn solche Daten unberechtigt

- angezeigt werden (z. B. SAP GUI, HTML, UI5, Smartforms, Adobe Forms ...),
- in Dateien gespeichert werden (sowohl Server- als auch Client-seitig),
- an andere Anwendungen oder Benutzer übertragen werden (z. B. via RFC, HTTP, FTP, E-Mail).

Deshalb müssen Institutionen zunächst festlegen, welche Daten im SAP-System geschäftskritisch oder vertraulich sind oder auch besonderen gesetzlichen Anforderungen unterliegen. Es müssen immer Berechtigungsprüfungen durchgeführt werden, wenn diese Daten angezeigt, übermittelt oder exportiert werden. Jeder (beabsichtigte) Abfluss dieser Daten muss dokumentiert sein.

APP.4.6.M16 Verzicht auf systemabhängige Funktionsausführung [Entwickler]

Mit der Systemvariablen SY-SYSID kann ein ABAP-Programm abfragen, auf welchem System es gerade ausgeführt wird. Sie kann somit dazu verwendet werden, den Kontrollfluss eines Programms systemabhängig zu beeinflussen.

Entwickler stellen mit SY-SYSID beispielsweise sicher, dass während des Tests auf dem Qualitätssicherungssystem keine produktiven Schnittstellen mit Testdaten bedient werden. Da die System-ID eines Qualitätssicherungssystems nicht der System-ID des Produktivsystems entspricht, werden die betreffenden Codeabschnitte in der Testphase nicht durchlaufen. Diese Vorgehensweise kann jedoch dazu führen, dass ungetestete Codeabschnitte oder auch Schadcode in das Produktivsystem übertragen werden.

Das folgende Beispiel zeigt, wie geschäftskritische Daten im Produktivbetrieb an einen anderen Empfänger umgeleitet werden können:

IF sy-sysid = 'P23'

lv_mailtarget = 'vicky.lieks@datenklau.ko'.

ELSE.

lv_mailtarget = 'hr@careless-company.com'.

ENDIF.

Sollten systemabhängige Funktionsausführungen tatsächlich erforderlich sein, muss detailliert dokumentiert werden, wo sie verwendet werden und warum. Dadurch kann die Qualitätssicherung zumindest mittels manueller Codeanalyse erfolgen.

APP.4.6.M17 Verzicht auf mandantenabhängige Funktionsausführung [Entwickler]

Mit der Systemvariablen SY-MANDT kann ein ABAP-Programm abfragen, in welchem Mandanten es gerade ausgeführt wird. Sie kann somit dazu verwendet werden, den Kontrollfluss eines Programms mandantenabhängig zu beeinflussen. Entwickler benutzten die Variable oft in Mehrmandantensystemen, um leicht abweichende Anforderungen für verschiedene Mandanten innerhalb eines Programms abzubilden.

Da die Mandantenstruktur eines Qualitätssicherungssystems nicht notwendigerweise der des Produktivsystems entspricht, werden die betreffenden Codeabschnitte in der Testphase nicht durchlaufen. Diese Vorgehensweise kann jedoch dazu führen, dass ungetestete Codeabschnitte oder Schadcode in das Produktivsystem übertragen werden. Das folgende Beispiel zeigt, wie geschäftskritische Daten im Produktivbetrieb an einen anderen Empfänger umgeleitet werden können:

IF sy-mandt = '100'

lv_mailtarget = 'vicky.lieks@datenklau.ko'.

ELSE.

lv_mailtarget = 'hr@careless-company.com'.

ENDIF.

Sollten mandantenabhängige Funktionsausführungen trotzdem erforderlich sein, muss detailliert dokumentiert werden, wo sie verwendet werden und warum. Dadurch kann die Qualitätssicherung auf den entsprechenden Mandanten stattfinden oder zumindest mittels manueller Codeanalyse erfolgen.

APP.4.6.M18 Vermeidung von Open-SQL-Injection-Schwachstellen [Entwickler]

Mit dynamischem Open SQL können bestimmte Teile eines Open SQL-Befehls auch zur Laufzeit übergeben werden. Werden in einem solchen dynamischen Teil des Open SQL-Befehls Benutzereingaben verarbeitet, kann der betroffene Befehl manipuliert werden. Dadurch kann ein Angreifer sich unberechtigten Zugang zu Daten beschaffen und diese, je nach Art der Schwachstelle, sogar manipulieren oder löschen.

Beispiel:

Der Entwickler eines ABAP-Programms hat vorgesehen, dass ein Benutzer aus einer Tabelle, nur Sätze löschen darf, die zu diesem Benutzer gehören. Zusätzlich soll der Benutzer die zu löschenden Sätze aber zeitlich weiter einschränken können. Hierzu wird ihm die Eingabe eines weiteren Filters auf das Feld TA_REF angeboten.

DATA: cl_where TYPE string.

DATA: cref TYPE string.

DATA: request TYPE REF TO IF_HTTP_REQUEST.

cref = request->get_form_field('reference') .

CONCATENATE ‘uname = ‘’’ sy-uname ‘’’ INTO cl_where.

CONCATENATE cl_where ‘ AND ta_ref = ‘’’ cref ‘’’ INTO cl_where.

DELETE FROM orders WHERE (cl_where).

Mit der Eingabe des Wertes "000100" werden also alle Einträge gelöscht, die der Bedingung:

UNAME = <aktueller Benutzer> AND TA_REF = ‘000100‘

genügen.

Ändert der Benutzer jedoch seine Eingabe in *’OR TA_REF LIKE ,%‘*, so wird daraus die Gesamtbedingung:

UNAME = <aktueller Benutzer> AND TA_REF = ‘ ‘ ’ OR TA_REF LIKE ,%‘

In diesem Fall würde die Tabelle also komplett gelöscht werden.

Die Verwendung von dynamischem Open SQL sollte deshalb durch die Entwicklungsrichtlinie verboten sein. Sollten dennoch Datenbankzugriffe mit dynamischen SQL-Bedingungen notwendig sein, sollten möglichst keine Benutzereingaben in die Abfrage übertragen werden. Wenn das dennoch der Fall ist, muss die Benutzereingabe zwingend geprüft werden (Output Encoding). Der SAP-Hinweis 1520356 (SQL-Injections vermeiden) beschreibt Module, die dazu verwendet werden können.

Zusätzlich ist in höheren Releases auch die eingebaute Funktion ESCAPE verfügbar, mit der das Encoding durchgeführt werden kann.

Beispiel:

DATA: cl_where TYPE string.

DATA: cref TYPE string.

DATA: request TYPE REF TO IF_HTTP_REQUEST.

cref = request->get_form_field('reference') .

cref = cl_abap_dyn_prg=>escape_quotes(cref).

CONCATENATE ‘uname = ‘’’ sy-uname ‘’’ INTO cl_where.

CONCATENATE cl_where ‘ AND ta_ref = ‘’’ cref ‘’’ INTO cl_where.

DELETE FROM orders WHERE (cl_where).

APP.4.6.M19 Schutz vor Cross-Site-Scripting [Entwickler]

Bei Cross-Site-Scripting-Angriffe (XSS) werden speziellen Befehlssequenzen in eine HTML-Seite eingefügt, wenn in dieser Seite (Benutzer-)Eingaben erfolgen. Ruft der Benutzer die HTML-Seite auf, wird der eingeschleuste Code im Browser ausgeführt.

Cross-Site-Scripting stellt in der Regel einen Angriff auf Client-Systeme dar. Um XSS-Angriffe zuverlässig abzuwehren, sollte jede Benutzereingabe mithilfe der ESCAPE_XSS_*-Methoden der SAP-Standard-Klasse CL_ABAP_DYN_PRG encodiert werden. Zusätzlich ist in höheren Releases auch die eingebaute Funktion ESCAPE verfügbar, mit der das Encoding durchgeführt werden kann.

Der beste Schutz wird jedoch erreicht, indem auf selbst entwickeltes HTML in Business-Server Pages-(BSP)-Anwendungen oder HTTP-Handlern verzichtet wird. Rendering-Mechanismen wie Web Dynpro oder UI5 generieren HTML automatisiert. Da Entwickler nicht mehr in das HTML-Rendering eingreifen können, sind diese Plattformen deutlich sicherer.

APP.4.6.M20 Keine Zugriffe auf Daten eines anderen Mandanten [Entwickler]

Ein SAP-System besitzt immer mindestens einen, oft aber auch mehrere Mandanten. Ein Mandant ist die organisatorisch höchste Einheit im System. Jeder Mandant kann betriebswirtschaftlich als Konzern, Unternehmen, Behörde oder Betrieb aufgefasst werden. Der Mandant stellt somit eine Einheit dar, die handelsrechtlich, organisatorisch und auch datentechnisch abgeschlossen ist. Er verfügt über von anderen Mandanten getrennte Sätze an Tabellen und Daten.

Werden in ABAP-Programmen nur Open SQL-Befehle verwendet, ist durch den SAP-Kernel sichergestellt, dass standardmäßig nur auf Daten aus dem aktuellen Mandanten zugegriffen wird. Dadurch ist gewährleistet, dass die Daten unterschiedlicher Mandanten voneinander getrennt sind. Es gibt jedoch verschiedene Möglichkeiten, diese automatische Mandantentrennung zu umgehen. So kann mit Open SQL durch den Zusatz CLIENT SPECIFIED auf Daten aus einem anderen Mandanten zugegriffen werden. Auch wenn natives SQL benutzt wird, ist ein direkter Zugriff auf andere Mandanten möglich (siehe APP.4.6.M14 Vermeidung von nativen SQL-Anweisungen). Ein solcher Zugriff auf Daten eines anderen Mandanten ist vor allem bei Systemen gefährlich, deren SAP-Mandanten verschiedene Unternehmen abbilden. Das betrifft insbesondere Hosting-Systeme.

Deswegen sollte es Entwicklern über die Entwicklungsrichtlinie verboten werden, die Open SQL-Option CLIENT SPECIFIED sowie EXEC SQL zu benutzen.

APP.4.6.M21 Verbot von verstecktem ABAP-Quelltext [Entwickler]

In allen SAP-Netweaver-Versionen älter als 7.50 ist es möglich, den ABAP-Quellcode durch Voranstellen einer bestimmten Zeichensequenz zu verstecken. Diese Methode wird z. B. von Drittanbietern verwendet, um die Entschlüsselung von Lizenzschlüsseln nicht offenlegen zu müssen. In Eigenentwicklungen sollte diese Technik jedoch verboten sein, da der ABAP-Code sonst weder manuell überprüft, noch von automatischen Codeanalysen erfasst werden kann. Bestenfalls ist ein funktionaler Test möglich, dessen Ergebnis durch Verwendung weiterer illegaler Methoden aber leicht verfälscht werden kann.

Techniken, die das Lesen von Quellcode verhindern, sollten deswegen nicht erlaubt sein. Das Verbot ist in der Entwicklungsrichtlinie zu dokumentieren.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

APP.4.6.M22 Einsatz von ABAP-Codeanalyse Werkzeugen (CIA)

Werden SAP-Systeme in Umgebungen mit erhöhtem Schutzbedarf eingesetzt, so sollte eine automatisierte Überprüfung der Eigenentwicklungen auf sicherheitsrelevante Programmierfehler, funktionale und technische Fehler sowie qualitative Schwachstellen durchgeführt werden. Dies kann mit Werkzeugen von der SAP wie SAP ABAP Test Cockpit oder SAP Code Inspector erfolgen oder mit Werkzeugen von Fremdanbietern.

3 Weiterführende Informationen

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "SAP ABAP-Programmierung" finden sich unter anderem in folgenden Veröffentlichungen:

[1497003] SAP-Hinweis 1497003

"Mögliche Directory Traversals in Anwendungen", SAP SE, 2011, https://service.sap.com/sap/support/notes/1497003, zuletzt abgerufen am 01.02.2018

[1520356] SAP-Hinweis 1520356

"SQL-Injections vermeiden", SAP SE, 2011, https://service.sap.com/sap/support/notes/1520356, zuletzt abgerufen am 01.02.2018

[DSAGABAP] Best Practice Guide

Leitfaden Development ABAP 2.0, Deutschsprachige SAP Anwendergruppe e.V. (DSAG), 2016, https://www.dsag.de/seite/best-practice-guide-leitfaden-development-abap-20 , zuletzt abgerufen am 05.10.2018

[SABAP] Sichere ABAP-Programmierung

Wiegenstein, Schuhmacher, Schinzel, Weidemann, SAP Press 2009

Umsetzungshinweise für die Bausteinschicht SYS

Umsetzungshinweise zum Baustein SYS.1.1 Allgemeiner Server

1 Beschreibung

1.1 Einleitung

Diese Umsetzungshinweise decken allgemeine Sicherheitsanforderungen für alle IT-Systeme ab, die Dienste anderen IT-Systemen bereitstellen, wie Clients oder anderen Servern. Diese Dienste können Basisdienste für das lokale oder externe Netz sein, aber auch den E-Mail-Austausch ermöglichen oder Datenbanken und Druckerdienste anbieten. Server haben eine zentrale Bedeutung für die Informationstechnik und damit für funktionierende Arbeitsabläufe einer Institution. Oft erfüllen Server Aufgaben, ohne dass eine direkte interaktive Nutzung durch einen Benutzer erfolgt. Ergänzend gibt es Serverdienste, die direkt mit den Anwendern interagieren und nicht auf den ersten Blick als Server-Dienst wahrgenommen werden, beispielsweise X-Server unter Unix.

1.2 Lebenszyklus

Planung und Konzeption

Im Vorfeld der eigentlichen Planung ist die generelle Architektur des Netzes festzulegen bzw. zu analysieren, aus der sich im Allgemeinen auch Vorgaben für die einzusetzenden Betriebssysteme (Server und Client) ergeben. Insbesondere ist dabei festzulegen, welche Ziele mit dem aufzubauenden Server verfolgt werden. Dazu sind die voraussichtlichen Einsatzszenarien zu beschreiben und der Einsatzzweck zu definieren.

Falls ein neues Netz aufgebaut wird, ist zunächst die Struktur des Netzes insgesamt zu planen, wobei Fragen wie die Festlegung einer Netztopographie und die Entscheidung über den Grad der Serverzentrierung (Terminalserver, "klassische" Client-Server-Architektur oder Nutzung von Peer-to-Peer-Funktionalität) zu klären sind. Hier sind die Maßnahmen des Bausteins NET.1.1 Netz-Architektur und -Design heranzuziehen.

In einem weiteren Schritt folgt die Festlegung der auf der Ebene der Server und der Clients verwendeten Betriebssysteme und gegebenenfalls auch die Auswahl spezifischer Varianten (z. B. Windows Server 2016 gegenüber Windows Server 2012 oder Linux gegenüber einer herstellerspezifischen Variante von Unix).

Falls ein neues Netz aufgebaut wird, muss als genaue technische Grundlage für die weiteren Arbeiten der detaillierte Aufbau des Netzes geplant werden. Anzahl und Zusammenspiel der vorgesehenen Server sind festzulegen. Die Aufgaben der Server und die Art ihrer Nutzung durch die Clients sind zu bestimmen. Anhand der Anforderungen an die Verfügbarkeit muss festgelegt werden, bis zu welchem Grad redundante Strukturen im Netz vorzusehen sind. Hier sind auch die notwendigen Vorgaben für die Infrastruktur (vor allem Klimatisierung und Stromversorgung, siehe dazu SYS.1.1.M15 Lokale unterbrechungsfreie und stabile Stromversorgung) festzulegen. Parallel dazu ist eine allgemeine Sicherheitsrichtlinie zu erarbeiten (siehe SYS.1.1.M11Festlegung einer Sicherheitsrichtlinie für einen allgemeinen Server), die anschließend durch systemspezifische Sicherheitsrichtlinien und detaillierte Richtlinien für den Einsatz der Hard- und Software im Netz zu ergänzen ist (siehe dazu die Bausteine zu den einzelnen Server-Betriebssystemen).

Beschaffung

Im nächsten Schritt muss die Beschaffung der Hardware und eventuell zusätzlich benötigter Software erfolgen. Aufbauend auf Einsatzszenarien sind die Anforderungen an zu beschaffende Produkte zu formulieren und basierend darauf die Auswahl der geeigneten Produkte zu treffen. Mit der Beschaffung dieser Produkte ist dann die Grundlage für die Arbeiten des nächsten Schrittes gelegt. Vertiefende Informationen zur Beschaffung sind im Baustein OPS.1.2.6 Beschaffung, Ausschreibung und Einkauf zu finden.

Umsetzung

Die Benutzer bzw. die Administratoren haben einen wesentlichen Einfluss auf die Sicherheit eines Servers. Vor der tatsächlichen Inbetriebnahme müssen die Benutzer und Administratoren daher für den Umgang bzw. die Nutzung des aufzubauenden Servers geschult werden. Insbesondere für Administratoren empfiehlt sich aufgrund der Komplexität in der Planung und in der Verwaltung eine intensive Schulung. Die Administratoren sollen dabei detaillierte Systemkenntnisse erwerben, so dass eine konsistente und korrekte Systemverwaltung gewährleistet ist. Benutzern sollte insbesondere die Nutzung der verfügbaren Sicherheitsmechanismen vermittelt werden. Hier sind die Anforderungen des Bausteins ORP.3 Sensibilisierung und Schulung zur Informationssicherheit heranzuziehen.

Nachdem die organisatorischen und planerischen Vorarbeiten durchgeführt wurden, kann die Installation und Inbetriebnahme des Servers erfolgen. Dabei sind die folgenden Empfehlungen zu beachten:

- Schon die Installation und Grundkonfiguration eines Servers muss mit besonderer Sorgfalt durchgeführt werden, um schwer reparierbare Fehler von vornherein zu vermeiden. Allgemeine Hinweise hierzu finden sich in SYS.1.1.M16 Sichere Installation. Neben den allgemeinen Maßnahmen, die in diesen Umsetzungshinweisen beschrieben sind, sind jeweils auch die weitergehenden Maßnahmen, die in den betreffenden Bausteinen für das jeweilige Betriebssystem empfohlen werden, umzusetzen.
- Nach der Installation und Grundkonfiguration der Server müssen gegebenenfalls übergeordnete Verwaltungsstrukturen konfiguriert werden. Dabei kommt unter anderem auch zum Tragen, für welchen Einsatzzweck die einzelnen Server geplant sind, beispielsweise als Dateiserver, Druckserver oder, im Falle von Thin Clients, als Terminalserver. Hier ist insbesondere die Maßnahme SYS.1.1.M6 Deaktivierung nicht benötigter Dienste und Kennungen wichtig, um einen kontrollierbaren Betrieb des Servers gewährleisten zu können.
- Nachdem die Installation und Grundkonfiguration des Servers abgeschlossen ist, kann die eigentliche Serversoftware installiert und konfiguriert werden. Die dafür notwendigen Schritte unterscheiden sich je nach Art und Einsatzzweck der Software teilweise erheblich und werden teilweise in eigenen Bausteinen behandelt. Prinzipiell wird empfohlen, für die Installation und Konfiguration der Serversoftware analog wie für die Konfiguration des Betriebssystems selbst vorzugehen:
    - Erstellung eines Installationskonzepts
    - Falls mehrere Server mit ähnlichen Einsatzgebieten und Konfiguration installiert werden sollen: Erstellen einer Referenzinstallation
    - Installation, Grundkonfiguration, Aktualisierung und Härtung
    - Test und optionaler Penetrationstest bei erhöhtem Schutzbedarf

Betrieb

Nach der Erstinstallation und einer Testbetriebsphase wird der Regelbetrieb aufgenommen. Unter Sicherheitsgesichtspunkten sind dabei folgende Aspekte zu beachten:

- Client-Server-Netze ändern sich sehr häufig. Dabei muss bei jeder Änderung sichergestellt werden, dass die Sicherheit auch nach der Änderung nicht beeinträchtigt wird. Die dabei im Detail zu beachtenden Aspekte sind in den Bausteinen zu den jeweiligen Serverbetriebssystemen enthalten. Dabei ist zu berücksichtigen, dass auch der Entzug von Berechtigungen sowie das Löschen nicht mehr benötigter Datenbestände so geregelt wird, dass durch veraltete Strukturen keine Sicherheitslücken entstehen. Eine wesentliche Hilfe ist dabei eine effiziente, umfassende Systemverwaltung, die sich jederzeit auf aktuelle Informationen über den Zustand des Systems und seiner Rechtestrukturen abstützen kann (siehe dazu SYS.1.1.M3 Restriktive Rechtevergabe und SYS.1.1.M21 Betriebsdokumentation).
- Ein Mittel im Rahmen der Aufrechterhaltung der Sicherheit eines Servers ist die Überwachung des Systems bzw. seiner Einzelkomponenten. Die hier relevanten Empfehlungen finden sich in SYS.1.1.M10 Protokollierung und SYS.1.1.M23 Systemüberwachung. Dabei spielen auch insbesondere Datenschutzaspekte eine Rolle. Die häufigen Sicherheitslücken der meisten Client-Server-Systeme und die Vielzahl von Angriffen, die sich gegen diese Schwächen richten, fordern von den Administratoren, dass diese sich permanent über den Sicherheitsstatus der Systeme und über neue Bedrohungen informieren und rechtzeitig Gegenmaßnahmen einleiten (siehe dazu SYS.1.1.M7 Updates und Patches für Betriebssystem und Anwendungen).

Aussonderung

Ein Server darf nicht einfach ohne Ankündigung abgeschaltet werden. Wenn ein Server außer Betrieb genommen werden soll, dann müssen, wenn es direkte Auswirkungen für die Anwender hat, diese rechtzeitig informiert werden und es muss eine Reihe von Punkten beachtet werden, um Ausfallzeiten und Datenverluste zu verhindern. Diese Punkte sind in SYS.1.1.M25 Geregelte Außerbetriebnahme eines Servers beschrieben.

Bei der Aussonderung eines Servers ist außerdem darauf zu achten, dass keine schützenswerten Informationen mehr auf den Datenträgern vorhanden sind. Dazu genügt es nicht, die Datenträger einfach neu zu formatieren, sondern sie müssen mindestens einmal vollständig überschrieben werden. Es ist zu beachten, dass ein reines logisches Löschen und auch nicht das Neuformatieren der Datenträger mit den Mitteln des installierten Betriebssystems die Daten nicht von den Datenträgern entfernt, so dass sie mit geeigneter Software, oft sogar ohne großen Aufwand, wieder rekonstruiert werden können. Vertiefende Informationen sind in OPS.1.1.8 Löschen und Vernichten zu finden.

Die Aussonderung des Servers muss dokumentiert werden. Bestandsverzeichnisse und Netzpläne müssen aktualisiert werden und sofern sich durch die Aussonderung strukturelle Veränderungen des Informationsverbundes ergeben, sollte auch das Sicherheitskonzept entsprechend angepasst werden.

Notfallvorsorge

Nur eine regelmäßige und umfassende Datensicherung gewährleistet zuverlässig, dass alle gespeicherten Daten auch im Falle von Störungen, Ausfällen der Hardware oder (absichtlichen oder unabsichtlichen) Löschungen weiter verfügbar gemacht werden können. Die notwendigen Anforderungen sind im Baustein OPS.1.1.5 Datensicherung beschrieben.

Neben der Absicherung im laufenden Betrieb spielt jedoch auch die Notfallvorsorge eine wichtige Rolle, da nur so der Schaden im Notfall verringert werden kann. Hinweise zur Notfallvorsorge finden sich im Baustein DER.4 Notfallmanagement. Hierzu gehört auch die Planung des Umgangs mit Sicherheitsvorfällen, die sich auf die Anforderungen des Bausteins DER.2.1 Incident Management abstützen sollte. Einige Hinweise zu besonderen Aspekten, die bei der Notfallvorsorge für einen Server beachtet werden sollten, sind in SYS.1.1.M22 Einbindung in die Notfallvorsorge beschrieben.

Es wird vorausgesetzt, dass der Server in einem Serverraum (siehe Baustein INF.12 Serverraum), einem Serverschrank (siehe Baustein INF.6 Schutzschränke) oder in einem Rechenzentrum (siehe Baustein INF.2 Rechenzentrum) untergebracht ist. Die für die Serverbetriebssysteme umzusetzenden Anforderungen sind den jeweiligen betriebssystemspezifischen Bausteinen zu entnehmen. Dies gilt analog auch für die angeschlossenen Clients. Die Anforderungen des Bausteins OPS.1.1.2 Netz und System-Management bilden in jedem Fall den übergeordneten Rahmen für den Betrieb servergestützter Netze.

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Allgemeiner Server" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

SYS.1.1.M1 Geeignete Aufstellung [Haustechnik]

Ein Server muss grundsätzlich in einem abschließbaren Rechnerraum oder Serverschrank aufgestellt oder eingebaut werden. Dabei ist zu regeln, wer Zutritt zu dem Raum beziehungsweise Zugang auf den Server selbst erhält. Hierfür sind die Anforderungen der Bausteine INF.5 Technikraum, INF.6 Schutzschrank, beziehungsweise Rechenzentrum umzusetzen. Zusätzlich muss gewährleistet werden, dass nur dafür vorgesehene Wechselspeicher an die Server angeschlossen werden können, hierzu sollten die vorhandenen Schnittstellen geeignet geschützt werden.

Schutz von Schnittstellen

Handelsübliche PCs sind heute in der Regel mit einem CD-/DVD-Brenner ausgestattet. Zusätzlich besteht die Möglichkeit, über Schnittstellen externe Speichermedien anzuschließen, die von den meisten Betriebssystemen automatisch erkannt und eingebunden werden. Beispiele sind USB-Speicher, die an die USB-Schnittstelle angeschlossen werden, und Firewire-Festplatten. Außerdem sind in vielen IT-Systemen Kartenleser für Speicherkarten eingebaut. Durch solche Laufwerke für Wechselmedien und externe Datenspeicher ergeben sich folgende potenzielle Sicherheitsprobleme:

- Das IT-System könnte von solchen Laufwerken unkontrolliert gebootet werden.
- Es könnte unkontrolliert Software von solchen Laufwerken eingespielt werden.
- Daten könnten unberechtigt auf Wechselmedien kopiert werden.

Wenn von Wechselmedien gebootet oder Fremdsoftware installiert wird, können nicht nur Sicherheitseinstellungen umgangen werden, sondern das IT-System kann auch mit Schadprogrammen infiziert werden. Diesen Gefahren sollten die Verantwortlichen durch geeignete organisatorische oder technische Sicherheitsmaßnahmen entgegenwirken. Hierfür bieten sich verschiedene Vorgehensweisen an, deren spezifische Vor- und Nachteile im Folgenden kurz dargestellt werden:

- Ausbau von Laufwerken
  Der Ausbau der Laufwerke für Wechselmedien (bzw. der Verzicht bei der Beschaffung) bietet zwar den sichersten Schutz vor den oben genannten Gefährdungen, ist aber meist mit erheblichem Aufwand verbunden. Oft ist ein Ausbau überhaupt nicht möglich, z. B. bei Speicherkartenlesern bei Notebooks. Weiterhin ist zu berücksichtigen, unter Umständen die IT-Systeme nur schwer administriert und gewartet werden können, wenn diese Laufwerke ausgebaut wurden. Diese Lösung sollte in Betracht gezogen werden, wenn besondere Sicherheitsanforderungen bestehen.
- Verschluss von Laufwerken
  Für einige Laufwerksarten gibt es abschließbare Einschubvorrichtungen, mit denen die unkontrollierte Nutzung verhindert werden kann. Bei der Beschaffung sollte sichergestellt werden, dass die Laufwerksschlösser für die vorhandenen Laufwerke geeignet sind und diese nicht beschädigen können. Es muss beachtet werden, dass nicht für alle Laufwerksarten, wie für eingebaute Speicherkartenleser, Schlösser angeboten werden. Außerdem sollte darauf geachtet werden, dass die Schlösser herstellerseitig mit hinreichend vielen unterschiedlichen Schlüsseln angeboten werden. Nachteilig sind die Beschaffungskosten für die Laufwerksschlösser und der Aufwand für die erforderliche Schlüsselverwaltung. Daher ist diese Lösung nur bei höherem Schutzbedarf oder besonderen Sicherheitsanforderungen sinnvoll.
- Deaktivierung im BIOS bzw. Betriebssystem
  Im BIOS bieten die meisten PCs Einstellmöglichkeiten dafür, von welchen Laufwerken gebootet werden kann. In Verbindung mit einem Passwort-Schutz der BIOS-Einstellungen kann dadurch das unkontrollierte Booten von Wechselmedien und mobilen Datenträgern unterbunden werden. Weiterhin können die vorhandenen Laufwerke und Schnittstellen bei modernen Betriebssystemen einzeln deaktiviert werden.Dies erschwert die unberechtigte Nutzung, z. B. die Installation von Fremdsoftware oder das Kopieren auf Wechselmedien. Die Deaktivierung der Laufwerke im BIOS bzw. Betriebssystem hat den Vorteil, dass keine Hardware-Änderungen erforderlich sind. Die entsprechenden Einstellungen im Betriebssystem können gegebenenfalls zentral vorgenommen werden. Damit diese Vorgehensweise wirksam ist, muss sichergestellt sein, dass die Benutzer nicht über die Berechtigungen im Betriebssystem verfügen, um die Laufwerke wieder zu aktivieren.
- Kontrolle der Schnittstellennutzung
  Die Nutzung von Schnittstellen sollte durch entsprechende Rechtevergabe auf Ebene des Betriebssystems oder mit Hilfe von Zusatzprogrammen geregelt werden. Bei einigen dieser Zusatzprogramme zur Absicherung der USB- oder Firewire-Schnittstellen lässt sich festlegen, dass von mobilen Datenträgern nur gelesen werden kann. Alternativ kann überwacht werden, ob Geräte hinzugefügt werden.
- Verschlüsselung
  Es gibt Produkte, die dafür sorgen, dass ausschließlich Zugriffe auf dafür zugelassene mobile Datenträger möglich sind. Eine Lösung ist beispielsweise, dass nur noch mobile Datenträger gelesen und beschrieben werden können, die mit bestimmten kryptographischen Schlüsseln verschlüsselt worden sind. Dies schützt nicht nur vor unbefugtem Zugriff über manipulierte mobile Datenträger, sondern schützt auch die Daten auf den mobilen Datenträgern bei Verlust oder Diebstahl.
- Richtlinien für die Nutzung
  In vielen Fällen dürfen die Benutzer die eingebauten Laufwerke für Wechselmedien oder Speichermedien an externen Schnittstellen durchaus verwenden, die Nutzung ist jedoch durch entsprechende Richtlinien reglementiert. Auf technischer Ebene sollte dann lediglich das Booten von Wechselmedien im BIOS deaktiviert werden. Ausbau, Verschluss oder Deaktivierung der Laufwerke im Betriebssystem kommen nicht infrage.In diesem Fall sollten die Richtlinien für die Nutzung der Laufwerke und Speichermedien so explizit wie möglich definiert werden. Beispielsweise kann ein generelles Verbot ausgesprochen werden, nur das Kopieren öffentlicher Text-Dokumente wird erlaubt. Die Richtlinien müssen allen Benutzern bekannt gemacht und die Einhaltung kontrolliert werden. Die Installation und das Starten von Programmen, die von Wechselmedien eingespielt wurden, sollte untersagt und soweit wie möglich auch technisch unterbunden werden.Diese rein organisatorische Lösung sollte nur dann gewählt werden, wenn die Benutzer hin und wieder oder regelmäßig auf die Laufwerke zugreifen müssen. Anderenfalls sollte der Zugriff, wie oben beschrieben, durch technische Maßnahmen unterbunden werden.Bei der Auswahl einer geeigneten Vorgehensweise müssen immer alle Anschlussmöglichkeiten für mobile Datenträger berücksichtigt werden, aber ebenso auch alle Wege, über Vernetzung Daten auszutauschen, also insbesondere auch E-Mail und Internet-Anbindungen. Wenn das IT-System über eine Verbindung zum Internet verfügt, ist es nicht allein ausreichend, alle Laufwerke für Wechselmedien zu deaktivieren oder auszubauen.

Unabhängig davon, für welche Vorgehensweise sich die Institution entscheidet, ist zu verhindern, dass Inhalte von mobilen Datenträgern automatisch ausgeführt werden, wenn diese angeschlossen werden. Hierzu sind die entsprechenden Autorun- und Autoplay-Funktionen des Betriebssystems zu deaktivieren.

SYS.1.1.M2 Benutzerauthentisierung

Die Identifikations- und Authentikationsmechanismen von IT-Systemen bzw. IT-Anwendungen müssen so gestaltet sein, dass Benutzer eindeutig identifiziert und authentisiert werden. Die Identifikation und Authentisierung muss vor jeder anderen Interaktion zwischen IT-System und Benutzer erfolgen. Weitere Interaktionen dürfen nur möglich sein, nachdem die Benutzer sich erfolgreiche identifiziert und authentisiert haben. Die Authentisierungsinformationen müssen so gespeichert sein, dass nur autorisierte Benutzer darauf Zugriff haben (sie prüfen oder ändern können). Bei jeder Interaktion muss das IT-System die Identität des Benutzers feststellen können.

Es gibt verschiedene Techniken, über die die Authentizität eines Benutzers nachgewiesen werden kann. Die bekanntesten sind:

- PINs (Persönliche Identifikationsnummern)
- Passwörter
- Token wie z. B. Zugangskarten
- Biometrie

Für sicherheitskritische Anwendungsbereiche sollte starke Authentisierung verwendet werden, hierbei werden zwei oder mehr Authentisierungstechniken kombiniert, wie Passwort plus Transaktionsnummern (Einmalpasswörter) oder plus Chipkarte. Daher wird dies auch häufig als Zwei-Faktor-Authentisierung bzw. Mehr-Faktor-Authentisierung bezeichnet. Alle eingesetzten Authentisierungstechniken müssen sich auf dem Stand der Technik befinden.

Passwörter

Werden in einem Client Passwörter zur Authentisierung verwendet, so ist die Sicherheit der Zugangs- und Zugriffsrechteverwaltung des IT-Systems entscheidend davon abhängig, dass die Passwörter korrekt gebraucht werden. Dafür sollte eine Richtlinie zum Passwortgebrauch erstellt und veröffentlicht werden. Außerdem sollten die IT-Benutzer regelmäßig, z.B. bei Team-Meetings, darauf hingewiesen werden.

Wenn Passwörter zur Authentikation eingesetzt werden, sollte das IT-System Mechanismen bieten, die folgende Bedingungen erfüllen:

- Es wird gewährleistet, dass jeder Benutzer individuelle Passwörter benutzt (und diese auch selbst auswählen kann).
- Es wird überprüft, dass alle Passwörter den definierten Vorgaben genügen (z. B. Mindestlänge, keine Trivialpasswörter). Die Prüfung der Passwortgüte sollte individuell regelbar sein. Beispielsweise sollten vorgegeben werden können, dass die Passwörter mindestens ein Sonderzeichen enthalten müssen oder bestimmte Zeichenkombinationen verboten werden.
- Das IT-System generiert Passwörter, die den definierten Vorgaben genügen. Das IT-System muss die so erzeugten Passwörter dem Benutzer anbieten.
- Der Passwortwechsel sollte von den IT-Systemen regelmäßig initiiert werden. Die Lebensdauer eines Passwortes sollte einstellbar sein.
- Die Wiederholung alter Passwörter beim Passwortwechsel sollte vom IT-System verhindert werden (Passwort-Historie).
- Bei der Eingabe sollte das Passwort nicht auf dem Bildschirm angezeigt werden.
- Nach der Installation bzw. der Neueinrichtung von Benutzern sollte das Passwort-System einen Passwort-Wechsel nach der Erst-Anmeldung erzwingen.

Vertiefende Informationen zur Authentisierung sind in ORP.4 Identitäts- und Berechtigungsmanagement zu finden.

SYS.1.1.M3 Restriktive Rechtevergabe

Zugriffsrechte auf Dateien, die auf den Datenträgern des Servers gespeichert sind, müssen restriktiv vergeben werden. Benutzer dürfen nur auf die Dateien ein Zugriffsrecht erhalten, die sie für ihre Aufgabenerfüllung benötigen. Das Zugriffsrecht selbst wiederum wird auf die notwendige Zugangssart beschränkt (siehe dazu "Vergabe von Zugangsberechtigungen"). So ist es zum Beispiel in den seltensten Fällen notwendig, ein Schreibrecht auf Programmdateien zu vergeben.

Meist darf über die Vererbung von Rechten auf Dateien in Unterverzeichnissen zugegriffen werden, wenn ein Zugriffsrecht auf das übergeordnete Verzeichnis bestand. Daraus ergibt sich, dass Zugriffsrechte auf höchster Ebene (Volume-Ebene) nur sehr restriktiv erteilt werden sollten. Insbesondere ist bei der Installation neuer Softwareprodukte die Rechtevergabe einer strengen Kontrolle zu unterwerfen.

Sollte der Speicherplatz des Servers gering ausgelegt sein, kann eine Beschränkung der maximalen Speicherkapazität, die ein Benutzer auf dem Server belegen darf, eingestellt werden.

Vergabe von Zugangsberechtigungen

Zugangsberechtigungen erlauben der betroffenen Person oder einem autorisierten Vertreter, bestimmte IT-Systeme bzw. System-Komponenten und Netze zu nutzen. Zugangsberechtigungen sollten möglichst restriktiv vergeben werden. Diese sind für jede nutzungsberechtigte Person aufgrund ihrer Funktion, unter Beachtung der Funktionstrennung, im einzelnen festzulegen. Entsprechend der Funktion ist der Zugang zum Rechner zu definieren, z. B. Zugang zum Betriebssystem (Systemverwalter) oder Zugang zu einer IT-Anwendung (Anwender). Ergänzend hierzu muss sichergestellt sein, dass personelle und aufgabenbezogene Änderungen unverzüglich berücksichtigt werden.

Der Zugang zu IT-Systemen oder IT-Anwendungen sollte erst nach einer Identifikation (z. B. durch Name, Benutzer-Kennung oder Chipkarte) und Authentisierung (z. B. durch ein Passwort oder über ein Authentisierungstoken) des Nutzungsberechtigten möglich sein und protokolliert werden.

Die Ausgabe bzw. der Entzug von Zugangsmitteln wie Benutzer-Kennungen oder Chipkarten ist zu dokumentieren. Regelungen über die Handhabung von Zugangs- und Authentisierungsmitteln (z. B. Umgang mit Chipkarten, Passworthandhabung) müssen ebenfalls getroffen werden. Alle Zugangsberechtigten müssen auf den korrekten Umgang mit den Zugangsmitteln hingewiesen werden.

Zugangsberechtigungen sollten bei längeren Abwesenheiten von berechtigten Personen vorübergehend gesperrt werden, um Missbrauch zu verhindern, z. B. bei Krankheit oder Urlaub. Dies sollte zumindest bei Personen mit weitreichenden Berechtigungen wie Administratoren erfolgen.

Es ist notwendig, die vorgenannten Festlegungen auf ihre korrekte Einhaltung sporadisch zu kontrollieren.

Administratoren-Kennungen

In vielen komplexen IT-Systemen, z. B. unter Unix oder in einem Netz, gibt es eine Administratorrolle, die keinerlei Beschränkungen unterliegt. Unter Unix ist das der Super-User root, in einem Novell-Netz der SUPERVISOR bzw. admin. Durch fehlende Beschränkungen ist die Gefahr von Fehlern oder Missbrauch besonders hoch.

Um Fehler zu vermeiden, soll unter dem Super-User-Login nur gearbeitet werden, wenn es notwendig ist; andere Arbeiten sollten auch Administratoren nicht unter einer Administrator-Kennung erledigen, sondern über eine personenbezogene Kennung. Insbesondere dürfen keine Programme anderer Benutzer mit Administrator-Rechten aufgerufen werden. Sollten für bestimmte Tätigkeiten dennoch administrative Rechte erforderlich sein, wird empfohlen, ein rollenbasiertes Administrationskonzept zu erstellen und umzusetzen (siehe SYS.1.1.M14 Erstellung eines Benutzer- und Administrationskonzepts). Ferner sollte die routinemäßige Systemverwaltung (zum Beispiel Backup, Einrichten eines neuen Benutzers) nur menügesteuert durchgeführt werden können.

Durch Aufgabenteilung, Regelungen und Absprache ist sicherzustellen, dass Administratoren keine inkonsistenten oder unvollständigen Eingriffe vornehmen. Zum Beispiel darf eine Datei nicht gleichzeitig von mehreren Administratoren editiert und verändert werden, da dann nur die zuletzt gespeicherte Version erhalten bleibt.

Für alle Administratoren sind zusätzliche Benutzer-Kennungen einzurichten, die nur über die eingeschränkten Rechte verfügen, die die Administratoren zur Aufgabenerfüllung außerhalb der Administration benötigen. Für Arbeiten, die nicht der Administration dienen, dürfen die Administratoren ausschließlich diese zusätzlichen Benutzer-Kennungen verwenden.

SYS.1.1.M4 Rollentrennung

Grundsätzlich kann zwischen Kennungen für Benutzer- und Administratoren unterschieden werden. Nur Administratoren verwalten die IT-Systeme, während normale Benutzerkennungen nur die Rechte besitzen, um ihre arbeitsplatzspezifischen Aufgaben erfüllen zu können. Normale Benutzerkennungen dürfen keine Administrationsrechte besitzen, damit das Betriebssystem und die Konfiguration der Clients vor versehentlicher, fahrlässiger oder vorsätzlicher Modifikation durch die Benutzer geschützt werden.

Falls Benutzer nur bestimmte administrative Aufgaben wahrnehmen müssen, ist es oftmals nicht erforderlich, ihnen alle mit einem eigenen Login verbundenen Rechte oder sogar Systemadministrator-Rechte zu geben. Beispiele sind bestimmte Tätigkeiten der routinemäßigen Systemverwaltung, wie die Erstellung von Backups oder das Einrichten eines neuen Benutzers, die mit einem Programm menügesteuert durchgeführt werden, oder Tätigkeiten, für die ein Benutzer nur ein einzelnes Anwendungsprogramm benötigt. Insbesondere bei Aushilfskräften und externen Dienstleistern sollte darauf geachtet werden, dass diese nur die Dienste verwenden und nur auf die Daten zugreifen dürfen, die sie tatsächlich benötigen. Wenn ihre Tätigkeit beendet ist, sollten deren Accounts deaktiviert und alle Zugangsberechtigungen entfernt werden.

Für diese Benutzer sollte eine eingeschränkte Benutzerumgebung geschaffen werden. Sie kann zum Beispiel unter Unix durch eine Restricted Shell (rsh) und eine Beschränkung der Zugriffspfade mit dem Unix-Kommando chroot realisiert werden. Eine weitere Möglichkeit besteht darin, einzelne Anwendungsprogramme, wie Web-Browser, im sogenannten Kiosk-Modus auszuführen, so dass nur ein beschränkter Zugriff besteht.

Werden an Benutzerkennungen besonders weitgehende Rechte vergeben, so sollte dies möglichst restriktiv erfolgen. Hierbei sollte zum einem der Kreis der privilegierten Benutzer möglichst eingeschränkt werden und zum anderen nur die für die Durchführung der Arbeit benötigten Rechte vergeben werden. Für alle Aufgaben, die ohne erweiterte Rechte durchgeführt werden können, sollten auch privilegierte Benutzer unter Kennungen mit Standard-Rechten arbeiten.

SYS.1.1.M5 Schutz der Administrationsschnittstellen

Es gibt unterschiedliche Zugangssmöglichkeiten, um Server zu administrieren. Abhängig von der genutzten Zugangsart müssen eine Reihe von Sicherheitsvorkehrungen getroffen werden. Bei größeren Netzen ist es empfehlenswert, auch die Server in ein zentrales Netzmanagement-System einzubinden, da sonst eine sichere und effiziente Administration kaum gewährleistet werden kann. Die zur Administration verwendeten Methoden müssen in der Sicherheitsrichtlinie festgelegt werden und die Administration darf nur entsprechend der Sicherheitsrichtlinie durchgeführt werden.

Allgemein ist es wichtig, einen Überblick darüber zu erhalten, welcher Teil der Administration eines Servers normalerweise

- lokal über die Konsole,
- remote über das Netz, aber unter Nutzung der Standardmechanismen des Betriebssystems, oder
- über ein zentrales netzbasiertes Administrationswerkzeug

durchgeführt werden soll. Es wird empfohlen, für die verschiedenen Nutzungsarten eine Übersicht zu erstellen, welche Administrationstätigkeiten auf welchem Weg durchgeführt werden können. Insbesondere ist es wichtig festzuhalten, ob bestimmte Tätigkeiten auf einem bestimmten Weg normalerweise nicht durchgeführt werden dürfen.

- Lokale Administration
  Ein Server sollte prinzipiell in einem Serverraum oder zumindest einem abschließbaren Serverschrank aufgestellt sein. Für den Teil der Administration, der trotzdem teilweise lokal über die Konsole erfolgen soll oder muss, müssen entsprechende Vorgaben dafür gemacht werden, wer Zugang zur Konsole erhält, welche Art der Authentisierung für den lokalen Zugang genutzt werden darf und welche anderen Vorgaben berücksichtigt werden müssen.
- Remote-Administration
  Meist wird ein Server nicht lokal an der Konsole sondern von einem Arbeitsplatzrechner aus über das Netz administriert. Um zu verhindern, dass dabei Authentisierungsinformationen der Administratoren und Konfigurationsdaten der Server abgehört oder gar von einem Angreifer manipuliert werden, sollte die Administration nur über sichere Protokolle (beispielsweise nicht über Telnet, sondern über SSH, nicht über HTTP, sondern über HTTPS) erfolgen. Alternativ kann ein eigenes Administrationsnetz eingerichtet werden, das vom dem restlichen Netz getrennt ist.Eine ungesicherte Remote-Administration über externe (unsichere) Netze hinweg darf in keinem Fall erfolgen. Dies muss bereits bei der Festlegung der Sicherheitsrichtlinie berücksichtigt werden. Auch im internen Netz sollten, soweit möglich, keine unsicheren Protokolle verwendet werden.
- Administration über ein zentrales Managementsystem
  Falls für die Administration des Servers ein zentrales Managementsystem genutzt werden soll, so sollten für diesen Zugangsweg analoge Vorüberlegungen angestellt werden, wie für die Remote-Administration. Zusätzlich ist es wichtig, dass das zentrale Managementsystem selbst entsprechend sicher konfiguriert und administriert wird.

Sichere Authentisierung

IT-Systeme aller Art sollten grundsätzlich sicherstellen, dass sich alle Benutzer, die darauf zugreifen möchten, authentisieren müssen. Nur so kann verhindert werden, dass unautorisierte Personen Zugang auf die Dienste erlangen, die das System anbietet, oder auf die Daten, die auf dem System gespeichert sind.

In der Regel werden Server über eine Netzverbindung administriert. Die Informationen, die für eine netzbasierte Authentisierung benötigt werden, müssen hierfür über ein LAN oder WAN übertragen werden. Daher ist es zwingend erforderlich, dass diese Informationen nicht mitgelesen oder verändert werden können.

Außerdem muss sichergestellt werden, dass ein Angreifer sich nicht anmelden kann, indem er aufgezeichnete Anmeldeinformationen wieder einspielt. Daher müssen die Anmeldeinformationen, die für die Authentisierung zwischen Server und Client ausgetauscht werden, verschlüsselt und zusätzlich, beispielsweise mit Challenge-Response-Verfahren, dynamisiert werden.

Nachdem die Authentisierung erfolgreich abgelaufen ist, muss das System sicher stellen, dass die Benutzer nur auf solche Dienste und Daten Zugriff erhalten, für die sie entsprechende Berechtigungen besitzen.

Wenn die Gefahr des Abhörens von Leitungen zu Terminals besteht, sollten Administratoren nur an der Konsole arbeiten, damit keine Passwörter abgehört werden können. Bei der Administration von Unix-Systemen kann eine verschlüsselte Kommunikation beispielsweise mit dem Protokoll Secure Shell erfolgen. Hiermit ist eine gesicherte Administration von entfernten Arbeitsstationen aus möglich .

SYS.1.1.M6 Deaktivierung nicht benötigter Dienste und Kennungen

Die Standardinstallation eines Betriebssystems enthält oft eine Reihe von Programmen und Diensten, die normalerweise nicht benötigt werden und die gerade deswegen eine Quelle von Sicherheitslücken sein können. Dies gilt insbesondere für Netzdienste. Nach der Installation muss deswegen überprüft werden, welche Dienste auf dem System installiert und aktiviert sind. Nicht benötigte Dienste müssen deaktiviert oder ganz deinstalliert werden.

Die Überprüfung auf laufende Dienste kann einerseits lokal mit den Mitteln des installierten Betriebssystems und bei Netzdiensten andererseits von außen durch einen Portscan von einem anderen System aus erfolgen. Durch eine Kombination beider Methoden kann weitgehend ausgeschlossen werden, dass das System noch weitere ungewollte Netzdienste anbietet.

Gesichertes Login

Es sollte ein Login-Programm verwendet bzw. Optionen aktiviert werden, so dass die folgenden Maßnahmen durchgeführt werden können:

- Jeder Benutzer muss eine eigene Kennung und ein eigenes Passwort erhalten. Es darf kein Zugang ohne Kennung oder Passwort möglich sein. Als Passwort-Ersatz kann die Authentisierung des Benutzers auch über elektronische Signaturen, Pass-Tickets oder Ähnliches erfolgen.
- Die Anzahl erfolgloser Login-Versuche kann beschränkt werden. Nach jedem erfolglosen Login-Versuch vergrößert sich die Wartezeit bis zur nächsten Login-Aufforderung. Nach einer bestimmten Anzahl von Fehlversuchen wird die betroffene Benutzer-Kennung und / oder das Terminal gesperrt. Dabei ist zu bedenken, dass dadurch nicht die Administratoren ausgesperrt werden dürfen, es muss an der Konsole eine Zugangsmöglichkeit für die Administration offen bleiben.
- Der Zeitpunkt des letzten erfolgreichen Logins wird dem Benutzer beim Login gemeldet.
- Erfolglose Login-Versuche werden dem Benutzer beim Login gemeldet. Eventuell sollte diese Meldung bei mehreren darauf folgenden Anmeldungen wiederholt werden.
- Der Zeitpunkt des letzten Logouts wird dem Benutzer beim Login gemeldet. Hierbei wird zwischen Logouts zu einem interaktiven Login und solchen zu einem nicht-interaktiven Login (Logout von Hintergrundprozessen) unterschieden.
- Für das Login über Netze, in denen Passwörter unverschlüsselt übertragen werden, empfiehlt sich die zusätzliche Verwendung von Einmalpasswörtern.

Sperren und Löschen nicht benötigter Accounts und Terminals

Wenn keine gravierenden Gründe dagegen sprechen, sollten Accounts, die über einen längeren Zeitraum nicht benutzt werden, gesperrt und später gelöscht werden. Wenn beim Löschen von Accounts Dateien übrig bleiben, die keinem existierenden Benutzereintrag mehr zugeordnet sind, besteht die Gefahr, dass diese Dateien später eingerichteten Benutzern unberechtigt zugeordnet werden.

Bevor die Heimatverzeichnisse der Benutzer gelöscht werden, sollten diese vorher gesichert werden. Bei der Sperrung bzw. auf jeden Fall vor dem Löschen eines Accounts sollte der betroffene Benutzer informiert werden. Beim Löschen von Accounts ist darauf zu achten, dass auch die Dateien des Benutzers gefunden werden, die nicht in seinem Heimatverzeichnis liegen. Solche Dateien müssen gelöscht oder anderen Benutzern zugeordnet werden. Weiterhin ist darauf zu achten, dass laufende Prozesse und noch anstehende Aufträge gelöscht werden, z. B. unter Unix in der crontab.

Ebenso sollten Terminals, die über einen längeren Zeitraum nicht benutzt werden, gesperrt und später entfernt werden.

Wenn ein neu einzurichtender Benutzer seinen Account nur für einen begrenzten Zeitraum benötigt, sollte dieser nur befristet eingerichtet werden. Es kann vorteilhaft sein, Accounts grundsätzlich nur befristet einzurichten und in regelmäßigen Abständen (z. B. jährlich) bei Bedarf zu verlängern.

Quotas

Auch wenn bei der Beschaffung eines IT-Systems darauf geachtet wurde, dass dieses genügend Speicherplatz bietet, wird in vielen Fällen bei längerer Nutzung der Speicherplatz früher oder später knapp. Auf IT-Systemen, die von verschiedenen Benutzern genutzt werden, müssen die vorhandenen Ressourcen daher so aufgeteilt werden, dass alle Benutzer möglichst optimal arbeiten können.

Häufig lässt sich das Phänomen beobachten, dass die Benutzer mehr Speicherplatz haben möchten, als ihnen zur Verfügung steht. Neben dem ständig wachsenden Speicherplatzbedarf von Anwendungen ist ein anderer Grund hierfür, dass sich viele Benutzer nur ungern von alten und unbenötigten Dateien trennen. Werden keine Regelungen zur Speicherplatz-Begrenzung und zur Archivierung getroffen, besteht die Gefahr, dass Speicherplatz für große Mengen an Altdaten verschwendet wird oder die Benutzerverzeichnisse überlaufen.

Eine einfache Lösung wäre es, bei steigender Nachfrage grundsätzlich immer mehr Speicherplatz als benötigt bereitzustellen. Dies ist allerdings in der Praxis nicht immer machbar. Auch wenn die Anwender für eine sparsame Datenhaltung sensibilisiert werden, wird jede unbenötigte Datei dennoch oft als wichtig angesehen.

Für Benutzer oder Benutzergruppen, aber auch für Anwendungen kann durch Disk Quotas ein Speichervolumen festgelegt werden, das nicht überschritten werden darf. Auf Servern und allen IT-Systemen, die von mehreren Benutzern bzw. Anwendungen konkurrierend benutzt werden, sollte daher der Speicherplatz für die einzelnen Benutzer, aber auch für Anwendungen durch Disk Quotas beschränkt werden. Hierzu gehören Server (z. B. Datei-, Web- und Mailserver) und Clients mit mehreren Benutzerkennungen. Für Clients, auf denen die Daten- von der Systempartition getrennt ist und die nur von einem Benutzer genutzt werden, kann auf eine Disk Quota verzichtet werden.

Dabei ist die Wahl des Quota-Volumens wichtig. Sollen alle Benutzer das gleiche Quota-Volumen erhalten, kann das erforderliche Volumen errechnet werden, indem der zu nutzende Speicherplatz durch die Anzahl der Benutzer dividiert wird. Zusätzlich sollte aber eine Speicherplatz-Reserve eingeplant werden. Problematisch ist die Wahl einer zu kleinen Disk Quota. Steht den Benutzern zu wenig Speicherplatz zur Verfügung, könnten sie versuchen, die Informationen außerhalb der vorgesehenen Verzeichnisse abzulegen, um die Restriktionen zu umgehen. Hierfür werden dann häufig Speicherorte verwendet, die dafür nicht geeignet sind, z. B. temporäre Verzeichnisse oder andere für alle Benutzer beschreibbare Verzeichnisse. Wenn der Speicherplatz auf Dateiservern zu knapp bemessen ist, weichen Benutzer oft auf lokale Datenträger aus. Dies verstößt in vielen Fällen gegen die Regelungen und kann beispielsweise dazu führen, dass die Dateien nicht in die zentrale Datensicherung (Backup) einbezogen werden.

Es sollte einerseits festgelegt werden, welche Informationen wo abgespeichert werden sollen und auch, wie viele Versionen einer Datei wie lange auf dem Produktivsystem gespeichert werden sollen.

Datenbestände aus abgeschlossenen Projekten sollten geordnet archiviert und nicht "für alle Fälle" auf den Produktivsystemen vorrätig gehalten werden. Andererseits sollte festgelegt werden, wie viel Speicherplatz den verschiedenen Benutzergruppen und Anwendungen zur Verfügung gestellt wird. Zusätzlich sollte eine Reserve eingeplant werden. Es muss auch festgelegt werden, wie den Benutzern bei Bedarf ein höheres Speichervolumen zugeteilt werden kann. Die festgesetzten Werte müssen dokumentiert werden. Außerdem müssen sie regelmäßig überprüft und aktualisiert werden.

Wurde die Größe der Disk Quota bestimmt, sollte überlegt werden, ob und wie auf einen höheren Bedarf an Speicherplatz reagiert werden soll. Diese Entscheidung wird durch die Auswahl eines Quota-Typs beeinflusst. Bei Hard Quotas werden feste Obergrenzen gesetzt, so dass die Benutzer nicht die Möglichkeit haben, mehr als das ihnen zugewiesene Speicherkontingent zu nutzen. Eine Soft Quota hingegen ermöglicht es den Benutzern, für eine festgelegte Zeitspanne und bis zu einer festgelegten Grenze die Disk Quota zu überschreiten. Wird die Disk Quota überschritten, muss mindestens der Benutzer hierüber informiert werden, beispielsweise per E-Mail. Es sollte überlegt werden, ebenfalls den IT-Betrieb zu benachrichtigen, damit er auf eventuell eintretende Probleme reagieren kann. Zusätzlich muss festgelegt werden, ob und wie einzelnen Benutzern zusätzlicher Speicherplatz zugeteilt werden kann. Dies sollte ein geregeltes und nachvollziehbares Verfahren sein. Disk Quotas sollten nicht "auf Zuruf" erhöht werden.

Bei vielen gängigen Betriebssystemen werden Hilfsmittel mitgeliefert, um Disk Quotas einzurichten. Es sollte aber geprüft werden, ob zusätzliche Software zur Einrichtung und Verwaltung einer Disk Quota benötigt wird.

SYS.1.1.M7 Updates und Patches für Firmware, Betriebssystem und Anwendungen

Häufig werden Fehler in Produkten bekannt, die dazu führen können, dass die Informationssicherheit des Informationsverbundes, wo diese betrieben werden, beeinträchtigt wird. Entsprechende Fehler können Hardware, Firmware, Betriebssysteme und Anwendungen betreffen. Diese Schwachstellen müssen so schnell wie möglich behoben werden, damit sie nicht durch interne oder externe Angreifer ausgenutzt werden können. Dies ist ganz besonders wichtig, wenn die betreffenden Systeme mit dem Internet verbunden sind. Die Hersteller von Betriebssystem- oder Software-Komponenten veröffentlichen in der Regel Patches oder Updates, die auf dem jeweiligen IT-System installiert werden müssen, um den oder die Fehler zu beheben.

Die Systemadministratoren sollten sich daher regelmäßig über bekannt gewordene Schwachstellen informieren.

Wichtig ist, dass Patches und Updates, wie jede andere Software, nur aus vertrauenswürdigen Quellen bezogen werden dürfen. Für jedes eingesetzte System oder Softwareprodukt muss bekannt sein, wo Sicherheitsupdates und Patches erhältlich sind. Außerdem ist es wichtig, dass Integrität und Authentizität der bereits installierten Produkte oder der einzuspielenden Sicherheitsupdates und Patches überprüft werden (siehe Abschnitt "Sicherstellung der Integrität und Authentizität von Softwarepaketen"), bevor ein Update oder Patch installiert wird. Vor der Installation sollten sie außerdem mit Hilfe eines Computer-Virenschutzprogramms geprüft werden. Dies sollte auch bei solchen Paketen gemacht werden, deren Integrität und Authentizität verifiziert wurde.

Sicherheitsupdates oder Patches dürfen jedoch nicht voreilig eingespielt werden, sondern müssen vor dem Einspielen getestet werden. Für diese Tests sollten stets aktuelle, auf die Systemumgebung abgestimmte Testpläne oder automatisierte Tests genutzt werden, um ein einheitliches, aussagekräftiges Ergebnis zu erzielen. Falls sich ein Konflikt mit anderen kritischen Komponenten oder Programmen herausstellt, kann ein solches Update sonst zu einem Ausfall des Systems führen. Nötigenfalls muss ein betroffenes System so lange durch andere Maßnahmen geschützt werden, bis die Tests abgeschlossen sind. Es sollte gewährleistet werden, dass Updates, die durch automatische Update-Mechanismen eingespielt werden, ebenfalls getestet werden.

Vor der Installation eines Updates oder Patches sollte stets eine Datensicherung des Systems erstellt werden, die es ermöglicht, den Originalzustand wieder herzustellen, falls Probleme auftreten. Dies gilt insbesondere dann, wenn ausführliche Tests aus Zeitgründen oder mangels eines geeigneten Testsystems nicht durchgeführt werden können.

In jedem Fall muss dokumentiert werden, wann, von wem und aus welchem Anlass Patches und Updates eingespielt wurden. Aus der Dokumentation muss sich der aktuelle Patchlevel des Systems jederzeit schnell ermitteln lassen, um beim Bekanntwerden von Schwachstellen schnell Klarheit darüber zu erhalten, ob das System dadurch gefährdet ist.

Falls festgestellt wird, dass ein Sicherheitsupdate oder Patch mit einer anderen wichtigen Komponente oder einem Programm inkompatibel ist oder Probleme verursacht, so muss sorgfältig überlegt werden, wie weiter vorgegangen wird. Wird entschieden, dass auf Grund der aufgetretenen Probleme ein Patch nicht installiert wird, so ist diese Entscheidung auf jeden Fall zu dokumentieren. Außerdem muss in diesem Fall klar beschrieben sein, welche Maßnahmen ersatzweise ergriffen wurden, um ein Ausnutzen der Schwachstelle zu verhindern. Eine solche Entscheidung darf nicht von den Administratoren alleine getroffen werden, sondern sie muss mit den Vorgesetzten und dem ISB abgestimmt sein.

Sicherstellung der Integrität und Authentizität von Softwarepaketen

Durch unvorsichtiges Ausführen von Programmen, die aus "unsicheren" Quellen stammen, kann beträchtlicher Schaden entstehen. Schadsoftware (so genannte Malware) kann beispielsweise Programme zum Ausspähen von Passwörtern, Trojanische Pferde oder Backdoors auf einem Computer installieren, oder ganz einfach Daten beschädigen oder löschen.

Typische Quellen für solche Schadsoftware sind beispielsweise Programme, die sich als Bildschirmschoner, Virenscanner oder sonstige Hilfsprogramme ausgeben, und an E-Mails angehängt sind. Häufig werden diese unter gefälschten Absenderadressen an sehr viele Empfänger verschickt. Oft werden die Programme aus dem Internet heruntergeladen und ohne Überprüfung installiert.

Selbst wenn ansonsten keine Verschlüsselungs- oder Signaturtechniken eingesetzt werden, sollte die Nutzung in dem Umfang, wie er in dieser Maßnahme beschrieben wird, in Erwägung gezogen werden.

Software sollte grundsätzlich nur aus bekannten Quellen installiert werden, besonders dann, wenn sie nicht auf Datenträgern geliefert, sondern beispielsweise aus dem Internet heruntergeladen wurde. Dies gilt besonders für Updates oder Patches, die normalerweise nicht mehr auf Datenträgern ausgeliefert werden. Die meisten Hersteller und Distributoren bieten zu diesem Zweck Prüfsummen an, die zumindest eine Prüfung der Integrität eines Paketes erlauben. Die Prüfsummen werden dabei meist auf den Webseiten der Hersteller veröffentlicht oder auch per E-Mail verschickt. Um die Integrität eines heruntergeladenen Programms oder einer Archivdatei zu verifizieren, wird dann die veröffentlichte Prüfsumme mit einer von einem entsprechenden Programm lokal erzeugten Prüfsumme verglichen.

Falls zu einem Softwarepaket Prüfsummen angeboten werden, so sollten diese vor der Installation des Paketes überprüft werden.

Eine Überprüfung der Authentizität kann mit Prüfsummen jedoch nicht erfolgen. Daher werden in vielen Fällen für Programme oder Pakete digitale Signaturen angeboten. Die zur Überprüfung der Signatur benötigten öffentlichen Schlüssel sind wiederum meist auf den Webseiten des Herstellers oder von Public-Key-Servern verfügbar. Häufig werden die Prüfsummen mit einem der Programme PGP oder GnuPG erzeugt.

Ergibt die Prüfung, dass es sich um eine gültige Signatur des jeweiligen Herstellers handelt, so resultiert daraus ein deutlich höherer Grad an Vertrauenswürdigkeit für das Paket, als lediglich durch das Vorhandensein einer Prüfsumme.

Manchmal führen selbst die eingebauten Software-Updatemechanismen des jeweiligen Betriebssystems oder der Anwendungssoftware keine Prüfsummenvergleiche durch. Wenn möglich, sollte allerdings bei jedem Softwarepaket vor dem Einspielen ein Prüfsummencheck durchgeführt werden.

Ferner sind nicht alle Prüfsummenvergleiche ohne Mitwirkung der Anwender durchführbar, da die hierfür erforderlichen Checksummen, Signaturen oder Zertifikate von den Herstellern nicht auf eine einheitliche Weise bereitgestellt werden. Daher ist häufig eine manuelle Verifikation auf den Herstellerseiten oder die Anpassung der URLs in der Patch- und Änderungssoftware nötig.

Falls zu einem Softwarepaket digitale Signaturen verfügbar sind, sollten diese auf jeden Fall vor der Installation des Pakets überprüft werden.

Ein prinzipielles Problem bei der Verwendung digitaler Signaturen stellt die Verifikation der Authentizität des verwendeten Schlüssels selbst dar. Trägt der öffentliche Schlüssel keine Signatur einer bekannten vertrauenswürdigen Person oder Organisation (etwa eines Trustcenters), so bieten die mit dem entsprechenden privaten Schlüssel erzeugten Signaturen keine wirkliche Sicherheit, dass das Softwarepaket tatsächlich vom Entwickler, Hersteller oder Distributor stammt. Daher sollten die öffentlichen Schlüssel, sofern sie nicht zertifiziert sind, möglichst aus einer anderen Quelle als das Softwarepaket selbst bezogen werden, beispielsweise von einer CD-ROM des Herstellers, von einem anderen Spiegelserver, auf dem das Paket ebenfalls heruntergeladen werden kann, oder von einem Public Key Server.

Zur Überprüfung von Prüfsummen und digitalen Signaturen müssen die entsprechenden Programme lokal vorhanden sein. Die Administratoren sollten über die Bedeutung und Aussagekraft von Prüfsummen und digitalen Signaturen informiert sein. Außerdem müssen die Administratoren genügend Zeit haben, die entsprechenden Programme im Arbeitsalltag einzusetzen und sich mit der Bedienung vertraut zu machen.

Von einem Bezug von Patches und Änderungen per E-Mail ist aus verschiedenen Gründen abzuraten. Die Herkunft von E-Mails ist ohne Einsatz zusätzlicher Sicherheitsmechanismen schwer festzustellen und die Empfängeradressen in den Institutionen sind oft Verteilerlisten, deren Adresse leicht zu erraten ist. Patches und Änderungen können außerdem mittlerweile sehr umfangreich sein. Viele Unternehmen und Behörden haben die Größe von E-Mail-Anhängen beschränkt und verbieten unter Umständen zudem die Annahme ausführbarer Anhänge. Ferner werden durch die großen Datenmengen die E-Mail-Systeme unnötig belastet. Daher kann eine rechtzeitige Verfügbarkeit der Software-Änderungen, welche besonders bei Sicherheitspatches kritisch sein kann, via E-Mail nicht ausreichend gewährleistet werden.

Des Weiteren bieten einige Hersteller an, Änderungen und Patches dem Kunden direkt auf Datenträgern zuzusenden. Auch in diesem Fall sollten die Patches und Änderungen möglichst anhand von Prüfsummen oder digitalen Signaturen verifiziert werden, denn Absender-Angaben auf Postsendungen und Hersteller-Logos auf CDs und DVDs lassen sich leicht fälschen.

Ein weiterer Aspekt zur Prüfung der Echtheit der Aktualisierung können vom Hersteller veröffentlichte Nachrichten auf seiner Webseite, per Newsletter oder über ähnliche Kanäle sein. Einige Hersteller haben Zyklen und Zeitpunkte etabliert, zu denen in der Regel systematisch Informationen über Änderungen veröffentlicht werden.

SYS.1.1.M8 Regelmäßige Datensicherung

Nur eine regelmäßige und umfassende Datensicherung gewährleistet zuverlässig, dass alle gespeicherten Daten auch im Falle von Störungen, Auswirkungen von Schadsoftware, Ausfällen der Hardware oder (absichtlichen oder unabsichtlichen) Löschungen weiter verfügbar gemacht werden können. Die notwendigen Anforderungen sind im Baustein OPS 1.1.5 Datensicherung beschrieben.

SYS.1.1.M9 Einsatz von Viren-Schutzprogrammen

Zum Schutz vor Schadprogrammen können unterschiedliche Wirkprinzipien genutzt werden. Programme, die IT-Systeme nach sämtlichen bekannten Schadprogrammen durchsuchen, haben sich in der Vergangenheit als wirksames Mittel in der Schadprogramm-Prävention erwiesen. Entsprechend der in OPS1.1.4 Schutz vor Schadprogrammen beschriebenen Anforderungen sollten daher Viren-Schutzprogramme eingesetzt werden.

SYS.1.1.M10 Protokollierung

Die am Server mögliche Protokollierung ist in einem sinnvollen Umfang zu aktivieren. In regelmäßigen Abständen muss der IT-Betrieb die Protokolldateien der Server überprüfen. Es sollten alle sicherheitsrelevanten Ereignisse protokolliert werden. Dabei sind insbesondere folgende Vorkommnisse von Interesse:

- falsche Passworteingabe für eine Benutzer-Kennung bis hin zur Sperrung der Benutzer-Kennung bei Erreichen der Fehlversuchsgrenze,
- Versuche von unberechtigten Zugriffen,
- Stromausfall,
- Daten zur Netzauslastung und -überlastung.

Wie viele Ereignisse darüber hinaus protokolliert werden, hängt unter anderem vom Schutzbedarf der jeweiligen IT-Systeme ab. Je höher deren Schutzbedarf ist, desto mehr sollte protokolliert werden.

Da die Protokoll-Dateien mit der Zeit sehr umfangreich werden können, sollten die Auswertungsintervalle so kurz gewählt werden, dass eine sinnvolle Auswertung möglich ist. Um eine sinnvolle Auswertung zu ermöglichen, sollte jeder Protokoll-Eintrag Benutzer-Kennung bzw. Prozessnummer, Kennzeichnung des Endgeräts, Datum und Uhrzeit enthalten.

Es ist zu prüfen, welche gesetzlichen oder vertraglichen Aufbewahrungsfristen für Protokoll-Dateien beachtet werden müssen. Um die Nachvollziehbarkeit von Aktionen zu gewährleisten, kann eine Mindestspeicherdauer vorgeschrieben sein, aus Datenschutzgründen kann es auch eine Löschungspflicht geben.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Allgemeiner Server".

SYS.1.1.M11 Festlegung einer Sicherheitsrichtlinie für Server

Die Sicherheitsvorgaben für jeden Server ergeben sich aus der organisationsweiten Sicherheitsrichtlinie. Ausgehend von der allgemeinen Richtlinie müssen die Anforderungen für den gegebenen Kontext konkretisiert werden und in einer Sicherheitsrichtlinie für den Server oder eine Gruppe von Servern zusammengefasst werden. In diesem Zusammenhang ist zu prüfen, ob neben der organisationsweiten Sicherheitsleitlinie weitere übergeordnete Vorgaben wie IT-Richtlinien, Passwortrichtlinien oder Vorgaben zur Internetnutzung zu berücksichtigen sind.

Die Sicherheitsrichtlinie muss allen Personen und Gruppen, die an der Beschaffung und dem Betrieb der Server beteiligt sind, bekannt sein und Grundlage für deren Arbeit sein. Wie bei allen Richtlinien sind ihre Inhalte und ihre Umsetzung im Rahmen einer übergeordneten Revision regelmäßig zu prüfen.

Die Sicherheitsrichtlinie sollte das generell zu erreichende Sicherheitsniveau spezifizieren und grundlegende Festlegungen zum Betrieb des Servers treffen. Zur Verbesserung der Übersichtlichkeit kann es sinnvoll sein, für verschiedene Einsatzgebiete gesonderte Sicherheitsrichtlinien zu entwickeln.

Als erstes sollte die allgemeine Konfigurations- und Administrationsstrategie ("Liberal" oder "Restriktiv") festgelegt werden, da die weiteren Entscheidungen von dieser Festlegung wesentlich abhängen.

Für Server, die lediglich Daten mit normalem Schutzbedarf speichern und verarbeiten, kann eine relativ liberale Strategie gewählt werden, was in vielen Fällen die Konfiguration und Administration vereinfacht. Generell ist es aber auch in diesen Fällen empfehlenswert, die Strategie nur "so liberal wie nötig" auszulegen.

Bei einem Server, auf dem Daten mit hohem Schutzbedarf gespeichert oder verarbeitet werden, wird grundsätzlich eine restriktive Strategie empfohlen. Für Server mit besonderem Schutzbedarf bezüglich eines der drei Grundwerte sollte unbedingt eine restriktive Konfigurations- und Administrationsstrategie umgesetzt werden.

Nachfolgend sind einige Punkte aufgeführt, die berücksichtigt werden sollten:

- Regelungen zur physikalischen Zugangsskontrolle: Ein Server sollte grundsätzlich in einem abschließbaren Rechnerraum oder Serverschrank aufgestellt oder eingebaut werden. Dabei ist zu regeln, wer Zutritt zu dem Raum beziehungsweise Zugang auf den Server selbst erhält.
- Entscheidung, ob der Server virtualisiert werden soll (siehe SYS.1.5. Server-Virtualisierung).
- Regelungen für die Arbeit der Administratoren und Revisoren:
  - Nach welchem Schema werden Administrationsrechte vergeben? Welcher Administrator darf welche Rechte ausüben und wie erlangt er diese Rechte?
  - Über welche Zugangswege dürfen Administratoren und Revisoren auf die Systeme zugreifen (beispielsweise nur lokal an der Konsole, über ein eigenes Administrationsnetz oder über verschlüsselte Verbindungen)?
  - Welche Vorgänge müssen dokumentiert werden? In welcher Form wird die Dokumentation erstellt und gepflegt?
  - Gilt für bestimmte Änderungen ein Vier-Augen-Prinzip?
- Vorgaben für die Installation und Grundkonfiguration
  - Welche Installationsmedien werden zur Installation verwendet?
  - Soll ein zentraler Authentisierungsdienst genutzt werden oder erfolgt die Benutzerverwaltung und -authentisierung nur lokal?
  - Regelungen zur Benutzer- und Rollenverwaltung, Berechtigungsstrukturen (Ablauf und Methoden der Authentisierung und Autorisierung, Berechtigung zu Installation, Update, Konfigurationsänderungen etc.). Nach Möglichkeit sollte ein Rollenkonzept für die Administration erarbeitet werden.
  - Vorgaben für die zu installierenden Softwarepakete.
- Falls bei der Planung für den Server festgelegt wurde, dass Teile des Dateisystems verschlüsselt werden sollen, so ist es empfehlenswert, an dieser Stelle festzulegen, wie dies zu geschehen hat:
  - Welche Teile des Dateisystems sollen verschlüsselt werden?
  - Welcher Mechanismus zur Einbindung des verschlüsselten Dateisystems soll verwendet werden?
  - Welche Kryptoalgorithmen und Schlüssellängen sollen verwendet werden?
  - Welche Daten sollen in den verschlüsselten Dateisystemen gespeichert werden?
  - Wie werden die verschlüsselten Dateisysteme in das Backup einbezogen?
- Regelungen zu Erstellung und Pflege von Dokumentation
- Vorgaben für den sicheren Betrieb
  - Welcher Benutzerkreis darf sich lokal auf dem System anmelden?
  - Welche Benutzer erhalten Zugang über das Netz? Welche Protokolle dürfen verwendet werden?
  - Auf welche Ressourcen dürfen die Benutzer zugreifen?
- Vorgaben für die Passwortnutzung (Passwortregeln, Regeln und Situationen für Passwortänderungen, gegebenenfalls Hinterlegung von Passwörtern)
  - Wer darf das System herunterfahren?
- Netzkommunikation und -dienste
  - Soll ein lokaler Paketfilter aufgesetzt werden?
  - Welche Netzdienste werden von dem Server angeboten?
  - Welche Authentisierungsverfahren sollen für die angebotenen Dienste gewählt werden?
  - Auf welche externen Netzdienste soll von dem Rechner aus zugegriffen werden können?
  - Soll ein verteiltes Dateisystem eingebunden werden?Verteilte Dateisysteme, bei denen die Nutzdaten unverschlüsselt übertragen werden, sollten nur im internen Netz verwendet werden. Soll ein verteiltes Dateisystem über ein unsicheres Netz hinweg genutzt werden, so muss es durch zusätzliche Maßnahmen (kryptographisch geschütztes VPN, Tunneling) gesichert werden.
- Protokollierung
  - Welche Ereignisse werden protokolliert?
  - Wo werden die Protokolldateien gespeichert? Werden sie lokal gespeichert oder soll ein zentraler Server eingesetzt werden, an dem die einzelnen Systeme im Netz ihre Protokollierungsinformationen schicken?
  - Wie und in welchen Abständen werden die Protokolle ausgewertet?
  - Wer hat Zugriff auf die Logdateien?
  - Ist gewährleistet, dass personenbezogene Informationen nicht an unbefugte Personen gelangen?
  - Wie lange sollen die Logdateien gespeichert werden?

Anhand der oben genannten Punkte kann eine Checkliste erstellt werden, die bei Audits oder Revisionen hilfreich sein kann.

Die Verantwortung für die Sicherheitsrichtlinie liegt beim Sicherheitsmanagement, Änderungen und Abweichungen hiervon dürfen nur in Abstimmung mit dem Sicherheitsmanagement erfolgen.

Bei der Erstellung einer Sicherheitsrichtlinie ist es empfehlenswert, so vorzugehen, dass zunächst ein Maximum an Forderungen und Vorgaben für die Sicherheit der Systeme aufgestellt wird. Diese können anschließend den tatsächlichen Gegebenheiten angepasst werden. Idealerweise wird so erreicht, dass alle notwendigen Aspekte berücksichtigt werden. Für jede im zweiten Schritt verworfene oder abgeschwächte Vorgabe sollte der Grund für die Nicht-Berücksichtigung dokumentiert werden.

SYS.1.1.M12 Planung des Server-Einsatzes

Eine grundlegende Voraussetzung dafür, dass ein Server sicher betrieben werden kann ist ein angemessenes Maß an Planung im Vorfeld.

Die Planung für den Einsatz eines Servers kann in mehreren Schritten nach dem Prinzip des Top-Down-Entwurfs erfolgen: Ausgehend von einem Grobkonzept für das Gesamtsystem werden konkrete Planungen für Teilkomponenten in spezifische Teilkonzepten festgelegt. Die Planung betrifft dabei nicht nur Aspekte, die klassischerweise mit dem Begriff Sicherheit verknüpft werden, sondern auch normale betriebliche Aspekte, die Anforderungen im Bereich der Sicherheit nach sich ziehen.

Im Grobkonzept sollten beispielsweise folgende typische Fragestellungen behandelt werden:

- Welche Aufgaben soll das zu planende System erfüllen? Welche Dienste sollen von dem Server bereitgestellt werden? Gibt es besondere Anforderungen an die Verfügbarkeit des Systems oder an die Vertraulichkeit oder Integrität der gespeicherten oder verarbeiteten Daten?
- Diese Vorgaben kommen aus der übergreifenden Planung und werden von den allgemeinen Zielvorgaben bestimmt. Je genauer die Rahmenbedingungen bekannt und je präziser die Vorgaben formuliert sind, desto einfacher werden die folgenden Planungsschritte.
- Sollen in dem System bestimmte Hardwarekomponenten eingesetzt werden? Dies kann beispielsweise für die Auswahl des Betriebssystems wichtig sein.
- Welche Anforderungen an die Hardware (CPU, Arbeitsspeicher, Kapazität der Datenträger, Kapazität des Netzes etc.) ergeben sich aus den allgemeinen Anforderungen?
- Handelt es sich bei dem eingesetzten Netz um einen homogenen oder heterogenen Rechnerverbund?
- Ersetzt das System ein altes, vorhandenes? Sollen von dem alten System Datenbestände oder Hardwarekomponenten übernommen werden?
- Sollen die Daten lokal oder auf einem SAN-System abgelegt werden?
- Sollen die Server virtualisiert werden?

Die folgenden Teilkonzepte sollten bei der Planung des Servereinsatzes berücksichtigt werden:

- Authentisierung und Benutzerverwaltung:
  Welche Arten der Benutzerverwaltung und Benutzerauthentisierung sollen auf dem System genutzt werden? Werden Benutzer nur lokal verwaltet oder soll ein zentrales Verwaltungssystem genutzt werden? Soll das System auf einen zentralen, netzbasierten Authentisierungsdienst zugreifen, oder wird nur eine lokale Authentisierung benötigt?
- Benutzer- und Gruppenkonzept:
  Ausgehend vom organisationsweiten Benutzer-, Rechte- und Rollenkonzept müssen entsprechende Regelungen für das System erstellt werden.
- Administration:
  Wie soll das System administriert werden? Werden alle Einstellungen lokal vorgenommen oder der Server in ein zentrales Administrations- und Konfigurationsmanagement integriert?
- Partitions- und Dateisystem-Layout:
  In der Planungsphase sollte eine erste Abschätzung des benötigten Plattenplatzes durchgeführt werden. Zur einfacheren Administration und Wartung ist es empfehlenswert, so weit wie möglich eine Trennung von Betriebssystem (Systemprogramme und -konfiguration), Anwendungsprogrammen und -daten (beispielsweise Datenbank-Server und Daten) und gegebenenfalls Benutzerdaten vorzunehmen. Verschiedene Betriebssysteme bieten hierfür unterschiedliche Mechanismen an (Aufteilung in Laufwerke unter Windows, Filesysteme unter Unix). Oft kann es sinnvoll sein, bestimmte Daten sogar auf einer eigenen Festplatte oder einem eigenen Plattensystem zu speichern. Dies erlaubt es beispielsweise, bei einer Neuinstallation oder einem Update des Systems die Daten auf den anderen Partitionen ohne Umkopieren zu übernehmen.
  Falls auf dem Server Daten mit hohem Schutzbedarf bezüglich der Vertraulichkeit gespeichert werden, so wird der Einsatz verschlüsselter Dateisysteme dringend empfohlen. Dabei brauchen nicht notwendigerweise alle Dateisysteme verschlüsselt zu werden, sondern es wird oft ausreichend sein, für den Teil des Dateisystems eine Verschlüsselung vorzusehen, auf dem die Daten selbst gespeichert werden. Dies wird durch eine entsprechende Planung des Partitions- und Dateisystemlayouts erleichtert. Bei der Auswahl einer Verschlüsselung von einzelnen Dateien und Verzeichnissen sollte den Anwendern die Auswahl abgenommen werden, ob die Dateien verschlüsselt werden oder unverschlüsselt abgelegt werden.In der Planungsphase sollte die vorgesehene Aufteilung der Partitionen und deren Größe dokumentiert werden.
- Netzdienste und Netzanbindung:
  In Abhängigkeit von den Anforderungen an die Vertraulichkeit, Integrität und Verfügbarkeit der Daten, die auf dem Server gespeichert oder verarbeitet werden sollen, muss die Netzanbindung des Servers geplant werden.
  Generell wird empfohlen, einen Server nicht direkt im selben IP-Subnetz zu platzieren wie die Clients, die auf den Server zugreifen sollen. Wenn der Server zumindest durch einen Router von den Clients getrennt ist, dann bestehen wesentlich bessere Möglichkeiten zur Steuerung des Zugangs und zur Erkennung von Anomalien im Netzverkehr, die auf mögliche Probleme hindeuten.
- Ein Server, der Daten mit einem hohen Schutzbedarf bezüglich Vertraulichkeit oder Integrität speichert oder verarbeitet, sollte in einem eigenen IP-Subnetz angesiedelt werden und zumindest durch einen Paketfilter vom Rest des Netzes getrennt werden. Bei einem sehr hohen Schutzbedarf sollte ein Application Level Gateway eingesetzt werden.
- Bei normalem Schutzbedarf kann ein Server, der ausschließlich von Clients aus dem internen Netz genutzt wird, ausnahmsweise auch im selben Teilnetz angesiedelt werden. Es wird jedoch empfohlen, auch in diesem Fall den Server bei anstehenden Umstellungen in der Netzstruktur in ein eigenes Teilnetz zu verlegen.
- Abhängig vom festgelegten Einsatzzweck des Rechners wird außerdem eventuell der Zugang auf bestimmte Dienste im Netz (etwa Web-, File-, Datenbank-, Druck-, DNS oder Mailserver) benötigt. Dies muss bereits im Rahmen der Planung berücksichtigt werden, damit nicht zu einem späteren Zeitpunkt Schwierigkeiten beispielsweise durch zu geringe Übertragungskapazitäten oder Probleme mit zwischengeschalteten Sicherheitsgateways entstehen.
- Neben dem eigentlichen Dienst, für den ein Server aufgesetzt wird, werden oft noch andere Dienste benötigt, um den Server effizient nutzen und administrieren zu können. Beispielsweise wird für eine Administration über das Netz ein sicherer Zugang (beispielsweise SSH) benötigt, oder die Dateien für ein Webangebot können über das Netz auf den Webserver übertragen werden. Wenn die dadurch entstehende Netzkommunikation über unsichere Netze stattfindet, so müssen geeignete sichere Protokolle benutzt werden. Außerdem dürfen die Dienste nur autorisierten Benutzern und Rechnern zur Verfügung gestellt werden. Dies kann durch eine Passwortvergabe, durch den Einsatz eines Paketfilters oder anderer Mechanismen realisiert werden. Kein Dienst sollte in einem unsicheren Netz wie dem Internet bereitgestellt werden, wenn dies nicht ausdrücklich vorgesehen ist.

Alle Entscheidungen, die in der Planungsphase getroffen wurden, müssen so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können. Dabei ist zu beachten, dass meist andere Personen neben dem Autor diese Informationen auswerten müssen. Daher ist auf passende Strukturierung und Verständlichkeit zu achten.

SYS.1.1.M13 Beschaffung von Servern

Die Beschaffung eines Servers betrifft sowohl die Hard- als auch die Software, aus der der Server aufgebaut werden soll. Werden bei der Beschaffung eines Servers Fehler gemacht, so kann dies schwerwiegende Folgen auf den sicheren Betrieb eines Netzes haben, da mit ungeeigneter Hard- und Software das angestrebte Sicherheitsniveau unter Umständen nur schwer erreichbar ist.

Bevor ein Server beschafft wird, muss daher eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden. Aufgrund der Bewertung kann dann eine fundierte Kaufentscheidung erfolgen, die sicherstellt, dass der Server im praktischen Betrieb den Anforderungen genügt.

Auch rein funktionale Merkmale von Servern können Auswirkungen auf die Informationssicherheit haben. Meist ist dann der Grundwert Verfügbarkeit betroffen, beispielsweise wenn ein Server wegen unzureichender Speicherausstattung nicht die geforderten Antwortzeiten oder Durchsatzraten erreicht. Außerdem spielt die Unterstützung durch den Hersteller eine nicht zu vernachlässigende Rolle, wenn es beispielsweise darum geht, dass zeitnah Patches für Sicherheitslücken zur Verfügung gestellt werden.

Aus dem Blickwinkel der Informationssicherheit sind zentrale Anforderungen an Server, dass

- Hard- und Software so ausgelegt sind, dass die Anforderungen an die Verfügbarkeit des Servers und die Integrität der Daten erfüllt werden können,
- die Administration über sichere Protokolle möglich ist,
- die Benutzerverwaltung es erlaubt, das organisationsweite Rollenkonzept entsprechend umzusetzen, und
- dass es gegebenenfalls möglich ist, besonders sensitive Daten zu verschlüsseln.

Nachfolgend werden einige Anforderungen aufgelistet, die bei der Beschaffung von Servern berücksichtigt werden sollten:

- Grundlegende funktionale Anforderungen
  - Unterstützt das Gerät alle benötigten Hardwareschnittstellen?
  - Unterstützt die Software alle benötigten Protokolle und Datenformate?
  - Sicherheit
  - Unterstützt das System sichere Protokolle zur Administration?
  - Wenn Server nicht über ein eigenes Administrationsnetz administriert werden, muss die Administration mit Hilfe von sicheren Netzprotokollen möglich sein.
- Wartbarkeit
  - Wird die Hard- und Software ausreichend lange vom Hersteller unterstützt und gepflegt?
    Der Hersteller sollte solange den Server unterstützen, wie er auch eingesetzt werden soll. Hierzu gehört es, dass Support angeboten wird und Updates bereitgestellt werden.
  - Bietet der Hersteller regelmäßige Updates und schnell verfügbare Sicherheitspatches für die Software an?
    Es ist insbesondere wichtig, dass der Hersteller zeitnah auf bekannt gewordene Sicherheitsmängel reagiert.
  - Wird für das Produkt die Möglichkeit des Abschlusses von Wartungsverträgen angeboten?
    Oft ist der Zugriff auf Updates und Unterstützungsleistungen vom Hersteller nur in Verbindung mit einem gültigen Wartungsvertrag möglich.
  - Können im Rahmen der Wartungsverträge maximale Reaktionszeiten für die Problembehebung festgelegt werden?
    Ein Wartungsvertrag ist nur dann geeignet, wenn mit den garantierten Reaktions- und Wiederinbetriebnahmezeiten die festgelegten Ansprüche an die Verfügbarkeit der Geräte abgedeckt werden können.
  - Bietet der Hersteller einen technischen Kundendienst (Hotline) an, der in der Lage ist, sofort bei Problemen zu helfen?
    Dieser Punkt sollte Bestandteil des abgeschlossenen Wartungsvertrags sein. Beim Abschluss des Vertrags ist auf die Sprache der zur Verfügung gestellten Hotline des Herstellers zu achten.
- Zuverlässigkeit/Ausfallsicherheit
  - Gibt es verlässliche Informationen zur Zuverlässigkeit und Ausfallsicherheit von Hard- und Software?
  - Bietet der Hersteller gegebenenfalls Hochverfügbarkeitslösungen an?
  - Wenn die Verfügbarkeitsanforderungen nicht über Wartungsverträge abgedeckt werden können, sollte das System Hochverfügbarkeitslösungen unterstützen.
- Benutzerfreundlichkeit
  - Lässt sich das Produkt einfach installieren, konfigurieren, administrieren und benutzen?
  - Es sollten darüber hinaus Schulungen für das Produkt angeboten werden.
- Kosten
  - Wie hoch sind die Anschaffungskosten für Hard- und Software?
  - Wie hoch sind die voraussichtlichen laufenden Kosten (Wartung, Betrieb, Support)?
    Diese Kosten müssen bereits in der Beschaffungsphase mit berücksichtigt werden. Der Inhalt der Wartungs- und Supportverträge sollte geprüft werden (Reaktionszeiten, Hotline, Qualifikation des Personals, etc.).
  - Wie hoch sind die voraussichtlichen laufenden Kosten für das Personal?
  - Müssen zusätzliche Soft- oder Hardware-Komponenten angeschafft werden?
    Diese Frage sollte bereits in der Planungsphase beantwortet werden. Wenn beispielsweise bereits ein Netz-Management-System im Einsatz ist, sollte die Kompatibilität mit den zu beschaffenden Geräten geprüft werden.
    Zudem sollte der Aufwand zur Integration in eine bestehende Infrastruktur beachtet werden.
  - Wie hoch sind die Kosten für die Schulung von Administratoren?
  - Mit welchen Kosten muss gerechnet werden, wenn wegen erhöhter Kapazitätsanforderungen ein Upgrade der Hardware notwendig ist?
    Die Kosten können in diesem Fall erheblich höher ausfallen, als die Kosten für die Hardware selbst, da in etlichen Lizenzmodellen von Softwareanbietern der Lizenzpreis von der Anzahl der Prozessoren oder dem Prozessortakt abhängt, so dass bei einem Hardwareupgrade auch gleichzeitig eine neue Programmlizenz erforderlich sein kann.
- Protokollierung
  - Welche Möglichkeiten der Protokollierung sind vorhanden?
    Die angebotenen Möglichkeiten zur Protokollierung müssen mindestens die in der Sicher-

Die Anforderungen und die auf ihrer Basis getroffenen Auswahlentscheidungen sollten so dokumentiert werden, dass zu einem späteren Zeitpunkt nachvollziehbar ist, wie die Entscheidung zu Stande gekommen ist.

SYS.1.1.M14 Erstellung eines Benutzer- und Administrationskonzepts

Ablauf, Rahmenbedingungen und Anforderungen an administrative Aufgaben, sowie die Aufgabentrennungen zwischen den verschiedenen Rollen der Benutzer des IT-Systems sollten in einem Benutzer- und Administrationskonzept festgeschrieben werden. Hierzu sollten die am IT-System zugelassenen Benutzer, angelegten Benutzergruppen und Rechteprofile dokumentiert werden. Folgende Angaben zur Rechtevergabe an Benutzer und Benutzergruppen sollten festgelegt werden:

Zugelassene Benutzer:

- zugeordnetes Rechteprofil (gegebenenfalls Abweichungen vom verwendeten Standard-Rechteprofil)
- Begründung für die Wahl des Rechteprofils (und gegebenenfalls der Abweichungen)
- Zuordnung des Benutzers zu einer Organisationseinheit, Raum- und Telefonnummer
- Zeitpunkt und Grund der Einrichtung
- Befristung der Einrichtung

Zugelassene Gruppen:

- zugehörige Benutzer
- Zeitpunkt und Grund der Einrichtung
- Befristung der Einrichtung

Vertiefende Informationen und konkrete Anforderungen hierzu sind im Baustein ORP.4 Identitäts- und Berechtigungsmanagement zu finden.

SYS.1.1.M15 Unterbrechungsfreie und stabile Stromversorgung [Haustechnik]

Eine lokale unterbrechungsfreien Stromversorgung (USV) hat die Aufgabe, ein einzelnes IT-System oder sehr wenige IT-Geräte gegen die Folgen kurzfristiger Unterbrechungen der Stromversorgung zu schützen. Diese Zielsetzung ist meist in kleineren IT-Strukturen gegeben, die zudem nicht über eine Netzersatzanlage verfügen.

Für größere IT-Strukturen oder gar die Versorgung ganzer Gebäude werden vornehmlich zentrale USV-Systeme eingesetzt.

Gleichgültig, ob eine lokale USV als Beistellgerät oder als 19-Zoll-Einschub eingesetzt wird, ist ihre Leistung und ihre Stützzeit durch die Geräteeigenschaften festgeschrieben und können in der Regel nicht verändert werden.

Bei den heute verfügbaren lokalen USV-Geräten und den üblicherweise durch sie bereitzustellenden geringen Leistungen (im Bereich bis circa 1 kVA) können diese Stromausfälle bis zu 120 Minuten problemlos überbrücken (Stützzeit). Welche Stützzeit tatsächlich im konkreten Szenario erforderlich ist, hängt davon ab, wie lange einerseits das Herunterfahren der angeschlossenen Geräte (Shutdown) dauert und wie lange andererseits darauf gewartet werden soll, dass die Stromversorgung wieder anspringt (Wartezeit). Da ein großer Teil aller Stromausfälle nur wenige Minuten dauert, dürfte eine Wartezeit von 15 Minuten meistens ausreichen, um eine Versorgungsunterbrechung zu überbrücken. Dauert die Versorgungsunterbrechung länger als die Wartezeit, und muss das versorgte IT-System heruntergefahren werden, um Datenverluste zu vermeiden, sollte die gesamte Stützzeit nach der Formel

Stützzeit = Wartezeit plus zweifache Shutdown-Zeit

dimensioniert werden. Durch den zweifachen Ansatz der Shutdown-Zeit ist eine Sicherheitsreserve gegeben, falls das Herunterfahren länger dauert als angenommen. Bei jedem Austausch oder Ergänzung von IT-Geräten, die durch eine USV versorgt werden, muss erneut geprüft werden, ob die vorhandene Stützzeit ausreicht.

Drei USV-Arten sind zu unterscheiden:

- VFD-USV
  Bei der VFD-USV (VFD steht für Voltage and Frequency Dependent) werden die angeschlossenen Verbraucher im Normalbetrieb direkt aus dem Stromversorgungsnetz gespeist. Kleinere Störungen im Versorgungsnetz können also direkt bis zu den angeschlossenen Verbrauchern gelangen. Erst wenn dieses ausfällt, schaltet sich die VFD-USV selbsttätig zu und übernimmt die Versorgung. Dazu benötigt sie bis zu 10 ms (Umschaltlücke), was für manche IT-Geräte schon zu viel sein kann. Die VFD-USV wurde früher auch Offline-USV genannt.
- VI-USV (Voltage Independent)
  Hierbei wird die Versorgungsspannung bei kleineren Schwankungen nachgeregelt (VI steht für Voltage Independent), ohne dass die USV als solche die Versorgung der angeschlossenen Verbraucher komplett übernimmt. Die Frequenz am Ausgang einer VI-USV ist aber wie bei einer VFD-USV direkt vom Versorgungsnetz abhängig. Auch bei der VI-USV kann es bei der Umschaltung auf Batteriebetrieb zu einer Umschaltlücke kommen.
- VFI-USV (Voltage and Frequency Independent)
  Bei der VFI-USV (Voltage and Frequency Independent) gibt es im Normalfall keine direkte Verbindung zwischen USV-Eingang und -Ausgang. Die elektrische Energie wird eingangsseitig gleichgerichtet und in den Zwischenkreis gespeist. Von dort werden die Batterien im optimalen Ladezustand gehalten und der Wechselrichter versorgt. Dieser erzeugt die für die angeschlossenen Verbraucher erforderliche Wechselspannung.
  Da die Ausgangsenergie unabhängig vom Eingang permanent über den Wechselrichter erzeugt wird, gibt es hier keine Umschaltlücke. Die VFI-USV wurde früher als Online-USV bezeichnet.

Da die VFI-USV als einzige der drei Systeme wirklich unterbrechungsfrei arbeitet, sollt diesem immer der Vorzug geben werden. Unter Berücksichtigung weiterer, hier nicht behandelter Qualitätsmerkmale stellt eine USV, die nach DIN IEC 62040-3 gemäß VFI-SS-111 klassifiziert ist, das Optimum für die IT-Versorgung dar.

Entgegen einer immer wieder geäußerten Annahme stellt eine USV gleich welcher Bauart keinen Überspannungsschutz im eigentlichen Sinn dar. Eine USV ist zwar in der Lage, im Rahmen ihrer normalen Funktion zu hohe Spannungen von den angeschlossenen Verbrauchern fernzuhalten. Gegen Überspannungen, wie sie durch die technischen Einrichtungen des Überspannungsschutzes abgefangen werden, hilft aber eine USV keinesfalls. Im Gegenteil, eine USV muss wie alle anderen elektrischen Verbraucher durch geeignete Schutzmaßnahmen gegen Überspannungen geschützt werden (siehe Abschnitt "Überspannungsschutz").

Um mögliche Probleme mit Schutzleiterströmen zu vermeiden, sollten IT-Geräte, die über eine lokale USV versorgt werden, nicht über geschirmte Leitungen (z. B. Druckerkabel) mit anderen IT-Geräten verbunden werden, die über einen anderen Weg versorgt werden.

Da die Batterien einer lokalen USV in den seltensten Fällen in ihrem optimalen Temperaturbereich (typischerweise um 20°C) betrieben werden, ist die Batterie-Lebensdauer bei lokalen USV-Geräten recht gering, im günstigsten Fall bis zu 5 Jahre, meist weniger. Während dieser Betriebszeit verlieren die Batterien permanent an Leistung, so dass eine lokale USV nach vielleicht zwei oder drei Jahren allenfalls noch die Hälfte der Stützzeit im Neuzustand bereitstellen kann. Um sicher zu stellen, dass die USV die erforderliche Stützzeit bereitstellt, sollte etwa einmal pro Jahr die tatsächliche Stützzeit ermittelt werden. Manche USV-Systeme verfügen dazu über eingebaute Prüfmechanismen. Ist das nicht der Fall, kann der Wert durch einen Lasttest ermittelt werden.

Wie bei allen anderen elektrischen Geräten ist auch bei USV-Systemen darauf zu achten, dass sie in den vom Hersteller genannten Temperaturbereichen betrieben werden. Dies ist bei der Dimensionierung der Kühlung zu berücksichtigen.

Da die USV die letzte Bastion gegen den Stromausfall vor der IT-Hardware ist, kommt ihr große Bedeutung für die Sicherstellung der Verfügbarkeit zu. Sie hat also denselben Schutzbedarf wie die durch die USV versorgte IT. Wenn die USV-versorgten IT-Systeme redundant ausgelegt sind, sollten auch USV-Systeme redundant vorhanden sein.

Außerdem ist bei einer USV besonders auf den Schutz vor dem Zugang Unbefugter, Brand und Wasser zu achten. Ein sinnvoller Schutz gegen Brand macht es nahezu unverzichtbar, einander Redundanz bietenden USV-Einheiten in getrennten Brandabschnitten unterzubringen. Nur so kann verhindert werden, dass bei Brand einer Einheit nach kurzer Zeit auch alle anderen durch Brand ausfallen.

Um die Schutzwirkung einer USV aufrechtzuerhalten, muss sie regelmäßig gewartet werden. Dafür sind die vom Hersteller vorgesehenen Wartungsintervalle der USV einzuhalten.

Überspannungsschutz

In jedem elektrisch leitenden Netz, gleichgültig ob es der Energieversorgung oder der Datenübertragung dient, kann es zu jeder Zeit zu Überspannungen kommen. Überwiegend werden solche Überspannungen durch andere Stromverbraucher im gleichen Versorgungsnetz verursacht. Überspannungen durch Blitz sind dagegen zwar sehr viel seltener, haben aber ein ungleich höheres Schadenspotential.

Nicht nur über die im Haus verlegten Leitungen, sondern auch über alle elektrisch leitenden Außenanbindungen wie Telefon-, Wasser- oder Gasleitungen können Überspannungen in ein Gebäude und die dort betriebene IT gelangen. Darüber hinaus können Überspannungen auch auf interne Leitungen eingekoppelt werden.

Die erforderlichen Maßnahmen zum Schutz von IT-Geräten sind unabhängig von der Ursache der Überspannung im Wesentlichen die gleichen. Die Normenreihe zum Blitzschutz von baulichen Anlagen DIN EN 62305 "Blitzschutz" (entspricht der Normenreihe VDE 0185-305 und IEC 62305) beschreibt ein Gesamtkonzept zum Blitzschutz. Auf Basis dieser Normenreihe DIN EN 62305 ist ein Überspannungsschutzkonzept zu erstellen.

Die DIN EN 62305 beschreibt in ihrem Teil 2 "Risiko-Management" allgemeinverbindlich den Weg zu einem risikoorientierten Blitz- und Überspannungsschutz. Im Teil 3 wird der "Schutz von baulichen Anlagen und Personen" behandelt, in Teil 4 "Elektrische und elektronische Systeme in baulichen Anlagen".

Im Überspannungsschutzkonzept sind natürlich auch Netzersatzanlagen (NEA) und unterbrechungsfreie Stromversorgungen (USVen) zu berücksichtigen. Obwohl USVen einen gewissen Schutz der angeschlossenen Geräte bewirken, sind sie keinesfalls als Überspannungsschutzeinrichtung zu betrachten, sondern einzig und allein als zu schützendes elektronisches Gerät.

An die Stelle der bisherigen drei Stufen Grob-, Mittel- und Feinschutz ist das Konzept der energetischen Koordination getreten. Nach der Norm ist eine energetische Koordination zwar nur dann zwingend erforderlich, wenn es einen äußeren Blitzschutz gibt. Im Sinne der Informationssicherheit sollte die energetische Koordination auch in Fällen ohne äußeren Blitzschutz berücksichtigt werden. Vereinfacht dargestellt bedeutet das folgendes:

- Hinter jedem Schutzelement (SPD - Surge Protecting Device) darf maximal so viel durch Überspannung verursachte Energie wirken, wie alle dahinter befindlichen elektrischen Einrichtungen (inklusive der folgenden SPDs) verkraften. Ein reines Leitungsnetz ist natürlich wesentlich robuster und verträgt deutlich mehr Energie als z. B. die Schnittstelle einer Netzwerkkarte in einem Rechner .
- Alle eingesetzten SPDs müssen sich miteinander vertragen. Der Ausgang eines vorderen SPDs und der Eingang des folgenden müssen aufeinander angepasst sein. Der Nachweis der energetischen Koordination kann auf dreierlei Weise erbracht werden:

1 Einzelfallprüfung durch einen Fachprüfer,
2 Computersimulation mittels geeigneter Näherungsverfahren,
3 Einbau von SPDs aus einer Produktfamilie, für die der Hersteller den Nachweis erbringt.

Durch den Aufbau des Blitz- und Überspannungsschutzes werden wie Zwiebelschalen ineinander liegende Blitzschutzzonen (LPZ, Lightning Protection Zone) gebildet. Mit steigendem Schutz werden sie von außen nach innen mit LPZ 0, LPZ 1, LPZ 2 etc. bezeichnet. Dabei kann eine Zone nur dann gebildet werden, wenn es die nächst äußere gibt: So ist es nicht möglich, eine LPZ 2 zu realisieren, ohne auch die LPZ 1 zu haben.

Für einfache elektrische und elektromechanische Geräte ist die LPZ 1 meist ausreichend. Zum Schutz elektronischer Geräte (IT-Hardware, USV etc.) ist mindestens die LPZ 2 zu realisieren. Bei besonders empfindlichen Geräten, z. B. in der Medizin- oder Messtechnik kann durchaus die LPZ 3 erforderlich werden.

Hinweis:

Die LPZ (Blitzschutzzonen) sind nicht zu verwechseln mit den Schutzklassen des äußeren Blitzschutzsystems, das mit LPS (Lightning Protection System) bezeichnet wird.

Ob ein LPS erforderlich ist und mit welcher Schutzklasse, muss anhand der Risikobewertung (gemäß Teil 2 der DIN EN 62305) entschieden werden. Der früher ausreichende Blick in eine Gebäudeliste genügt nicht mehr!

In vielen Fällen ist der gebäudeweite Aufbau einer LPZ 2 oder LPZ 3 gar nicht erforderlich. Während der Übergang von der LPZ 0 (das ist alles außerhalb eines Gebäudes, wo der Blitz also tatsächlich direkt einschlagen kann) zur LPZ 1 tatsächlich möglichst nah an der Gebäudehülle zu erfolgen hat, kann der Aufbau höherer LPZ an beliebiger Stelle und in beliebigem Umfang erfolgen. Wichtig ist dabei aber darauf zu achten, dass keine Leitung, die nur den Schutz der LPZ 1 genießt (z. B. Heizungsrohre) durch höherwertige LPZ hindurch läuft.

Die früher notwendigen Mindestleitungslängen zwischen den SPDs, also den Schutzelementen, und der unterschiedlichen LPZ sind heute nicht mehr zwingend. Es gibt SPDs, die in einem Bauteil den Übergang von der LPZ 0 direkt in die LPZ 2 realisieren.

Die Schutzwirkung eines SPDs reicht nach beiden Seiten (auf die kommende und die gehende Leitung) nur über eine bestimmte Kabelstrecke, die im Einzelnen vom Hersteller zu benennen ist. Wird die Kabellänge abgehend überschritten, sind wiederholt SPDs einzubauen, um den Schutz aufrecht zu erhalten.

Nach DIN EN 62305 müssen Blitzschutzsysteme (LPS) abhängig von der Schutzklasse in Abständen von ein bis vier Jahren überprüft werden. Für die Überspannungsschutzeinrichtungen sieht die Norm keine ausdrücklichen Prüfintervalle vor. Im Sinne der Informationssicherheit sollten aber alle SPDs periodisch (mindestens einmal pro Jahr) und nach bekannten Ereignissen geprüft und gegebenenfalls ersetzt werden. Um diese Prüfung überhaupt durchführen zu können, sollten, sofern verfügbar, ausschließlich solche SPDs eingebaut werden, die eine integrierte Defektanzeige oder (noch besser) eine Lebensdaueranzeige besitzen.

Neben dem Überspannungsschutz auf allen elektrisch leitenden Systemen müssen in Serverräumen und den Kerneinheiten eines Rechenzentrums Maßnahmen gegen elektrostatische Aufladung getroffen werden. Der Durchgangswiderstand der Bodenbeläge in solchen Räumen muss zwischen 10 und 100 Megaohm liegen. Die Einstufung nach DIN-Vorschrift 4102-1 "Brandverhalten von Baustoffen und Bauteilen" muss mindestens "B1 schwer entflammbar" erreichen. Dies gilt auch für einen Doppelboden oder Installationsboden.

Unabhängig von Umfang und Ausbau des Überspannungsschutzes ist zu beachten, dass ein umfassender Potentialausgleich aller in den Überspannungsschutz einbezogenen elektrischen Betriebsmittel erforderlich ist! Die Mehrzahl der Schäden an IT-Geräten durch Überspannungen ist auf nicht konsequent umgesetzten Potentialausgleich zurückzuführen.

SYS.1.1.M16 Sichere Installation und Grundkonfiguration von Servern

Nachdem die Planung eines neuen Servers abgeschlossen und eine Sicherheitsrichtlinie erstellt wurde, kann mit der Installation des Servers begonnen werden.

Die Installation des Systems sollte nur von autorisierten Personen (Administratoren oder vertraglich gebundene Dienstleister) durchgeführt werden. Administratoren für IT-Systeme und deren Vertreter müssen sorgfältig ausgewählt werden. Sie müssen regelmäßig darüber belehrt werden, dass die Befugnisse nur für die erforderlichen Administrationsaufgaben verwendet werden dürfen. Da Administratoren hinsichtlich der Funktionsfähigkeit der eingesetzten Hard- und Software eine Schlüsselrolle innehaben, muss auch beim Ausfall von Administratoren die Weiterführung der Tätigkeiten gewährleistet sein. Hierzu müssen die benannten Vertreter über den aktuellen Stand der Systemkonfiguration verfügen sowie Zugriff auf die für die Administration benötigten Passwörter, Schlüssel und Sicherheitstoken haben. Vertiefende Informationen hierzu sind in ORP.4 Identitäts- und Berechtigungsmanagement zu finden.

Es ist empfehlenswert, zunächst ein kurzes Installationskonzept entsprechend den funktionalen Anforderungen aus der Planung und den Vorgaben der Sicherheitsrichtlinie zu erstellen. Prinzipiell ist es vorteilhaft, die Installation in zwei Phasen vorzunehmen: Zunächst wird ein Grundsystem installiert und konfiguriert, anschließend werden die weiteren benötigten Dienste und Anwendungen eingerichtet. Die Installationsprogramme der meisten Betriebssysteme unterstützen diese Vorgehensweise mehr oder weniger gut.

Die beschriebenen Schritte brauchen nicht notwendigerweise alle für jeden Server erneut durchgeführt zu werden. Dies könnte sogar insofern kontraproduktiv sein, als die ständige Wiederholung die Gefahr von Fehlern erhöht. Es wird daher empfohlen, die beschriebenen Schritte einmal besonders sorgfältig auf einem Referenz-System durchzuführen, die nötigen Konfigurationen genau zu dokumentieren und so ein angepasstes Installationskonzept für das betreffende Betriebssystem zu erhalten. Dabei muss beachtet werden, dass dieses Installationskonzept auch bei Änderungen am Betriebssystem, die kein komplett neues Release darstellen (Service-Packs, Update-Releases oder ähnliches) überprüft und gegebenenfalls angepasst werden muss.

Bei virtuellen Server wird in den seltensten Fällen für jede Instanz ein abgeändertes Betriebssystem installiert, hier wird in der Regel ein Grundsystem erstellt, dass in die Instanz kopiert und als eigenständiger Klon gestartet wird. In dieser Instanz werden im nächsten Schritt die benötigten Serverdienste oder Anwendungsprogramme installiert und zu jedem späteren Zeitpunkt kann ein neuer Klon generiert werden, um beispielsweise mehrere Instanzen mit identischen Serverdiensten oder Anwendungsprogrammen zu erhalten. Damit können sich aber auch Fehlentscheidungen und falsche Einstellungen, die bei der Erstellung des Grundsystems getroffen wurden, bei der Installation der Klone auf zahlreiche weitere Instanzen vererben. Für jeden einzelnen Klon sollten daher alle Empfehlungen dieser Maßnahme ebenfalls sorgfältig umgesetzt werden.

Installation

Diese Maßnahme beinhaltet nur Empfehlungen für die ersten Schritte einer Installation und nicht für die endgültige Konfiguration für den geplanten Einsatzzweck. Die weitergehenden Konfigurationsschritte sind sehr stark vom jeweiligen System und Einsatzgebiet abhängig und werden in eigenen Maßnahmen in den Betriebssystem-Bausteinen behandelt.

Während der Installation und der späteren Konfiguration sollten zumindest die wichtigen Schritte so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können. Beispielsweise kann eine Checkliste für die Installation erstellt werden, auf der durchgeführte Schritte abgehakt und vorgenommene Einstellungen vermerkt werden können. Eine entsprechende Dokumentation ist für eine Fehleranalyse oder spätere Neuinstallation hilfreich. Dabei sollte beachtet werden, dass neben dem Autor auch weitere, auf diesem Gebiet eventuell weniger spezialisierte, Administratoren auf die Dokumentation zurückgreifen müssen. Daher ist es wichtig, dass die Dokumentation gut strukturiert und verständlich ist.

Wird der Server von Datenträgern wie DVDs oder anderen Speichermedien installiert, wird empfohlen, die Installation und Grundkonfiguration offline oder zumindest in einem sicheren Netz (Installations- oder Administrationsnetz) durchzuführen. Generell sollte verhindert werden, dass andere IT-Systeme während der Installation auf das zu installierende IT-System zugreifen können. Dies ist wichtig, weil während der Installation meist noch keine Passwörter vergeben und keine Schutzmechanismen aktiv sind, aber eventuell schon Zugänge möglich sind. Falls die Installation mehrerer IT-Systeme teilweise über das Netz erfolgen soll (beispielsweise Nachladen von Paketen), so wird empfohlen, einen Installationsserver im Administrationsnetz zu nutzen.

Insbesondere beim Betriebssystem selbst ist es wichtig, dass die installierte Version aus einer vertrauenswürdigen Quelle stammt. Dies ist besonders wichtig, wenn beispielsweise CD -Images aus dem Internet heruntergeladen wurden. In diesem Fall sollte unbedingt geprüft werden, ob digitale Signaturen der Pakete verfügbar sind, die zur Verifikation von Integrität und Authentizität der Pakete verwendet werden können. Pakete und CD-Images, für die keine digitalen Signaturen oder wenigstens Prüfsummen existieren, sollten möglichst nicht eingesetzt werden.

Bei der Einrichtung der Festplattenpartitionen muss das in der Planungsphase erstellte Konzept umgesetzt werden. Wenn ein verschlüsseltes Dateisystem eingesetzt werden soll, so muss es meist initialisiert werden, bevor Daten hineinkopiert werden können, denn oft lässt sich ein Dateisystem nicht im Nachhinein verschlüsseln. Auch einige RAID-Systeme und -Level erfordern eine Konfiguration, die abgeschlossen sein muss, bevor die betreffenden Dateisysteme eingerichtet werden können.

Sofern dies nicht bereits automatisch geschehen ist, sollte spätestens beim Abschluss der Grundinstallation auch die Protokollierung der Systemereignisse aktiviert werden. Die Protokolldaten können bei Problemen bei der weiteren Installation und Konfiguration wertvolle Informationen liefern.

Aktualisierung

Wird das System von einer CD, DVD oder einem anderen "Offline-Medium" installiert, so sollte nach der Grundinstallation überprüft werden, ob zwischenzeitlich Aktualisierungen oder Sicherheitspatches vom Hersteller oder Distributor veröffentlicht wurden.

Installation der jeweiligen Serverdienste und Anwendungsprogramme

Nachdem das Betriebssystem installiert und Grundkonfiguration und Aktualisierung abgeschlossen wurde, können die jeweiligen Serverdienste installiert und konfiguriert werden. Sowohl auf Clients als auch Servern werden in der Regel Serverdienste zur Fernadministration benötigt. Bei Servern kommen die eigentlichen Serverdienste hinzu, bei Clients müssen in der Regel grafische Benutzeroberflächen und Anwendungsprogramme installiert und eingerichtet werden. Hierfür wird ein analoges Vorgehen wie für das Betriebssystem selbst empfohlen. Außerdem wird empfohlen, das Betriebssystem zu härten.

SYS.1.1.M17 Einsatzfreigabe

Bevor das Serversystems im produktiven Betrieb eingesetzt und bevor es an ein produktives Netz angeschlossen wird, sollte eine Einsatzfreigabe durchgeführt werden, diese ist zu dokumentieren. Die Einsatzfreigabe basiert auf einer Prüfung der Installations- und Konfigurationsdokumentation und der Funktionsfähigkeit des Systems in einem Test. Sie erfolgt durch eine in der Institution dafür autorisierte Stelle.

Vertiefende Informationen hierzu sind in OPS.1.1.7 Softwaretests- und Freigaben zu finden.

Bei erhöhtem Schutzbedarf sollte überlegt werden, einen internen Penetrationstest durchzuführen (siehe DER.3.3 Penetrationstest).

Falls festgestellt wird, dass ein Sicherheitsupdate oder Patch mit einer anderen wichtigen Komponente oder einem Programm inkompatibel ist oder Probleme verursacht, so muss sorgfältig überlegt werden, wie weiter vorgegangen wird. Wird entschieden, dass auf Grund der aufgetretenen Probleme ein Patch nicht installiert wird, so ist diese Entscheidung auf jeden Fall zu dokumentieren. Außerdem muss in diesem Fall klar beschrieben sein, welche Maßnahmen ersatzweise ergriffen wurden, um ein Ausnutzen der Schwachstelle zu verhindern. Eine solche Entscheidung darf nicht von den Administratoren alleine getroffen werden, sondern sie muss mit den Vorgesetzten und dem ISB abgestimmt sein.

SYS.1.1.M18 Verschlüsselung der Kommunikationsverbindungen

Wenn möglich, sollte die Netzkommunikation von oder zu einem Server verschlüsselt werden. Die Verschlüsselung ist abhängig von dem Dienst, den der Server bereitstellt, vertiefende Informationen zu den jeweiligen Netzdiensten sind in APP.3 Netzbasierte Dienste zu finden. Eine der am verbreitetsten Möglichkeiten, Netzdienste zu verschlüsseln, ist der Einsatz von TLS.

Transport Layer Security (TLS) ist eine Weiterentwicklung von Secure Sockets Layer (SSL) und wird dazu verwendet, Informationen während der Übertragung in Netzen, in der Regel zwischen Serverdiensten und Clients oder zwischen Serverdiensten untereinander kryptographisch abzusichern. Clients können die Verschlüsselung über SSL/TLS nur dann nutzen, wenn diese von den Serverdiensten unterstützt wird. SSL/TLS kann dazu eingesetzt werden, Informationen aus der Anwendungsschicht (z. B. HTTP, LDAP, POP3, IMAP und SMTP) verschlüsselt über TCP/IP zu übertragen. Überdies können mittels SSL/TLS auch sichere VPNs (Virtuelle Private Netze) aufgebaut werden. Mit OpenVPN, einer unter der GNU GPL (General Public License) frei verfügbaren Software, können VPNs mittels SSL/TLS verschlüsselte Verbindungen realisiert werden. Vertiefende Informationen zu VPNs sind in Baustein NET.3.3 Virtual Private Networks (VPN) zu finden.

In der Regel ist es bei vielen Serverdiensten nur ein geringer Mehraufwand, diese so zu konfigurieren, dass eine SSL/TLS-Verschlüsselung unterstützt wird, oder so, dass diese für einen Informationsaustausch ausschließlich genutzt wird. Daher ist für alle Serverdienste zu prüfen, ob mit vertretbarem Aufwand eine Verschlüsselung über SSL/TLS möglich und praktikabel ist. Ist dies mit vertretbarem Aufwand möglich, sollte die SSL/TLS-Verschlüsselung aktiviert werden. Generell sollte der interne und externe Nachrichtenstrom von und zu LDAP-, E-Mail- und Webservern mit SSL/TLS verschlüsselt werden.

Auswahl einer vertrauenswürdigen Zertifizierungsstelle

Zu Beginn eines neuen mit SSL/TLS abgesicherten Kommunikationsaufbaus findet ein sogenannter Handshake zwischen Client und Server statt. Hierbei verständigen sich Client und Server über die kryptographischen Algorithmen, die für Schlüsselaustausch, Verschlüsselung und Integritätssicherung eingesetzt werden. Außerdem einigen sich Client und Server über die SSL-Version, die verwendet wird. Zusätzlich dazu sendet der Server sein X.509-Zertifikat an den Client. Optional kann der Server auch so konfiguriert werden, dass auch der Client aufgefordert wird, dem Server sein X.509-Zertifikat zu übermitteln.

Die Identität der Kommunikationspartner wird hierbei über diese Zertifikate geprüft. X.509-Zertifikate enthalten die öffentlichen Schlüssel sowie eine Bestätigung einer weiteren Instanz, der Zertifizierungsstelle oder auch Trustcenter oder Certificate Authority (CA) genannt, über die korrekte Zuordnung des öffentlichen Schlüssels zu dessen "Besitzer". Der Wert eines Zertifikates hängt davon ab, welche Felder des X.509-Zertifikats von der Zertifizierungsstelle geprüft werden, bevor das Zertifikat ausgestellt wird, und wie vertrauenswürdig die Zertifizierungsstelle selbst ist. Daher spielt die Auswahl einer vertrauenswürdigen Zertifizierungsstelle eine wichtige Rolle.

Aufgrund der Vielzahl von Zertifizierungsstellen auf dem Markt sollte eine Institution die Zertifizierungsstelle sorgfältig auswählen. Es ist ratsam, die für den späteren Betrieb wesentlichen Auswahlkriterien im Vorfeld festzulegen. Zu diesen können beispielsweise gehören:

- ob das Root-Zertifikat schon in CA-Listen der Clients, wie dem Browser, enthalten ist,
- wo sich Sitz und Rechtsstand der Zertifizierungsstelle befinden, und auch wo der Sitz des technischen Betriebs sich befindet,
- was die geschäftliche Ausrichtung der Zertifizierungsstelle ist (Ist CA-Betrieb ein zentrales Geschäftsfeld?), was die angebotenen CA-Dienste umfassen (z. B. OSCP, CRL),
- welches Sicherheitsniveau die Zertifizierungsstelle nachweisen kann,
- wie gut Umfang und Qualität des technischen Supports sind sowie,
- wie hoch die Zertifikatskosten sind.

Grundsätzlich sollten die Kosten eines Zertifikats jedoch keinesfalls das allein ausschlaggebende Kriterium darstellen. Wird der angebotene Serverdienst von einem beschränkten Benutzerkreis verwendet, z. B. nur innerhalb eines LAN s, kann ein Zertifikat auch ohne die Beteiligung einer Zertifizierungsstelle selbst erstellt und signiert und auf alle Clients eingespielt werden, auf denen der Serverdienst genutzt werden soll.

Extended Validation Zertifikate

Um Angriffe mit gefälschten Webseiten zu erschweren und der Problematik entgegen zu wirken, dass diverse Zertifizierungsstellen SSL/TLS-Anträge nicht immer zuverlässig prüfen, wurden Extended Validation Zertifikate zum Umgang mit Zertifikaten mit höheren Sicherheitsanforderungen eingeführt. Diese sollen verhindern, dass, wenn ein Zertifikat ausgestellt wird, eine CA nur den Domainnamen prüft. Darüber hinaus soll die CA außerdem noch eindeutig nachvollziehen, von wem die betreffende Domain registriert wurde. Im Unterschied zu den normalen X.509 SSL/TLS-Zertifikaten wird bei diesen erweiterten Zertifikaten (Extended Validation SSL-Zertifikate, EV-SSL) die Identität des Antragstellers ausführlicher überprüft. Hierbei verpflichten sich die beteiligten Zertifizierungsstellen und Browser-Hersteller, die "Guidelines for the Issuance and Management of Extended Validation Certificates" des CA/Browser Forums einzuhalten. Danach sind unter anderem folgende Kriterien vom Antragsteller zu erfüllen:

- Identitätsnachweis und Adresse des Antragstellers,
- Nachweis, dass der Antragsteller alleiniger Eigentümer der Domain ist,
- Bestätigung, dass die antragstellende Person überhaupt berechtigt ist, den Antrag zu stellen und
- Nennung einer Hauptkontaktperson.

Zusätzlich darf der Antragsteller oder die antragstellende Person auf keiner Liste mit verbotenen Organisationen oder Personen stehen. Außerdem darf das Land, in dem sich der Sitz oder der Rechtsstand des Antragstellers befindet, weder Handelsembargos oder irgendwelchen anderen Sanktionen ausgesetzt sein, die durch dasjenige Land verhängt wurden, dessen Gesetzgebung die Zertifizierungsstelle unterliegt.

Für die Anwender sind EV-SSL-Zertifikate daran zu erkennen, dass in den unterstützten Browsern bestimmte Bereiche, wie die URL im Adressfeld oder das von vielen Browsern verwendete Vorhängeschlosssymbol, das eine verschlüsselte Seite kennzeichnet, grün hinterlegt ist. Je nach Konfiguration des Sicherheitsgateways (Firewall), hinter dem die Benutzer auf Webseiten mit EV-SSL-Zertifikaten zugreifen, kann es aber vorkommen, dass diese Markierungen in den Browsern der Clients nicht angezeigt werden. Wird beispielsweise der Nachrichtenfluss zwischen Client und Webserver von einem Proxy ent- und wieder neu verschlüsselt, wird im Browser lediglich das SSL/TLS-Zertifikat des Sicherheitsgateways angezeigt.

Neben den höheren finanziellen Kosten, die für die Ausstellung eines EV-SSL-Zertifikats entstehen können, dauert die Antragstellung in der Regel auch länger, da zusätzliche Informationen von der Zertifizierungsstelle überprüft werden. Wenn es möglich ist, wird empfohlen, diesen zusätzlichen Aufwand in Kauf zu nehmen. Insbesondere in Bereichen, in denen Informationen mit höherem Schutzbedarf bezüglich Vertraulichkeit und Integrität übertragen werden, sollten EV-SSL-Zertifikate bevorzugt eingesetzt werden.

Common Name Eintrag

Browser zeigen immer eine Sicherheitswarnung an, wenn der im Zertifikat einer Webseite eingetragene Common Name (Allgemeiner Name) nicht mit dem vollständigen DNS-Name (Fully Qualified Domain Name) übereinstimmt, über den der Server im Web erreichbar ist. Daher sollte sichergestellt sein, dass der Common Name zu der URL passt, die tatsächlich verwendet wird, um mit dem Server zu kommunizieren. Wenn es möglich ist, sollten Wildcard-Zertifikate (z. B. *.example.de) vermieden werden. Diese werden häufig eingesetzt, um mit einem einzelnen Zertifikat mehrere Subdomains abzusichern.

Vollständige Zertifikatskette

Da für die Prüfung der hierarchischen Zertifikatskette durch den Browser auch alle Zwischen-Zertifikate benötigt werden, reicht das SSL-Zertifikat des Servers alleine nicht aus. Deshalb sollte der Server so konfiguriert werden, dass beim Verbindungsaufbau alle erforderlichen Zertifikate an den Client gesendet werden. Dazu sollte die Zertifikatskette im Webserver entsprechend hinterlegt werden.

Zu beachten ist außerdem, dass neben Zertifikate, die fehlen, auch abgelaufene oder gesperrte Zertifikate die Prüfung der Zertifikatskette fehlschlagen lassen. Nur wenn alle Zertifikate gültig sind und beim Verbindungsaufbau übertragen wurden, kann die Zertifikatskette erfolgreich geprüft werden.

Auswahl einer SSL/TLS Protokollversion

Derzeit existieren fünf SSL/TLS-Protokollversionen: SSL v2, SSL v3, TLS v1.0, TLS v1.1 und TLS v1.2. SSL v1 wurde nicht veröffentlicht. Um eine sichere Verbindung zwischen Client und Server zu gewährleisten, sollte TLS 1.2 verwendet werden. TLS 1.1 bietet ausreichende Sicherheit, aber im Vergleich zu TLS 1.2 weist es jedoch einige Schwächen auf, z. B. sind in TLS 1.1 noch Cipher-Suites vorhanden, die auf IDEA und DES basieren, in TLS 1.2 nicht mehr. TLS 1.0 kann in bestehenden Anwendungen übergangsweise weiter eingesetzt werden, falls eine sofortige Migration zu TLS 1.1 oder vorzugsweise TLS 1.2 nicht möglich ist und geeignete Maßnahmen gegen Chosen-Plaintext-Angriffe (z. B. BEAST) auf die CBC-Implementierung getroffen werden. Generell sollte jedoch eine Migration zu TLS 1.2 schnellstmöglich erfolgen. SSL v2 und SSL v3 dürfen nicht mehr eingesetzt werden. Siehe hierzu auch den BSI-Migrationsleitfaden zum Mindeststandard TLS 1.2.

Sichere Cipher-Suites

SSL/TLS nutzt Cipher-Suites, die bestimmen, wie sicher eine HTTPS -Verbindung ist. Jede Suite besteht aus spezifischen Modulen. Wenn ein bestimmtes Modul als unsicher oder schwach eingestuft wird, kann durch die Veränderung der Cipher Suite zu einem sichereren Modul gewechselt werden.

Da die Verwendung schwacher Cipher Suites clientseitig erzwungen werden kann, ist es erforderlich, serverseitig nur solche anzubieten, die Authentisierung und Verschlüsselung mit einer ausreichenden Stärke einsetzen. Darüber hinaus sollten die verwendeten Cipher-Suites Perfect Forward Secrecy (PFS) unterstützen. Weitere Hinweise zu kryptographischen Algorithmen und Schlüssellängen sind in der Technischen Richtlinie des BSI "Kryptographische Verfahren: Empfehlungen und Schlüssellängen - Teil 2 Verwendung von TLS" (TR-02102-2) und in CON.1 Kryptokonzept enthalten.

Session Renegotiation/TLS-Kompression

Mittels der sogenannten Session Renegotiation (Session-Neuverhandlung) können sowohl Client als auch Server die Parameter einer bestehenden HTTPS-Sitzung neu aushandeln. Aufgrund eines Fehlers in der Spezifikation des TLS-Protokolls (RFC 5246) ist es einem Man-in-the-Middle-Angreifer möglich, die Session Renegotiation zu missbrauchen, um beliebige Inhalte in eine existierende HTTPS-Sitzung einzufügen. Mittlerweile wurde das TLS-Protokoll erweitert (RFC 5746) und dieser Designfehler behoben. Generell sollte überlegt werden, ob serverseitig die Session Renegotiation erforderlich ist. Ist dies der Fall, dann sollte diese sicher konfiguriert werden, also auf Basis des RFC 5746. Eine Renegotiation, die durch den Client initiiert wird, sollte vom Server abgelehnt werden.

Darüber hinaus sollte die TLS-Kompression deaktiviert werden.

Webserverspezifische Aspekte

Generell wird empfohlen, die auf Webservern zur Verfügung gestellten Inhalte bei der Übertragung vom Server zum Client und umgekehrt mittels SSL/TLS zu schützen.

Wenn möglich, sollte darauf verzichtet werden, Webseiten mit gemischten Inhalten anzubieten. Als Webseite mit gemischtem Inhalt wird eine Seite bezeichnet, die zwar Verschlüsselung nutzt, dabei aber auch unverschlüsselte Inhalte (z. B. JavaScript-, CSS-Dateien oder Bilder) einbindet. Ein Man-in-the-Middle-Angreifer kann die Übertragung einer einzelnen unverschlüsselten Datei ausnutzen, um eine HTTPS-Session zu übernehmen. Da Webseiten mit gemischten Inhalten zudem üblicherweise Browser-Warnungen erzeugen, wird dadurch die Benutzerfreundlichkeit verschlechtert.

HTTP Strict Transport Security (HSTS) ist eine weitere Methode, die gegen bekannte Schwächen von SSL schützt. Damit wird erschwert, dass ein Besucher durch einen Angriff oder serverseitige Konfigurationsprobleme von einer gesicherten auf eine ungesicherte Seite umgeleitet wird. Befindet sich ein Angreifer beispielsweise in demselben WLAN wie das Opfer, könnte er so die Session Cookies mitlesen und die HTTPS-Session übernehmen. Um HSTS zu aktivieren, muss der HSTS-Header auf dem Server konfiguriert werden.

Schutz des privaten Serverschlüssels

Ein besonders wichtiger Sicherheitsaspekt beim Einsatz von SSL/TLS ist der Schutz des privaten Serverschlüssels. Daher ist es ratsam, den Server so zu konfigurieren, dass der private Serverschlüssel beim Start des Servers durch Passworteingabe freigegeben werden muss. Besteht der Verdacht, dass der private Schlüssel kompromittiert wurde, so muss das zugrunde liegende Zertifikat widerrufen werden.

Validierung

Die Auswirkungen von Konfigurationsänderungen auf dem Server lassen sich nicht immer mit Bestimmtheit vorhersagen. Auch Software Updates können mitunter zu überraschenden Änderungen führen. Es wird daher empfohlen, die SSL/TLS Konfiguration vor der Freigabe zur Nutzung auf Fehler zu prüfen und den Status in periodischen Abständen (regelmäßig) zu validieren.

SYS.1.1.M19 Einrichtung lokaler Paketfilter

Das gesamte Netz einer Institution sollte durch ein entsprechendes Sicherheitsgateway geschützt sein. Server, die Dienste nach außen hin anbieten, sollten in einer Demilitarisierten Zone (DMZ) aufgestellt werden. Trotzdem ist es empfehlenswert, auch auf jedem Rechner entsprechende Zugangsbeschränkungen auf Anwendungs- oder Netzebene einzurichten. Dies gilt auch für Server, die nur intern genutzt werden und nicht zuletzt auch für Clients.

Ein lokaler Paketfilter kann einen Rechner gegen Angriffe schützen, die aus dem selben Subnetz heraus gestartet werden. Außerdem kann ein solcher Paketfilter dazu benutzt werden, eine feiner abgestufte Zugangskontrolle für einzelne Dienste zu realisieren, als dies beispielsweise mit Paketfiltern nur an Netzübergängen möglich ist.

Darüber hinaus kann ein lokaler Paketfilter auch dazu benutzt werden, ausgehende Netzverbindungen zu beschränken und so die Folgen einer Kompromittierung des Systems zu begrenzen. Ein solcher Schutz kann zwar eventuell von einem Angreifer nach einer erfolgreichen Kompromittierung des Rechners deaktiviert werden, andererseits wird ein Angreifer auf diese Weise zumindest behindert. Auf diese Weise kann entscheidende Zeit bei der Entdeckung und für mögliche Reaktionen gewonnen werden.

Zuletzt kann die Protokollfunktion eines lokalen Paketfilters es ermöglichen, bestimmte Angriffe überhaupt zu entdecken.

Praktisch alle aktuellen Betriebssysteme bieten die Möglichkeit, Filter zu definieren, die alle empfangenen oder zu sendenden Pakete nach bestimmten Regeln untersuchen und behandeln. Die Filtermöglichkeiten unterscheiden sich dabei zwischen den einzelnen Betriebssystemen teilweise erheblich. Praktisch immer können jedoch Regeln basierend auf der Quell- und Zieladresse des Pakets sowie auf dem verwendeten Protokolltyp (TCP/IP, UDP/IP, ICMP etc.) sowie gegebenenfalls dem Quell- oder Zielport definiert werden. Mit Hilfe von Paketfilterregeln können so beispielsweise Pakete, die von bestimmten Rechnern oder aus bestimmten Subnetzen stammen, gezielt verworfen werden.

Manche Serveranwendungen besitzen eigene Mechanismen, um den Zugang auf den Dienst für einzelne IP-Adressen oder Adressbereiche zu erlauben oder zu verbieten. Gegenüber diesen Mechanismen hat ein lokaler Paketfilter auf Betriebssystemebene den Vorteil, dass er den Dienst selbst gegen mögliche Angriffe schützt, die zu einer Kompromittierung führen, bevor die eingebaute Zugangsbeschränkung überhaupt wirksam werden kann.

Prinzipiell sollten alle Server mit hohem Schutzbedarf mit einem lokalen Paketfilter geschützt werden.

Es gibt zwei allgemeine Strategien, mit der Paketfilter-Regeln implementiert werden können: Die Blacklist-Strategie erlaubt alle Arten von Verbindungen, die nicht bestimmte Ausschlusskriterien erfüllen (Freizügige Strategie: "Alles ist erlaubt, was nicht explizit verboten ist"). Der Vorteil liegt dabei in einem eventuell geringeren Aufwand bei der Administration und der Fehlersuche. Ein schwerwiegender Nachteil ist jedoch, dass vergessene Regeln, die den Zugang auf nicht geschützte Netzdienste ermöglichen, als Grundlage für einen Angriff dienen können.

Demgegenüber werden bei der Whitelist-Strategie alle Arten von Verbindungen blockiert, die nicht zu einer Liste erlaubter Dienste gehören (Restriktive Strategie: "Alles ist verboten, was nicht explizit erlaubt ist").

Die Whitelist-Strategie bietet die größere Sicherheit und sollte daher grundsätzlich verwendet werden, wenn nicht wichtige Gründe dagegen sprechen. Der Nachteil liegt in einem tendenziell höheren Administrationsaufwand, da bei jeder Änderung der Anforderungen neue Regeln definiert werden müssen. In Ausnahmefällen, beispielsweise wenn ein Protokoll nicht auf fest definierten Ports arbeitet, kann auf die Blacklist-Strategie zurückgegriffen werden.

Es ist empfehlenswert, auf allen Servern im Rahmen der Grundkonfiguration einen lokalen Paketfilter mit einem Basis-Regelwerk einzurichten, bei dem grundsätzlich alle Verbindungsanfragen von außen abgewiesen werden. Dieses Regelwerk sollte aktiv sein, wenn das System ans Netz angeschlossen wird. Je nachdem welche Dienste von dem System angeboten werden sollen, können nach deren Konfiguration die dafür benötigten Protokolle und Ports freigeschaltet werden. Auch für Clients sollte dieses Vorgehen zumindest dann in Betracht gezogen werden, wenn diese besondere Anforderungen an die Sicherheit stellen.

Paketfilter erlauben meist ein detailliertes Protokollieren des Netzverkehrs. Das Aufsetzen eines lokalen Paketfilters ist daher auch in sicheren Netzen, die mit einem Sicherheitsgateway von einem unsicheren Netz wie dem Internet getrennt sind, sinnvoll, denn gewonnene Informationen können für die Erkennung von Angriffen hilfreich sein. Allerdings muss dabei darauf geachtet werden, dass keine Datenschutzbestimmungen verletzt werden. Gegebenenfalls sollten die entsprechenden Stellen (Datenschutzbeauftragter, Personalvertretung oder andere) beteiligt werden.

Problem ICMP

Das Internet Control Message Protocol ICMP wird dazu verwendet, Nachrichten über Fehler bei der Übertragung von IP-Paketen zu übermitteln. Beispielsweise existieren Nachrichten, die dem Sender eines Pakets mitteilen, dass das Zielnetz nicht erreichbar ist oder dass das Paket zu groß war, um an das Zielsystem weitergeleitet zu werden. Die Funktion der Tools ping und traceroute beruhen ebenfalls auf ICMP.

Neben vielen nützlichen Eigenschaften gibt es jedoch einige ICMP-Nachrichtentypen, mit denen Angreifer sich wichtige Informationen über ein Netz verschaffen und diese direkt für Angriffe benutzen können. Leider ist der radikale Ansatz, ICMP grundsätzlich am Sicherheitsgateway zu blockieren, ebenfalls keine befriedigende Lösung, da bestimmte Funktionen dann nicht mehr verfügbar sind. Auf ping und traceroute kann zwar in der Regel auf normalen Arbeitsplatzrechnern und Servern verzichtet werden, eine globale Blockierung von ICMP kann aber zu Beeinträchtigungen führen, die schwer zu diagnostizieren sind. Daher sollte überlegt werden sowohl am Sicherheitsgateway, als auch beim lokalen Paketfilter eine selektive ICMP-Filterung vorzunehmen, sofern dieser die entsprechenden Möglichkeiten zur Verfügung stellt. Dies sollte stets unter der Berücksichtigung des Einsatzzweckes des Rechners (Server oder Arbeitsplatzrechner), dessen Schutzbedarfs und die am Sicherheitsgateway getroffenen Maßnahmen geschehen. Beispielsweise kann für das interne Netz eine größere Zahl von Nachrichtentypen zugelassen werden, als für das externe Netz.

Umsetzung und Überprüfung

Welche Möglichkeiten der Filterung und Protokollierung zur Verfügung stehen, unterscheidet sich je nach Betriebssystem. Vor dem Aufsetzen eines lokalen Paketfilters sollte die vorhandene Dokumentation zu Rate gezogen werden.

Bei der Einrichtung von Paketfilterregeln sollte mit großer Sorgfalt vorgegangen werden, da ein Fehler in einer Regel unter Umständen dazu führen kann, dass sich ein Administrator, der über das Netz auf dem Rechner arbeitet, auf diese Weise "aussperrt" und die Korrekturen von der Systemkonsole aus vornehmen muss.

Nach dem Aktivieren des lokalen Paketfilters sollte einerseits geprüft werden, ob die benötigten Dienste noch erreichbar sind, andererseits sollte mit einem Portscan überprüft werden, ob die restlichen Ports alle blockiert sind.

SYS.1.1.M20 Beschränkung des Zugangs über Netze

Der Einsatz eines Sicherheitsgateways und eine geeignete Netzsegmentierung verringern die Angriffsfläche eines Servers. Diese Empfehlungen können aber nicht direkt auf einen Server umgesetzt, sondern müssen schon während der Netzplanung berücksichtigt werden. Vertiefende Informationen sind im NET1.1 Netzarchitektur und -design zu finden.

SYS.1.1.M21 Betriebsdokumentation

Um einen reibungslosen Betriebsablauf zu gewährleisten, müssen Administratoren einen Überblick über das System haben bzw. sich verschaffen können. Dieses muss auch für deren Vertreter möglich sein, falls ein Administrator unvorhergesehen ausfällt. Der Überblick ist auch Voraussetzung, um Prüfungen des Systems (z. B. auf problematische Einstellungen, Konsistenz bei Änderungen) durchführen zu können.

Daher sollten die Veränderungen, die Administratoren am System vornehmen, dokumentiert werden, nach Möglichkeit automatisiert. Dieses gilt insbesondere für Änderungen an Systemverzeichnissen und -dateien.

Bei Installation neuer Betriebssysteme oder bei Updates sind die vorgenommenen Änderungen besonders sorgfältig zu dokumentieren. Durch die Aktivierung neuer oder durch die Änderung bestehender Systemparameter kann das Verhalten eines IT-Systems (insbesondere auch Sicherheitsfunktionen) maßgeblich verändert werden.

SYS.1.1.M22 Einbindung in die Notfallplanung

Der teilweise oder komplette Ausfall eines Servers kann gravierende Auswirkungen haben, wenn der Server wesentlicher Bestandteil innerbetrieblicher Arbeitsabläufe ist oder ein öffentlich zugängliches Angebot unterstützt (etwa in E-Commerce- oder E-Government-Anwendungen).

Im Rahmen der Notfallvorsorge ist daher ein Konzept zu entwerfen, wie die Folgen eines Ausfalls minimiert werden können und welche Aktivitäten im Falle eines Ausfalls durchzuführen sind.

Folgende Aspekte müssen dabei berücksichtigt werden:

- Die Notfallplanung für den Server muss in den existierenden Notfallplan integriert werden (siehe auch Baustein DER.4 Notfallmanagement).
- Durch einen Systemausfall kann es auch zu Datenverlusten kommen. Daher ist im Rahmen des allgemeinen Datensicherungskonzepts (siehe auch OPS.1.1.5 Datensicherung) ein Datensicherungskonzept für den Server zu erstellen. Darin muss nicht nur der Server selbst berücksichtigt werden, sondern auch die Systeme, von denen der Betrieb des Servers abhängt bzw. für die der Betrieb des Servers notwendig ist.
- Im Rahmen von Wartungs- und Serviceverträgen oder durch eigene Lagerhaltung muss die Versorgung mit Ersatzteilen innerhalb einer Frist sichergestellt werden. Die Ausfallzeit ist daher auf ein tragbares Maß zu reduzieren. Bei besonderen Anforderungen an die Verfügbarkeit des Servers muss gegebenenfalls eine Hochverfügbarkeitslösung eingesetzt werden.
- Die Systemkonfiguration muss dokumentiert werden. Wichtige Aufgaben müssen so beschrieben sein, dass das Gesamtsystem im Notfall auch ohne vorherige Kenntnis dieser Systemkonfiguration wiederhergestellt werden kann. Die Dokumentation sollte keinesfalls ausschließlich elektronisch vorliegen, sondern Handlungsanweisungen sollten auch in Papierform existieren. Gegebenenfalls können Konfigurationsdateien auch auf externe Datenträger geeignet hinterlegt werden.
- Es muss ein Wiederanlaufplan erstellt werden, der das geregelte Hochfahren des Systems gewährleistet. Hierzu sollte im Vorfeld ein Bootmedium erstellt werden, siehe Anschnitt "Bootmedium".
- Alle notwendigen Vorgehensbeschreibungen müssen regelmäßig überprüft und geprobt werden. Eventuell müssen variierende Vorgehensweisen bei unterschiedlichen Betriebssystemen berücksichtigt werden.

Bootmedium

Bei der Einrichtung eines Rechners sollte ein Bootmedium erstellt werden, das bei Ausfall einer Festplatte zum Starten des Systems oder bei Auftreten eines Schadprogramms zum Erzeugen eines kontrollierten Systemzustands genutzt werden kann. Solche Medien können beispielsweise CDs sein, deren Erstellung das jeweilige Betriebssystem eventuell anbietet, es können aber auch eigens eingerichtete CDs oder portable Laufwerke (beispielsweise USB-Sticks oder externe Festplatten mit USB- oder Firewire-Schnittstelle) erstellt werden. Neben "physischen" Medien können auch Image-Dateien verwendet werden, die erst bei Bedarf auf das Bootmedium kopiert oder gebrannt werden. Art und Umfang des Notfall-Bootmediums richten sich nach dem Einsatzzweck des Rechners und den vorhandenen Schnittstellen.

Das Notfall-Bootmedium kann unter anderem bei folgenden Problemen eingesetzt werden:

- Datenverlust durch Fehlbedienung,
- Bedienungs- und Administrationsfehler, die die Benutzung und einen Neustart verhindern,
- Infektion des Systems mit Schadprogrammen (beispielsweise Computer-Viren),
- Kompromittierung des Systems durch einen Angreifer, oder auch
- Hardware-Probleme.

Idealerweise sollte das Notfall-Bootmedium alle Programme und Daten enthalten, die zu einer Untersuchung und - falls möglich - der Behebung der Probleme benötigt werden. Gegebenenfalls können unterschiedliche Medien für verschiedene Problemszenarien erstellt werden.

Als "Grundausstattung" für ein Notfall-Bootmedium werden folgende Programme empfohlen:

- Viren-Schutzprogramme mit aktuellen Signaturen, beziehungsweise die Möglichkeit, aktuelle Signaturen einzupflegen,
- Programme zur Bearbeitung von Konfigurationsdateien oder Datenbanken des Systems (Editoren für Dateien, Registry oder ähnliches),
- Programm zur Wiederherstellung des Bootsektors und des MBR (Master Boot Record) der Systemplatte,
- Backup- / Recovery-Programme,
- Diagnoseprogramme zur Analyse von Hardware-Defekten.

Darüber hinaus können Programme zur weitergehenden Analyse hinzugefügt werden, etwa zur forensischen Untersuchung eines kompromittierten Systems.

Dabei ist es wichtig, dass alle Programme und Bibliotheken ausschließlich vom Bootmedium geladen werden. Es dürfen keine Komponenten des installierten Systems verwendet werden. Bei der Erstellung des Bootmediums ist außerdem darauf zu achten, dass neben den notwendigen Programmen auch alle Treiber vorhanden sind, die für den Zugriff auf die eingebauten Platten des Rechners benötigt werden. Dazu zählen beispielsweise Treiber für Festplattencontroller (insbesondere RAID-Controller) und Treiber für eine Festplattenverschlüsselung oder Festplattenkomprimierung.

In der Regel können auch weitere Programme oder Dokumentation auf dem Medium gespeichert werden. Beispielsweise kann es die Effizienz der Fehlersuche erhöhen, wenn auf dem Bootmedium stets eine aktuelle Dokumentation der Systemkonfiguration enthalten ist.

Das Notfall-Bootmedium muss selbst frei von Viren und anderen Schadprogrammen sein. Es dürfen deshalb nur Programme eingesetzt werden, die aus vertrauenswürdigen Quellen (etwa direkt vom Hersteller) stammen oder deren digitale Signatur überprüft wurde. Zumindest einmal nach der Erstellung sowie bei jeder Änderung sollte das Bootmedium außerdem mit einem Viren-Schutzprogramm überprüft werden.

Es ist nicht unbedingt notwendig, für jedes System ein eigenes Bootmedium zu erstellen. Ein entsprechend flexibel angelegtes Bootmedium kann für eine große Anzahl verschiedener Systeme ausreichend sein. Auf dem Bootmedium braucht nicht einmal notwendigerweise das selbe Betriebssystem eingesetzt zu werden, wie auf dem Zielsystem selbst. Aus Gründen der Kompatibilität ist dies jedoch oft vorteilhaft. Es muss allerdings unbedingt durch entsprechende Tests sichergestellt werden, dass das Medium auch wirklich bei allen Rechnern funktioniert, für die es eingesetzt werden soll. Je nach Betriebssystem müssen außerdem noch systemspezifische Aspekte beachtet werden, die in den jeweiligen IT-Grundschutz-Bausteinen beschrieben werden.

Nach Veränderungen am Zielsystem, etwa einem Update des Betriebssystems oder Konfigurationsänderungen, muss gegebenenfalls das Notfall-Bootmedium und die darauf gespeicherte Dokumentation aktualisiert werden. Änderungen am Bootmedium müssen dokumentiert werden.

Das Notfall-Bootmedium muss für die Systembetreuer schnell greifbar sein, damit im Falle einer Störung nicht wertvolle Zeit verloren geht. Andererseits muss es auch so sicher aufbewahrt werden, dass Unbefugte keinen Zugang darauf haben.

Die Funktion des Notfall-Bootmediums sollte regelmäßig getestet und die Bedienung der darauf gespeicherten Programme geübt werden, damit sichergestellt ist, dass das Medium im Fall von Problemen funktioniert und die Administratoren mit der Bedienung vertraut sind. Es sollte überlegt werden, mit dem Medium eine kurze gedruckte Anleitung aufzubewahren, die für typische Einsatzszenarien die wichtigsten Schritte zusammenfasst.

SYS.1.1.M23 Systemüberwachung

Um auf kritische Systemereignisse reagieren zu können, sollte für Server ein geeignetes Systemüberwachungs- bzw. Monitoringkonzept erstellt werden. Dazu gehört, dass Systemzustand und Funktionsfähigkeit der Servers und der darauf betriebenen Dienste laufend überwacht werden. Wenn Fehler auftreten oder definierte Grenzwerte über- oder unterschritten werden, sollte dies automatisch an das Betriebspersonal gemeldet werden.

Hierfür werden in der Regel Statusinformationen von einem zentralen IT-System abgerufen, auf dem die Ereignisse ausgewertet werden. Über die Schnittstelle, die benötigt wird, um die Systemereignisse vom IT-System abzurufen, können aber oft Systemeinstellungen des Betriebssystems verändert werden, z. B. über SNMP (Simple Network Management Protocol). Ist eine solche Modifikation nicht gewünscht, dann sollten diese Merkmale deaktiviert werden.

SYS.1.1.M24 Sicherheitsprüfungen

Es sollte regelmäßig, mindestens monatlich, ein Sicherheitscheck der Server durchgeführt werden. Für praktisch alle Betriebssysteme sind Programme verfügbar oder bereits im Lieferumfang des Betriebssystems oder der Betriebssystem-Distribution enthalten, die entsprechende Funktionen zur Verfügung stellen.

Bei einem solchen Sicherheitscheck sollten beispielsweise folgende Punkte überprüft werden:

- Gibt es Benutzer ohne Passwort?
- Gibt es Benutzer, die längere Zeit die Server nicht mehr benutzt haben?
- Gibt es Benutzer, deren Passwort nicht die erforderlichen Bedingungen einhält?
- Welche Benutzer besitzen die Administrator-Rechte?
- Sind Systemprogramme und Systemkonfiguration unverändert und konsistent?
- Entsprechen die Berechtigungen von
  - Systemprogrammen und Systemkonfiguration
  - Anwendungsprogrammen und -daten
  - Benutzerverzeichnissen und -daten
  - den Vorgaben der Sicherheitsrichtlinie?
- Welche Netzdienste laufen auf den einzelnen Systemen? Sind sie den Vorgaben der Sicherheitsrichtlinie entsprechend konfiguriert?

Bei einem regelmäßigen Sicherheitscheck können auch Penetrationstests im lokalen Subnetz integriert werden. Dabei kann der "Grad" der Penetrationstests variiert werden (beispielsweise: wöchentlich einfache automatisierte Überprüfungen, monatlich gründlicherer Test mit teilweise manueller Durchführung, einmal jährlich ein grundlegender Test des gesamten Netzes).

Bei der Durchführung des Sicherheitschecks sollten die Administratoren ihre Schritte so dokumentieren, dass sie (beispielsweise bei einem Verdacht auf ein kompromittiertes System) nachvollzogen werden können. Die Ergebnisse des Sicherheitschecks müssen dokumentiert werden, Abweichungen vom "Sollzustand" muss nachgegangen werden.

SYS.1.1.M25 Geregelte Außerbetriebnahme eines Servers

Soll ein Server außer Betrieb genommen werden, so darf dies nicht unvorbereitet und ohne Ankündigung für die Benutzer geschehen, sondern es muss eine Reihe von Maßnahmen ergriffen werden, um sicher zu stellen, dass

- keine wichtigen Daten verloren gehen,
- keine Dienste oder Systeme beeinträchtigt werden, die von dem Server abhängen, und dass
- keine sensitiven Daten auf den Datenträgern des Servers zurück bleiben.

Dazu ist es insbesondere wichtig, einen Überblick darüber zu haben, welche Daten wo auf dem System gespeichert sind und von wo aus darauf zugegriffen wird. Ausgehend von diesen Informationen sollte eine Planung für die Außerbetriebnahme des Servers erfolgen. Dabei sollten die folgenden Punkte berücksichtigt werden:

- Datensicherung
  Vor der Außerbetriebnahme des Servers müssen Daten, die noch benötigt werden, entweder extern gesichert bzw. archiviert (beispielsweise auf Magnetbändern, CD - oder DVD-ROMs) oder auf ein Ersatzsystem übertragen werden. Nach der Sicherung sollte überprüft werden, dass wirklich alle Daten korrekt gesichert wurden. Weitere Informationen zu diesem Themenkomplex finden sich in den Bausteinen OPS.1.1.5 Datensicherung und OPS.1.2.2 Archivierung.
- Ersatzsystem
  Wenn die von dem Server bereitgestellten Dienste weiter benötigt werden, so muss rechtzeitig ein angemessenes Ersatzsystem bereitgestellt werden. Für die entsprechende Planung, Beschaffung und Inbetriebnahme müssen entsprechende Ressourcen zur Verfügung stehen, siehe auch Abschnitt "Migration eines Servers".
- Information der Benutzer
  Falls das System ersatzlos abgeschaltet wird, so müssen die Benutzer rechtzeitig über die bevorstehende Abschaltung informiert werden und gegebenenfalls die Gelegenheit erhalten, eigene Daten zu sichern.
- Entfernen von Verweisen auf das System
  Im Zuge der Außerbetriebnahme eines Systems müssen auch Verweise auf das System gelöscht werden. Dazu gehört beispielsweise das Löschen des DNS-Eintrags und der Einträge in sonstigen Verzeichnisdiensten sowie in Abhängigkeit vom Einsatzzweck weitere Verweise. Wird beispielsweise ein Webserver außer Betrieb genommen, so sollten Verweise auf diesen Server, die noch in eigenen Webseiten enthalten sind, gelöscht werden.
- Löschen der Daten auf dem abzuschaltenden System
  Es muss sichergestellt werden, dass keine schützenswerten Informationen mehr auf den Datenträgern vorhanden sind. Dazu genügt es nicht, die Platten einfach neu zu formatieren, sondern sie müssen mindestens einmal vollständig überschrieben werden. Es ist zu beachten, dass weder das logische Löschen mit den Löschfunktionen des Betriebssystems noch das Neuformatieren der Platten die Daten tatsächlich von den Datenträgern entfernt. Mit geeigneter Software können Daten in solchen Fällen, oft sogar ohne großen Aufwand, wieder rekonstruiert werden.
- Löschen von Datensicherungsmedien
  Nach der Außerbetriebnahme eines Systems müssen gegebenenfalls auch die entsprechenden Datensicherungsmedien gelöscht oder unbrauchbar gemacht werden, wenn die darauf gespeicherten Daten nicht mehr benötigt werden.
- Entfernen sonstiger Informationen
  Oft enthalten Serversysteme weitere Daten (beispielsweise Konfigurationsdaten), die in einem nichtflüchtigen Speicher abgelegt sind, oder sind von außen beschriftet (beispielsweise mit dem Rechnernamen, der IP-Adresse und weiteren technischen Informationen). Diese Informationen sollten nach Möglichkeit vor der Weitergabe des Gerätes entfernt werden, da ein Angreifer auch aus solchen Informationen eventuell Hinweise für mögliche Angriffe ziehen kann.

Es wird empfohlen, anhand der oben gegebenen Empfehlungen eine Checkliste zu erstellen, die bei der Außerbetriebnahme eines Systems abgearbeitet werden kann. Auf diese Weise kann vermieden werden, dass einzelne Schritte vergessen werden.

Migration eines Servers

Sollen die Dienste des Servers von einem anderen System übernommen werden, so muss der Übergang geplant werden. Insbesondere dann, wenn besondere Anforderungen an die Verfügbarkeit der Dienste bestehen, ist eine besonders sorgfältige Planung erforderlich.

In den meisten Fällen ist es empfehlenswert, den "Funktionsübergang" auf das Ersatzsystem außerhalb der normalen Betriebszeiten durchzuführen. Falls dies nicht möglich ist müssen Maßnahmen getroffen werden, die sicher stellen, dass weder Daten beim Funktionsübergang verloren gehen, noch untragbare Ausfallzeiten entstehen.

Für die Migration wichtiger Server muss deswegen vorab ein entsprechendes Migrationskonzept erstellt werden. Dabei sollten insbesondere folgende Punkte mit berücksichtigt werden:

- Migration der Daten und Konfiguration
  Nach der Übertragung der Daten auf das neue System muss überprüft werden, ob die Daten vollständig und korrekt übertragen wurden.
  Wenn auf dem neuen System eine neue Version der Serversoftware eingesetzt werden soll, so muss sichergestellt sein, dass die neue Version mit den vorhandenen Datenbeständen korrekt umgehen kann. Dies betrifft nicht nur die Aufgabe, Daten der alten Version korrekt einzulesen, sondern insbesondere auch, diese Daten zu modifizieren oder neue Datensätze hinzuzufügen. Gerade in solchen Fällen tauchen oft Probleme auf, so dass gründliche Tests empfohlen werden.Außerdem ist es wichtig, dass die Konfiguration des alten Dienstes auf dem neuen System korrekt übernommen oder zumindest "funktional äquivalent nachgebaut" werden kann.
- Kompatibilität des Dienstes
  Es muss sichergestellt sein, dass der Dienst auf dem Ersatzsystem mit dem ursprünglichen Dienst kompatibel ist. Dies ist insbesondere dann von Bedeutung, wenn im Rahmen der Migration auf dem neuen System eine neue Version des Serverprogramms eingesetzt werden soll, auf die jedoch weiter mit Clients der alten Version zugegriffen wird. Selbst dann, wenn ein Hersteller Berichte von Referenzkunden über erfolgreiche Migrationen vorlegt oder "problemlose Abwärtskompatibilität", "vollständige Rückwärtskompatibilität mit früheren Versionen" oder ähnliches zusichert, wird dringend empfohlen, vorab entsprechende Tests durchzuführen.
- Kryptographische Schlüssel
  Falls Teile der Daten oder der Dateisysteme eines Servers verschlüsselt sind, so kommt der Sicherung oder Übertragung der entsprechenden kryptographischen Schlüssel besondere Bedeutung zu: Oft sind diese an einer anderen Stelle auf dem System gespeichert als die Nutzdaten selbst. Beispielsweise dann, wenn die Daten mit Hilfe systemnaher Programme blockweise direkt kopiert werden oder die Festplatten aus dem alten in das neue System umgebaut werden, muss sichergestellt sein, dass auch die kryptographischen Schlüssel mit übertragen werden, da sonst kein Zugriff mehr auf die verschlüsselten Daten möglich ist.
- Umstellung von Namen und Adressen
  Falls auf einen Server nur über seine IP-Adresse oder einen DNS-Namen zugegriffen wird, so ist eine Migration meist relativ unproblematisch, da in diesem Fall einfach das Ersatzsystem die IP-Adresse des alten Systems übernehmen kann. Problematischer wird es beispielsweise, wenn das neue System den selben DNS-Namen bekommen soll, aber nicht die IP-Adresse übernehmen kann. Denn es dauert eine gewisse Zeit, bis die Änderung der Adresse bei allen Clients "angekommen" ist. Solche Latenzzeiten müssen bei der Planung der Migration berücksichtigt werden.
  Falls auf das System anders zugegriffen wird (beispielsweise wenn die Adresse von einem anderen Verzeichnisdienst aufgelöst wird), so muss berücksichtigt werden, dass auch die Änderung auf diesem Weg eventuell ebenfalls eine gewisse Latenzzeit hat, bevor sie wirksam wird.
  Das größte Problem entsteht dann, wenn Clients auf den Servern über eine Anwendung zugreifen, bei der die IP-Adresse oder der Name des Servers in einer lokalen Konfigurationsdatei oder -datenbank gespeichert sind. Falls eine größere Anzahl Clients manuell umkonfiguriert werden müssen, so kann dies eine erhebliche Zeit in Anspruch nehmen und muss vorab geplant werden.
- Dauerhafte Verbindungen
  Falls es Clients gibt, die länger bestehende oder gar dauerhafte Netzverbindungen zu dem Dienst aufbauen, der auf einen neuen Rechner migriert werden muss (dies ist beispielsweise bei manchen Datenbankanwendungen der Fall), so muss dies bei der Migration berücksichtigt werden. Gegebenenfalls müssen diese Verbindungen auf den betreffenden Clients manuell beendet werden. Auch hierfür ist eine entsprechende Planung erforderlich.

Für die Durchführung der Migration ist es empfehlenswert, im Rahmen der Erarbeitung des Migrationskonzeptes eine Checkliste zu erstellen, die bei der Umstellung Schritt für Schritt durchgegangen werden kann. Bei der Planung der Migration und der Erstellung der Checkliste muss darauf geachtet werden, dass jeder Schritt nur von den vorhergehenden Schritten abhängig ist.

Bei hohen Anforderungen an die Verfügbarkeit des Dienstes sollte der gesamte Übergang vorab in einer Testumgebung unter möglichst realistischen Bedingungen geprobt werden, um mögliche Probleme frühzeitig zu identifizieren und zu beseitigen.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

SYS.1.1.M26 Mehr-Faktor-Authentisierung (C)

Zur Authentisierung gibt es unterschiedliche Verfahren, die auf folgenden Faktoren basieren können: Wissen, Besitz und biometrische Merkmale. Bei einem höheren Schutzbedarf wird eine Mehr-Faktor-Authentisierung empfohlen, bei der zwei der drei Faktoren verwendet werden.

Am gebräuchlichsten ist die Nutzung der Faktoren Wissen und Besitz. Der Authentisierungsschlüssel wird hierbei in einer Hardware, z. B. Chipkarte, gespeichert (Faktor Besitz), die nur nach Eingabe einer PIN oder eines Passwortes eingesetzt werden kann (Faktor Wissen). Je nach Sicherheitsanforderungen können Schlüssel auch auf Clients (z. B. Notebook) bzw. Servern im Netz der Institution gespeichert sein.

Alternativ kann die Nutzung einer Public-Key-Infrastruktur (PKI) empfohlen werden, die auf digitale Signaturen und asymmetrischen Kryptografieverfahren basiert. Die Gültigkeit der Signaturen wird über eine anerkannte Zertifizierungsstelle (CA – Certificate Authority) überprüft. Die Länge des Schlüssels bzw. der Signatur korreliert mit der Sicherheit des verwendeten Kryptoverfahrens.

SYS.1.1.M27 Hostbasierte Angriffserkennung (IA)

Mit dem Einsatz von hostbasierten Angriffserkennungssystemen (Host-based Intrusion Detection Systems, IDS) sollte das Systemverhalten auf Anomalien und Missbrauch hin überwacht werden. Die eingesetzten IDS-Mechanismen sollten geeignet ausgewählt, konfiguriert und ausführlich getestet werden. Im Falle einer Angriffserkennung muss eine geeignete Alarmierung des Betriebspersonals sichergestellt sein (siehe Baustein NET.3.4 IDS/IPS).

Regelmäßige Integritätsprüfung

Eine regelmäßige Kontrolle des Dateisystems, der Dateiattribute und der Prozessinformationen sowie weiterer wichtiger Elemente der Systemkonfiguration (beispielsweise unter Windows die Registry) auf unerwartete Veränderungen helfen dabei, Inkonsistenzen zu erkennen. Die Erkennung solcher Inkonsistenzen kann zur Vorbeugung gegen Systeminstabilitäten eingesetzt werden. Es können dadurch aber auch Angriffe zeitnah entdeckt werden. Sollte tatsächlich ein Angriff vorliegen, ist es wichtig, das Vorgehen des Angreifers zu rekonstruieren. Dies dient einerseits dazu, Manipulationen an Daten aufzudecken, und andererseits dazu, verborgene Hintertüren zu erkennen, die ein Angreifer für einen späteren Zugang auf den Rechner installiert haben könnte.

Berechnung kryptographischer Prüfsummen

Zur Erkennung von Manipulationen können Programme genutzt werden, die kryptographische Prüfsummen über einen Großteil der Dateien des Systems oder über andere Ressourcen berechnen. Zu unterscheiden sind dabei Integritätsprüfungsprogramme, welche nur auf Dateiebene arbeiten, und solche, die auch Prozesse und spezielle Konfigurationsdaten, wie die Windows-Registry oder Datenstrukturen des Kernels, überprüfen können. Es wird empfohlen, darauf zu achten, dass diese Werkzeuge auch zentral administriert und überwacht werden können. Außerdem müssen die von den Programmen verwendeten kryptographischen Mechanismen dem Stand der Technik entsprechen.

Einige Programme stellen lediglich fest, ob Veränderungen am Dateisystem durchgeführt wurden. Hierzu prüfen sie, ob die Zugriffsrechte, das Datum der letzten Modifikation oder die Inhalte der jeweiligen Datei geändert wurden. Modifikationen werden erkannt, indem die vorher erstellte kryptographische Prüfsumme mit der aktuell berechneten Prüfsumme verglichen wird. Mit einer speziellen Einstellung kann in vielen Fällen auch ein nur lesender Zugriff auf die Datei bemerkt werden.

Schutz der Prüfsummendatei

Um zu verhindern, dass das Integritätsprüfungsprogramm selbst oder die Datei, welche die Prüfsummen des Systems enthält, von einem Angreifer oder durch Schadsoftware verfälscht werden können, sollten sich diese auf einem schreibgeschützten Datenträger befinden. Allerdings muss die Prüfsummendatei bei erlaubten Veränderungen am Dateisystem ebenfalls geändert werden, so dass sich CDs, DVDs oder Wechselplatten für diesen Zweck empfehlen. Alternativ kann die Prüfsummendatei auch über das Netz schreibgeschützt zur Verfügung gestellt werden. Bei einer Verwaltung des Integritätsprüfungsprogramms über das Netz sollte dieser Weg auch bevorzugt werden. Einige Schadprogramme tarnen sich, so dass sie mit Methoden des manipulierten Betriebssystems nicht erkannt werden können. Daher ist es im Verdachtsfall sinnvoll, das System mittels eines manipulationsfreien Betriebssystems zu untersuchen. Dazu kann beispielsweise über ein vertrauenswürdiges Referenzsystem ein externer Datenträger erstellt werden, von dem dann das manipulationsfreie Betriebssystem gestartet wird.

Prüfintervall und Prüfumfang

Eine Integritätsprüfung sollte regelmäßig, beispielsweise jede Nacht, durchgeführt werden. Die Wahl eines geeigneten Prüfintervalls hängt stark vom Einsatzzweck des jeweiligen IT-Systems beziehungsweise der Einsatzumgebung ab. Bei der Durchführung von Integritätsprüfungen ist außerdem der Verbrauch an Speicherplatz und Rechenzeit, der für die Überprüfung der Prüfsummen notwendig ist, zu berücksichtigen. Der Einsatz des Integritätsprüfungsprogramms darf den ordnungsgemäßen Betrieb nicht beeinträchtigen.

Im normalen Betrieb jedes größeren IT-Systems ergeben sich ständig kleinere und größere Änderungen an Systemdateien. Generell ist es daher empfehlenswert, das Integritätsprüfungsprogramm so zu konfigurieren, dass nur Veränderungen an relevanten Dateien erfasst werden. Anderenfalls besteht die Gefahr, dass sehr viele Änderungsmeldungen ausgelöst werden, die auf ganz normale betriebliche Abläufe und nicht auf Angriffsversuche zurückzuführen sind (false positives). Als Folge kann es passieren, dass die Protokolldateien nicht mehr zeitnah ausgewertet werden können.

Prozessinformationen im Arbeitsspeicher

Neben dateibasierten Integritätsprüfungen gibt es auch die Möglichkeit, Prozessinformationen aus dem Arbeitsspeicher gegen eine Liste erlaubter Prozesse (Whitelist) zu prüfen. Auf diese Weise lassen sich auch bestimmte Manipulationen erkennen, die keine Spuren im Dateisystem hinterlassen. Andererseits gibt es Manipulationen, die nicht die Prozesse selbst, sondern nur deren Konfiguration betreffen. Solche Manipulationen lassen sich unter Umständen leichter durch eine Integritätsprüfung der Konfigurationsdateien aufdecken. Integritätsprüfungen des Dateisystems und des Arbeitsspeichers haben somit teilweise unterschiedliche Schutzwirkungen. Ein Vorteil der Prüfung von Prozessinformationen im Arbeitsspeicher ist, dass dazu nur wenige oder keine Festplattenzugriffe nötig sind, die deutlich langsamer sind als Arbeitsspeicherzugriffe. Dadurch kann wesentlich häufiger geprüft werden als bei einer dateibasierten Methode, bei der viele Informationen von der Festplatte gelesen werden müssen. So können unerwünschte Programme meist schneller entdeckt werden als bei einer dateibasierten Integritätsprüfung.

Benachrichtigung

Eine Benachrichtigung über das Ergebnis sollte, auch wenn keine Veränderungen festgestellt wurden, automatisch per E-Mail oder einen ähnlichen Weg an den IT-Betrieb erfolgen. Vorab sollte festgelegt werden, welche Maßnahmen einzuleiten sind, wenn ein Integritätsverlust festgestellt wird. Wichtig ist beispielsweise, ob automatische oder manuelle Aktionen durchgeführt werden.

SYS.1.1.M28 Redundanz (A)

Die Verfügbarkeit von Geschäftsprozessen, Anwendungen und Diensten hängt oft von der Funktion eines zentralen Servers ab. Je mehr Anwendungen aber auf einem Server laufen, desto ausfallsicherer muss dieser sein. Ein Server enthält in der Regel verschiedene potentielle Fehlerquellen ("Single Points of Failure"), also Komponenten, deren Ausfall den Ausfall des Gesamtsystems auslösen kann: Festplatten, Stromversorgung, Lüfter, Backplane, etc. Die Wiederherstellung des Gesamtsystems kann in diesem Fall erhebliche Zeit in Anspruch nehmen. Neben der Vorhaltung von Ersatzteilen können zusätzlich folgende Möglichkeiten zur Steigerung der Verfügbarkeit eingesetzt werden:

- Cold-Standby
- Hot-Standby (manuelles Umschwenken)
- Cluster (automatisches Umschwenken)
- Load balanced Cluster
- Failover Cluster

Jede einzelne dieser Techniken bietet ein unterschiedliches Niveau an Verfügbarkeit und ist in der Regel mit unterschiedlichen Kosten verbunden. Unter Umständen kann eine höhere Verfügbarkeit erzielt werden, wenn die betroffenen Server virtualisiert werden (siehe SYS.1.5 Server-Virtualisierung).

Cold-Standby

Beim Cold-Standby wird neben dem eigentlichen Produktivsystem ein zweites baugleiches Ersatzsystem bereitgehalten, das aber nicht aktiv ist. Wenn das erste System ausfällt, kann das Ersatzsystem manuell hochgefahren und ins Netz integriert werden.

Nach der Vorhaltung von einzelnen Ersatzteilen ist dies die einfachste Redundanz-Lösung, die mit den entsprechenden Vorteilen und Nachteilen verbunden ist:

Vorteile einer Cold-Standby Lösung:

- Cold-Standby Lösungen bringen keine Komplexitätserhöhung für das Gesamtsystem mit sich.
- Die Kosten für ein Cold-Standby System belaufen sich lediglich auf die Kosten der zusätzlichen Hardware und sind somit am geringsten unter den vorgestellten Möglichkeiten.
- Neuaufsetzen oder Änderungen im System sind ohne Verfügbarkeitseinbußen möglich. Der Produktivbetrieb wird dafür während der Änderungen auf das Cold-Standby System umgelegt.

Nachteile einer Cold-Standby Lösung

- Zum bestehenden System muss ein zweites System vorgehalten werden.
- Das Ersatzsystem muss ständig auf dem aktuellen Konfigurations- und Patch-Stand gehalten werden.
- Da das Ersatzsystem manuell aktiviert werden muss, müssen Administratoren das System kontinuierlich überwachen und im Notfall einschreiten.
- Wenn die Applikationsdaten nicht auf einem externen Speichersystem liegen, so dass der Zugang direkt aus dem Ersatzsystem möglich ist, dann müssen diese auf das Cold-Standby System migriert werden.

Der Einsatz eignet sich gut für Server mit Anwendungen, bei denen kurze bzw. begrenzte Ausfallzeiten, bis ein Eingriff des IT-Betriebs möglich ist, unkritisch sind. Beispiele dafür sind:

- Server in kleineren Netzen (Intranet)
- Wenig frequentierte Server im Internet

Hot-Standby (manuelles Umschwenken)

Bei einem Hot-Standby steht ebenfalls ein Ersatzsystem bereit, das aber neben dem Produktivsystem parallel in Betrieb gehalten wird. Die Funktion des Produktivsystems wird überwacht, bei Ausfall wird das Ersatzsystem aktiv. Der Wechsel kann automatisch erfolgen oder auch manuell. Für den automatischen Wechsel sind zusätzliche Funktionalitäten im Gesamtsystem erforderlich z. B. die automatische Erkennung von Ausfällen. Dieser Fall wird im nächsten Abschnitt unter "Cluster" behandelt.

Um die Ausfallzeiten möglichst gering zu halten, muss der Zustand des Ersatzsystems kontinuierlich überprüft werden.

Vorteile einer Hot-Standby Lösung

- Die Ausfallzeiten sind im Vergleich zu Cold-Standby geringer.
- Wie beim Cold-Standby ist diese Lösung auch relativ kostengünstig, verglichen mit höherwertigen Hochverfügbarkeitslösungen, die im Folgenden beschrieben werden.
- Das Ersatzsystem ist in Betrieb und kann auch zu Datenreplikation benutzt werden.
- Neuaufsetzen oder Änderungen im System sind ohne Verfügbarkeitseinbuße möglich. Der Produktivbetrieb wird dafür während der Änderungen auf das Hot-Standby System umgelegt.

Nachteile einer Hot-Standby Lösung

- Es wird auch hier immer nur die Hälfte der vorhandenen Hardware genutzt.
- Das Ersatzsystem muss ständig auf dem aktuellen Stand gehalten werden.
- Im Falle der manuellen Aktivierung des Hot-Standby Systems ist eine kontinuierliche Überwachung von einem Systemverantwortlichen erforderlich.

Der Einsatz von Hot-Standby Systemen eignet sich für Anwendungen, bei denen kurze Ausfallzeiten unkritisch sind. Die Problematik der Systemüberwachung und der Aktivschaltung des Hot-Standby Servers muss dabei mitbedacht werden. Mögliche Einsatzbereiche sind z. B. für:

- Webserver mit oft variierendem Content
- Server in kleineren Netzen (Application-Server, Mailserver)
- Datenbank-Server und Fileserver (z. B. sekundärer Server repliziert primären Server ständig und wird im Fehlerfall als primärer Server geschaltet)

Cluster (automatisches Umschwenken)

Ein Cluster besteht aus einer Gruppe von zwei oder mehreren Rechnern, die zur Steigerung der Verfügbarkeit oder auch der Leistung einer Anwendung oder eines Dienstes parallel betrieben werden. Die Anwendung oder der Dienst kann dabei auf einem der Rechner aktiv durchgeführt werden oder auf mehreren verteilt (Performance-Steigerung).

Cluster werden je nach Funktionsart in

- Load balanced Cluster
- Failover Cluster und

unterschieden.

Load balanced Cluster

Beim Load balanced Cluster werden Instanzen einer Anwendung oder eines Dienstes in Abhängigkeit von der Auslastung unter den Servern verteilt. Wenn dies für eine Anwendung oder einen Dienst möglich ist, dann kann damit nicht nur eine Lastverteilung (Load balancing) und somit eine Performancesteigerung erreicht werden, sondern auch die Probleme bei Ausfällen werden verringert.

Eine der Voraussetzungen für den Einsatz von Load balancing ist, dass die jeweiligen Anwendungen oder Dienste keinen schreibenden Datenzugriff benötigen dürfen.

Eine Redundanz kann in diesem Fall geschaffen werden, indem Systeme mit ähnlicher Leistung mit Hilfe eines Load-Balancing Prozesses "nebeneinander" gestellt werden und dafür gesorgt wird, dass beim Ausfall eines Servers die anderen Server diesen Ausfall auffangen.

Vorteile eines Load balanced Clusters

- Es können damit sowohl Verfügbarkeitssteigerung als auch Leistungssteigerung erreicht werden.
- Alle verfügbare Ressourcen werden dauerhaft genutzt.
- Die Lösung ist hochgradig skalierbar.
- Die Komplexität des Gesamtsystems ist geringer als bei einem Failover Cluster.

Nachteile eines Load balanced Clusters

- Der Einsatz ist nicht für alle Arten von Anwendungen möglich. Insbesondere Anwendungen, die keine reinen Lesezugriffe verwenden und zugleich den Zugriff aller Server auf die gleichen Speicherressourcen verlangen, sind für Load Balancing nicht geeignet.

Wenn neben der Verfügbarkeit die Performance hohen Stellenwert hat und die Applikation einen verteilten Einsatz erlaubt, bietet ein Load balanced Cluster eine optimale Lösung. Das kann z. B. der Fall sein für:

- Web-Server
- Front-end Applikationen mit ausschließlichen Lesezugriffen (z. B. Web-Server-Farmen)

Failover Cluster

Als Failover Cluster wird hier ein Cluster bezeichnet, wenn bei Ausfall eines der Cluster-Systeme automatisch der aktive Betrieb der Anwendung oder des Dienstes von einem anderen Teil des Clusters übernommen wird (Takeover). Die automatische Übernahme von Diensten beim Ausfall einer Systemkomponente durch eine funktional äquivalente Komponente wird Failover genannt. Für die Failover-Funktionalität ist eine dedizierte "heartbeat" (Herzschlag) Verbindung üblich, die die Kommunikation zwischen den Cluster-Servern gewährleistet. Die Cluster-Server müssen neben der Verbindung mit dem Client-Netz auch mit dem Administrationsnetz dediziert verbunden sein, um einen direkten Zugang im Notfall zu gewähren.

Ein automatisches Failover setzt voraus, dass alle Software- und Hardware-Komponenten geeignet überwacht werden. Daher ist es wichtig sicherzustellen, dass der Failover Mechanismus auf keinen falschen Annahmen basiert.

Folgende Punkte müssen beim Einsatz eines Failover-Clusters berücksichtigt werden:

- Zugriff auf gemeinsamen Speicher:
  Neben den servereigenen Festplatten, die das Betriebssystem und die für den Betrieb notwendigen Daten enthalten, ist es in einem Cluster ratsam, die Anwendungsdaten auf gemeinsamen Speicher zu verwalten.
  Der Zugriff auf diese Festplatten wird dem Teil des Clusters gewährt, der gerade aktiv ist. Es ist auch möglich, statt gemeinsamer Festplatten replizierte Festplatten zu verwenden. Dies ist dann sinnvoll, wenn das Failover von einem entfernten Standort aus stattfindet. Bei einem lokalen Failover sollte überlegt werden, ob die durch die Replikation erzeugte Komplexität und entstandene Abhängigkeiten nicht eine zusätzliche Bedrohung für die Verfügbarkeit darstellen.
- Portabilität der Anwendung:
  Die Installation und Inbetriebnahme einer Anwendung auf zwei oder mehreren Servern parallel erfordert in den meisten Fällen den Einsatz zusätzlicher Lizenzen. Darüber hinaus muss überprüft werden, ob die Applikation eine Failover-Funktionalität erlaubt.
- NSPoF (No Single Points of Failure):
  Wenn die Failover-Funktionalität des Clusters durch den Ausfall einer einzigen Komponente gestört werden kann, widerspricht dies dem eigentlichen Zweck der Cluster-Architektur. Um Single Points of Failure zu vermeiden, muss das Gesamtsystem analysiert werden und der Ausfall einzelner Komponenten (Netzteile, Systemspeicher, Hauptspeicher, Netzwerkkarten, Switche, Hubs etc.) in Betracht gezogen werden.
- Betriebssystem und Konfiguration der Cluster-Server:
  Die Cluster-Server sollten mit gleichen Betriebssystemversionen, Patches, Libraries und Applikationsversionen ausgestattet sein. Eine möglichst identische Hardware- und Software-Konfiguration kann ein möglichst identisches Verhalten im Falle eines Failovers gewährleisten. Darüber hinaus reduziert sich im Falle von identischen Systemen die Komplexität des Gesamtsystems (Einsatz der gleichen Failover Software, Netz-Schnittstellen, Kompatibilität der gemeinsamen Speichersystems, Administration, Service).
- Dedizierte und redundante Verbindung zwischen den Servern:
  Die Kommunikation zwischen den Cluster-Servern muss unabhängig von der Netzlast, möglichst verzögerungsfrei erfolgen, damit das Failover schnellstmöglichst stattfinden kann. Die Redundanz ist aufgrund der hohen Verfügbarkeitsanforderungen ebenfalls erforderlich.
- Einsatz von ausgereiften Software-Produkten für das Failover Management:
  Die Entscheidung, ob ein Failover stattfinden muss oder nicht, ist eine sehr komplexe. Neue oder selbstentwickelte Tools können Fehler enthalten und dadurch letztendlich die Verfügbarkeit des Gesamtsystems reduzieren.
- Ausführliches Testen aller möglichen Failover-Aspekte:
  Ein ausführliches Testen ist unter anderem auch dazu notwendig, um festzustellen, dass keine unerwarteten Fehlerquellen (Single Points of Failure) vorhanden sind. Insbesondere muss das Monitoring der Server und das Failover-Management auf alle möglichen Fehler getestet werden.

Vorteile eines Failover Clusters

- Durch das automatische Takeover kann die Verfügbarkeit erheblich gesteigert werden.
- Es sind keine manuellen Eingriff nötig.

Nachteile eines Failover Clusters

- Diese Lösung ist hoch komplex.
- Failover Cluster sind nicht gut skalierbar.
- Es wird immer nur ein Teil der Ressourcen genutzt.
- Es entstehen hohe Kosten aufgrund zusätzlicher Hardware und Software

Wie aus der Gegenüberstellung der Vorteile und Nachteile hervorgeht, ist der Einsatz eines Failover Clusters nur dann sinnvoll, wenn eine oder mehrere Applikationen sehr hohe Verfügbarkeitsanforderungen haben. Neben dem hohen Kostenaufwand sind sehr gute Kenntnisse des verantwortlichen Personals sowohl über die eingesetzten Betriebssysteme und Applikationen als auch über die Failover-Funktionalität erforderlich. Der Einsatz von Failover Lösungen für Server macht zudem nur dann Sinn, wenn auch alle Abhängigkeiten wie beispielsweise Netzanbindung oder Verfügbarkeit der Clients auch mit den entsprechenden Redundanzen ausgelegt sind.

Bereiche, für die typischerweise bei hohen Verfügbarkeitsanforderungen Failover Cluster eingesetzt werden, sind z. B.:

- Datenbank Anwendungen
- File Storage
- Anwendungen mit dynamischem Inhalt
- Mail Server

Wenn Geschäftsprozesse, Anwendungen oder Dienste hohe Anforderungen an die Verfügbarkeit haben, sollte auf jeden Fall überlegt werden, wodurch diese Anforderungen abgedeckt werden können. Die IT-Verantwortlichen und das Sicherheitsmanagement sollten für die entsprechenden Server ein Konzept erarbeiten und angemessene Architekturen auswählen.

SYS.1.1.M29 Einrichtung einer Testumgebung (CIA)

Für Server mit hohen Sicherheitsanforderungen sollte eine Testumgebung eingerichtet werden, in der Konfigurationsänderungen, Updates und Patches vor dem Einspielen auf dem Produktionssystem vorab getestet werden können. Dies betrifft sowohl Sicherheitspatches und -updates als auch normale Updates, die vom Hersteller herausgegeben werden.

Die Testumgebung muss so beschaffen sein, dass sie eine "funktional äquivalente" Installation von Hard- und Software erlaubt. Dies bedeutet nicht notwendigerweise, dass zu einem teuren Serverrechner ein zweites, identisch konfiguriertes System beschafft werden muss. Zum Testen von Konfigurationsänderungen, Updates und Patches von Anwendungsprogrammen und Serversoftware genügt meist ein technisch deutlich sparsamer ausgestattetes System.

Es sollte jedoch auch die Möglichkeit bestehen, neue Gerätetreiber vor dem Einspielen zu testen. Daher kann es gegebenenfalls vorteilhaft sein, für verschiedene Arten von Tests unterschiedliche Testsysteme zu nutzen, etwa ein System für Tests systemnaher Programme oder von Betriebssystempatches und ein anderes für Tests im Zusammenhang mit der eigentlichen Serversoftware. In einem solchen Fall ist es jedoch wichtig sich bewusst zu sein, dass auf diese Weise gewisse Arten von Wechselwirkungen zwischen Betriebssystemumgebung und Serversoftware nicht abgedeckt werden können. Bei besonderen Anforderungen an die Sicherheit und Zuverlässigkeit eines Servers kann es deswegen erforderlich werden, tatsächlich ein zweites, identisch konfiguriertes System als Testumgebung zur Verfügung zu haben.

Für verschiedene typische und häufiger wiederkehrende Testfälle sollten Checklisten erstellt werden, die beim Testen abgearbeitet werden können und die neben der reinen Dokumentation des Tests oft auch zu einer Erhöhung der Effizienz und zur Vermeidung von Fehlern beitragen können.

Alle Tests sollten so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können.

SYS.1.1.M30 Ein Dienst pro Server (CIA)

Viele Schwachstellen in IT-Systemen sind einzeln nicht für einen potentiellen Angreifer ausnutzbar. Häufig wird erst durch die Kombination von Schwachstellen ein erfolgreiches Eindringen in einen Rechner möglich. Abhängig von der Bedrohungslage und dem Schutzbedarf der Dienste kann es deshalb zweckmäßig sein, auf einem Rechner nur einen Dienst zu betreiben. Dies betrifft vor allem Server, die Dienste auch ins Internet oder in andere Fremdnetze anbieten.

Beispielsweise kann das Sicherheitsniveau dadurch gesteigert werden, dass sowohl der Webserver als auch der E-Mailserver jeweils auf eigenständigen, dedizierten Rechnern, die als Minimalsystem ausgelegt sind, betrieben werden.

Außerdem sind einzelne Dienste auch unterschiedlich in ihrer Sicherheitseinstufung. So ist ein erfolgreiches Eindringen in einen Webserver nicht unproblematisch und kann zu Reputationsverlusten führen, insbesondere wenn ein Angreifer die extern verfügbaren Webseiten abändert. Zugriff auf vertrauliche Informationen ist dem Angreifer hierdurch aber meist nicht möglich. Ist der Webserver aber gleichzeitig der E-Mailserver, so kann ein Angreifer unter Umständen den gesamten E-Mail-Verkehr mitlesen, was möglicherweise viel schlimmere Auswirkungen hat.

Die Aufteilung kann sogar noch verstärkt werden, indem für einen einzelnen Dienst verschiedene Aufgaben auf unterschiedliche Rechner verteilt werden. So könnte es beispielsweise einen E-Mailserver A geben, der E-Mails aus dem Internet annimmt und in das interne Netz weiterleitet, und einen anderen E-Mailserver B, der E-Mails aus dem internen Netz an das Internet weiterleitet. Da die Kommunikationsaufnahme aus dem Internet nur mit dem E-Mailserver A möglich ist, kann ein Angreifer auch nur diesen direkt attackieren. Der E-Mailserver A darf selber keine E-Mails in das Internet verschicken, deshalb kann dieser Rechner auch nicht für E-Mail-Spamming missbraucht werden.

Eine Aufteilung verschiedener Dienste auf unterschiedliche Rechner hat unter anderem folgende Vorteile:

- Leichtere Konfiguration der einzelnen Rechner
- Einfachere und sicherere Konfiguration eines vorgeschalteten Paketfilters
- Erhöhte Widerstandsfähigkeit gegenüber Angriffen
- Erhöhte Ausfallsicherheit
- Leichtere Wartbarkeit der einzelnen Dienste

Durch ein geeignetes zentrales Systemmanagement kann der zusätzliche Administrationsaufwand, der durch die höhere Anzahl der Rechner entsteht, begrenzt werden.

Virtualisierung

Im Falle von sicherheitskritischen Diensten sollten auch in virtuellen IT -Systemen jeweils nur ein Dienst betrieben werden, wie dies auch für physische Systeme gilt. Ein virtuelles IT-System selbst ist jedoch in diesem Sinne kein "Dienst" eines Virtualisierungsservers. Daher können auf einem Virtualisierungsserver mehrere virtuelle IT-Systeme betrieben werden. Je nachdem, auf welcher Virtualisierungstechnik (Server- oder Betriebssystemvirtualisierung) der Virtualisierungsserver beruht, kann allerdings die Varianz der durch die virtuellen IT-Systeme bereitgestellten Dienste eingeschränkt sein. Ob das eingesetzte Virtualisierungsprodukt geeignet ist, unterschiedliche Dienste in virtuellen IT-Systemen auf einem Virtualisierungsserver bereitzustellen, muss für das konkrete Produkt geprüft werden. Als Kriterien sind hierfür die Stärke der Isolation und der Kapselung der virtuellen IT-Systeme auf dem Virtualisierungsserver heranzuziehen. Je stärker die virtuellen IT-Systeme auf dem Virtualisierungsserver isoliert sind, desto eher eignet sich das Virtualisierungsprodukt dazu, unterschiedliche Dienste in den verschiedenen virtuellen IT-Systemen zu betreiben. Die folgenden Grundsätze lassen sich für eine erste Beurteilung heranziehen:

- Auf Virtualisierungsservern mit einer Betriebssystemvirtualisierungslösung sollten in der Regel nur virtuelle IT-Systeme mit einer Funktion bereitgestellt werden. So sollten auf einem solchen Virtualisierungsserver beispielsweise ausschließlich Webserver oder ausschließlich Mailserver, aber keine Mischung aus diesen Gruppen betrieben werden. Bei einigen Produkten zur Betriebssystemvirtualisierung ist die Isolation der virtuellen IT-Systeme allerdings stark genug, so dass von dieser Vorgabe abgewichen werden kann.
- Auf Virtualisierungsservern mit einer Servervirtualisierungslösung ist es meist zulässig, virtuelle IT-Systeme mit unterschiedlichen Diensten zu betreiben. Es können also unter Umständen Webserver und Mailserver auf einem Virtualisierungsserver in jeweils getrennten virtuellen IT-Systemen gemeinsam bereitgestellt werden.

Auf einem Virtualisierungsserver selbst sollten allerdings neben der Virtualisierungssoftware und damit direkt verbundener Dienste (Verwaltungsdienst für die Virtualisierung etc.) keine weiteren Dienste betrieben werden.

SYS.1.1.M31 Application Whitelisting (CI)

Grundsätzlich müssen Serversysteme nur Anwendungen ausführen können, die dafür notwendig sind, dass die angebotenen Dienste funktionieren. Entsprechende Whitelist-Lösungen können sicherstellen, dass nur erlaubte Programme ausgeführt werden können. Es gibt hier betriebssystemeigene Mechanismen und Lösungen von Drittanbietern, die zur Umsetzung von Whitelisting infrage kommen.

Ein einfacher Ansatz ist pfadbasiertes Application Whitelisting für vollständige Pfade, bei dem z. B. Programmverzeichnisse oder Verzeichnisse mit Betriebssystemdateien erlaubt werden. So kann verhindert werden, dass etwa ein Schadprogramm aus dem Browser-Cache oder einem temporären Ordner heraus ausgeführt wird.

Alternativ kann explizit einzelnen Anwendungen die Ausführung gestattet werden. Dieser Ansatz erhöht die Sicherheit zusätzlich, da nur vorab festgelegte Anwendungen gestartet werden können. Gleichzeitig erhöht sich aber auch der Aufwand, da z. B. sichergestellt werden muss, dass alle nötigen Betriebssystemkomponenten ausgeführt werden können. Auch bei Updates ist zusätzlicher Aufwand nötig, um geänderte Programme in der Whitelist nachzupflegen.

Bei Whitelisting ist zu beachten, dass z.B. auch Skripte nicht ausgeführt werden dürfen.

SYS.1.1.M32 Zusätzlicher Schutz der privilegierten Anmeldeinformationen (CI)

Die Passwörter der administrativen Konten sollten in mehrere Teile geteilt und durch Anwendung des Vier-Augen-Prinzips zusätzlich geschützt werden. Auch administrative Konten sollten so eingerichtet werden, dass diese nach einer vorher festgelegten Anzahl fehlerhafter Anmeldeversuche gesperrt werden.

SYS.1.1.M33 Aktive Verwaltung der Wurzelzertifikate (CI)

Weitere Informationen zur Verwaltung von Wurzelzertifikaten befinden sich in den folgenden Dokumenten:

- Windows: Configure Trusted Roots and Disallowed Certificates [MSROOT]
- Mozilla: CA:Root Change Process [MOZRCP]
- Java: keytool - Key and Certificate Management Tool [KEYTOOL]
- OpenSSL: Certificate Installation with OpenSSL [OPENSSL]
- GnuPG: Agent Configuration - Using the GNU Privacy [GNUPG]

3 Weiterführende Informationen

3.1 Wissenswertes

Server Virtualisierung

Zur Effizienz-Steigerung in Rechenzentren wird häufig Server-Virtualisierung eingesetzt. Da aktuelle Server-Hardware so leistungsfähig ist, dass klassische Server-Installationen die Hardware-Ressourcen oftmals nicht auslasten, können mehrere virtuelle Server auf einem Physischen betrieben werden. Dies spart Platz und Energie.

Durch das Zusammenfassen mehrerer Server auf einer Hardware muss diese unter Umständen jedoch auch besser abgesichert werden, als ein einzelner Server. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat daher eine Empfehlung zum Thema veröffentlicht: CSE-113: Server-Virtualisierung. Sie richtet sich an Verantwortliche für die Planung und den Betrieb von IT-Infrastrukturen sowie an Betreiber von IT-Rechenzentren. Im Fokus stehen dabei produktunabhängige Empfehlungen zum sicheren Einsatz von Server-Virtualisierungsprodukten, die als Bare-metal-Hypervisoren eingesetzt werden. Bei derartigen Einsatzszenarien laufen neben dem Hypervisor, ein speziell für Virtualisierung optimiertes Betriebssystem, keine anderen Anwendungen auf der physischen Hardware.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Allgemeiner Server" finden sich unter anderem in folgenden Veröffentlichungen:

[BSITLS] Migration auf TLS 1.2 Handlungsleitfaden

Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 1.2, Juni 2016, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Migrationsleitfaden_Mindeststandard_BSI_TLS_1_2_Version_1_2.pdf, zuletzt abgerufen am 06.09.2018

[CSE113] Server-Virtualisierung

BSI-Veröffentlichungen zur Cyber-Sicherheit (BSI-CS 113), Version 1.0., März 2015, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_113.htm , zuletzt abgerufen am 05.09.2018

[GNUPG] Using the GNU Privacy Guard

Agent Configuration, https://www.gnupg.org/documentation/manuals/gnupg/Agent-Configuration.html , zuletzt abgerufen am 06.09.2018

[IEC62305] IEC 62305 Merkblatt

Die Blitzschutz-Normen DIN EN 62305 / VE 01805-305:2006, VDE (ABB), Oktober 2006, https://www.vde.com/resource/blob/936756/5b65d838e75e83f750bd8fa23bb620b1/merkblatt-blitzschutznormen-13-download-data.pdf , zuletzt abgerufen am 05.09.2018

[KEYTOOL] keytool - Key and Certificate Management Tool

Oracle, https://docs.oracle.com/javase/6/docs/technotes/tools/windows/keytool.html , zuletzt abgerufen am 06.09.2018

[MOZRCP] Mozilla CA: Certificate Change Process: Mozilla Wiki

https://wiki.mozilla.org/CA:Root_Change_Process, zuletzt abgerufen am 28.08.2018

[MSROOT] Configure Trusted Roots and Disallowed Certificates

Microsoft, https://technet.microsoft.com/en-us/library/dn265983(v=ws.11).aspx , zuletzt abgerufen am 06.09.2018

[NISTSP800123] Guide to General Server Security

NIST Special Publication 800-123, Juli 2008, https://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf , zuletzt abgerufen am 05.09.2018

[OPENSSL] Certificate Installation with OpenSSL - Other People´s Certificates

http://gagravarr.org/writing/openssl-certs/others.shtml , zuletzt abgerufen am 06.09.2018

[RFC5246] The Transport Layer Security (TLS) Protocol

RFC 5246, Internet Engineering Task Force (IETF), June 1969, https://tools.ietf.org/html/rfc5246 , zuletzt abgerufen am 06.09.2018

[RFC5746] Transport Layer Security (TLS) Renegotiation Indication Extension

RFC 5746, Internet Engineering Task Force (IETF), Februar 2010, https://tools.ietf.org/html/rfc5746 , zuletzt abgerufen am 06.09.2018

[TR21022] Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen

Teil 2: Verwendung von Trasport Layer Security (TLS), Bundesamt für Sicherheit in der Informationstechnik (BSI), Januar 2017, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html, zuletzt abgerufen am 24.08.2018

SYS.1.2: Windows Server

Umsetzungshinweise zum Baustein SYS.1.2.2 Windows Server 2012

1 Beschreibung

1.1 Einleitung

Mit Windows Server 2012 hat Microsoft im September 2012 ein Serverbetriebssystem auf den Markt gebracht, das in Bezug auf die Sicherheit diverse Verbesserungen gegenüber bisherigen Windows-Versionen (insbesondere auch Windows Server 2008 R2) mitbringt. Technisch wird dabei nicht auf dem Vorgänger aufgebaut, sondern auf der Codebasis des Client-Betriebssystems Windows 8. Mit dem Release Windows Server 2012 R2 von Oktober 2013 sind weitere Verbesserungen und Erweiterungen verfügbar, die Windows 2012 R2 zum Server-Pendant zu Windows 8.1 auf der Clientseite machen.

Dieser Baustein beschäftigt sich mit der Absicherung von Windows Server 2012 und Windows Server 2012 R2 gleichermaßen, auf relevante Unterschiede und Besonderheiten wird jeweils geeignet hingewiesen. Dabei wird die Schreibweise „Windows Server 2012 (R2)“ verwendet, wenn beide Versionen gemeint sind. Das Ablaufdatum für den Mainstream Support bzw. den Extended Support („End-of-Life“, EOL) ist in beiden Fällen der 09.01.2018 bzw. der 10.01.2023.

1.2 Lebenszyklus

Planung und Konzeption

Die hauptsächlich notwendigen Überlegungen finden sich in SYS.1.2.2.M1 Planung von Windows Server 2012 (R2). Auch SYS.1.2.2.M2 Sichere Installation von Windows Server 2012 (R2) und SYS.1.2.2.M3 Sichere Administration von Windows Server 2012 (R2) enthalten wesentliche Konzeptionsanteile.

Beschaffung

Bezüglich der Beschaffung sind die allgemeinen Grundlagen zu beachten, die für allgemeine Serversysteme gelten. Zusätzlich behandelt SYS.1.2.2.M1 Planung von Windows Server 2012 (R2) das Thema der Auswahl der geeigneten Edition.

Umsetzung

Die Hauptmaßnahmen für die Basisabsicherung des Betriebs sind in folgenden drei Maßnahmen beschrieben:

- SYS.1.2.2.M2 Sichere Installation von Windows Server 2012 (R2)
- SYS.1.2.2.M3 Sichere Administration von Windows Server 2012 (R2)
- SYS.1.2.2.M4 Sichere Konfiguration von Windows Server 2012 (R2)

Hinzu kommen die spezielleren, aber ebenfalls wichtigen Umsetzungen von:

- SYS.1.2.2.M5 Schutz vor Schadsoftware
- SYS.1.2.2.M6 Sichere Authentisierung und Autorisierung in Windows Server 2012 (R2)
- SYS.1.2.2.M8 Schutz der Systemintegrität
- SYS.1.2.2.M9 Lokale Kommunikationsfilterung (CI)

Bei erhöhtem Schutzbedarf werden exemplarisch die folgenden Maßnahmen eingesetzt:

- SYS.1.2.2.M10 Festplattenverschlüsselung bei Windows Server 2012 (R2)
- SYS.1.2.2.M12 Redundanz und Hochverfügbarkeit (A)
- SYS.1.2.2.M13 Starke Authentifizierung bei Windows Server 2012 (R2) (CI)

Betrieb

Auch im Betrieb bleiben SYS.1.2.2.M3 Sichere Administration von Windows Server 2012 (R2) und SYS.1.2.2.M4 Sichere Konfiguration von Windows Server 2012 (R2) relevant. Als weitere Standardanforderungen ist das erreichte Sicherheitslevel regelmäßig zu prüfen (SYS.1.2.2.M7 Sicherheitsprüfung von Windows Server 2012 (R2)).

Bei erhöhtem Schutzbedarf können zusätzlich im Betrieb beachtet werden:

- SYS.1.2.2.M11 Angriffserkennung bei Windows Server 2012 (R2) (CIA)
- SYS.1.2.2.M14 Herunterfahren verschlüsselter Server und virtueller Maschinen (CI)

Aussonderung & Notfallvorsorge

Bezüglich der Phasen der Aussonderung und der Notfallvorsorge bestehen keine Besonderheiten von Windows Server 2012 (R2) gegenüber einem allgemeinen Server.

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Windows Server 2012" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

SYS.1.2.2.M1 Planung von Windows Server 2012

Da Windows Server 2012 (R2) ein komplexes Betriebssystem mit einer Vielzahl von Funktionen und Konfigurationsoptionen darstellt, muss der Einsatz sorgfältig und systematisch geplant werden. Eine Dokumentation der Entscheidungen samt kurzer Begründung sollte dabei angelegt werden, etwa in Form eines Betriebskonzepts oder eines Serverhandbuchs.

Editionen

Windows Server 2012 ist in vier Editionen verfügbar, die für unterschiedliche Einsatzgebiete vorgesehen und optimiert sind:

- Foundation
  - Grundlegende Server-Funktionen
  - keine Virtualisierung
- Essentials
  - einfache Benutzeroberfläche
  - voreingestellte Konnektivität zu Cloud-Diensten
  - keine Virtualisierung
- Standard
  - Voller Funktionsumfang
  - max. zwei virtuelle Instanzen
- Datacenter
  - wie Standard
  - mit unbegrenzten virtuellen Instanzen

Weitere Beschränkungen existieren bei Foundation bzw. Essentials bezüglich Speicher (max. 32/64 GB RAM) und Lizenzierung (max. 15/25 Benutzerkonten) sowie in den installierbaren Rollen und Funktionalitäten. Über weitere Details der Unterschiede bzgl. Beschränkungen, Rollen und Funktionen informiert Microsoft auf seiner Website. Der Server-Core-Modus etwa ist erst ab Edition Standard verfügbar, die Nutzung von WSUS erst ab Essentials. Zumindest Foundation ist daher nur in sehr begrenzten Szenarien für den professionellen Einsatz im Unternehmen oder in der Behörde zu empfehlen und wird in diesem Baustein nicht näher betrachtet.

Die Editionen Standard und Datacenter sind aus Sicherheitssicht gleichwertig und unterscheiden sich im Wesentlichen in Hinsicht auf das Lizenzmodell. Es bleibt also die Frage nach der Entscheidung zwischen Essentials und Standard bzw. Datacenter.

Eigenschaften der Essentials-Edition

Foundation und Essentials in Windows 2012 sind nicht dafür gedacht, innerhalb einer vollwertigen Domäne betrieben zu werden. Zwar ist dies für Essentials mit Windows Server 2012 R2 mittlerweile technisch möglich, jedoch richtet sich diese mit ihren Funktionen hauptsächlich an kleinere Institutionen, die nur einen einzigen Server zum Betrieb sämtlicher Funktionen einsetzen. Dies steht im Widerspruch zur etablierten Praxis in größeren IT-Umgebungen, möglichst wenige Dienste pro Server zu betreiben, um Abhängigkeiten aufzulösen und Risiken zu streuen, ein Trend, der durch zunehmende Virtualisierung weitere Verbreitung findet.

Die Essentials-Edition bietet ohne weitere Konfiguration eine Reihe von Funktionen, welche die Einrichtung erleichtern können:

- Hinzufügen zur Domäne
  Mit Essentials ist es einfach möglich, Rechner zur Domäne hinzuzufügen, die sich an einem entfernten Standort befinden. Es genügt, dass ein neuer Mitarbeiter auf den Pfad "/connect" der Essentials-Fernzugriffswebsite zugreifen kann.
- Vorkonfiguriertes VPN
  Es ist ein vorkonfigurierter VPN-Client verfügbar. Der Benutzer kann zudem die Autoeinwahl aktivieren, sodass er immer mit dem Firmen- bzw. Behördennetz verbunden ist.
- Server-SpeicherFür Speicherorte wie etwa die Heimatverzeichnisse der Benutzer können einfach Shared Folder auf einem weiteren Server im selben Netz angelegt werden. Dabei kann eine automatische Alarmierung erfolgen, wenn die Verzeichnisse eine bestimmte Größe überschreiten.
- Health Report
  Ein grundlegender "Gesundheitscheck" der Windows Server 2012 R2 Essentials-Umgebung ist bereits integriert und muss nicht erst als Add-in installiert werden. Es lassen sich verschiedene Werte konfigurieren, die über unterschiedliche Medien angezeigt werden, etwa auch auf dem Smartphone.
- BranchCache
  Bereits in Essentials kann der Mechanismus BranchCache aktiviert werden, der die Verfügbarkeit von Daten in Außenstellen durch Caching (Zwischenspeicherung) erhöht. Er verringert darüber hinaus gleichzeitig die Bandbreitennutzung über das WAN.
- Remote Web Access
  Viele Funktionen von Windows Server 2012 Essentials lassen sich aus der Ferne über eine Weboberfläche erreichen und bedienen (Remote Web Access), die in R2 zudem modernisiert und für die Nutzung mit Tablets und ähnlichen Geräten optimiert wurde.

Microsoft Azure Online Backup

In Windows Server 2012 ist Microsofts Cloud-Speicherlösung Azure Online Backup bereits in Essentials integriert und kann leicht aktiviert werden. Dafür muss lediglich im Essentials Dashboard das entsprechende Add-in installiert werden und ein (je nach Speichervolumen kostenpflichtiger) Account angelegt werden. In R2 ist nicht mal mehr ein Add-in notwendig, hier kann direkt per Klick die Registrierung bei Azure erfolgen.

Während dies eine sehr einfache Möglichkeit darstellt, regelmäßige Backups der auf dem Server gespeicherten Daten zu erzeugen, sollte diese Funktion keinesfalls leichtfertig aktiviert werden, sondern allenfalls nach einer umfassenden Beschäftigung mit den Themen der Bausteine OPS.2.2 Cloud-Nutzung und OPS.1.16 Datensicherung und einer erfolgten Abwägung zwischen Vertraulichkeit, Verfügbarkeit und verschiedenen Anbietern.

Blockieren von Microsoft-Konten

Der folgende Abschnitt ist nicht anzuwenden, wenn im Rahmen der Beschäftigung mit dem Baustein OPS.2.2 Cloud-Nutzung eine begründete und dokumentierte Entscheidung für die Nutzung von Microsoft Azure in Zusammenhang mit dem Windows Server 2012 (R2)-Serversystem getroffen wurde.

Andernfalls darf während der Einrichtung des Systems kein Microsoft-Konto angelegt werden. Die Erstellung von Microsoft-Konten auf dem Server muss zudem blockiert werden. Am verlässlichsten geschieht dies zentral über das Active Directory und die folgende Sicherheitsrichtlinie:

"Windows Settings/Security Settings/Local Policies/Security Options/Accounts: Block Microsoft Accounts"

SYS.1.2.2.M2 Sichere Installation von Windows Server 2012

Grundlegende Funktionen von Windows Server 2012 (R2) werden durch Serverrollen, Rollendienste und Features gesteuert.

Serverrollen

Eine Serverrolle ist eine Gruppe von Programmen, mittels derer eine bestimmte Funktion für mehrere Benutzer oder für andere IT-Systeme in einem Netz ausgeführt werden kann. Mit ihr wird häufig die Hauptfunktion eines Servers beschrieben. Ein Server könnte jedoch auch mehrere Rollen ausführen, wenn diese nur selten verwendet werden. Sind Rollen korrekt installiert und konfiguriert, werden sie automatisch ausgeführt.

Rollendienste

Rollendienste sind Programme, die die Funktionalität einer Rolle bereitstellen. Eine Rolle kann als Satz zusammenhängender, sich ergänzender Rollendienste betrachtet werden, wobei in der Regel die Installation einer Rolle die Einrichtung mindestens eines zugehörigen Rollendienstes bedingt.

Je Rolle kann festgelegt werden, welche Rollendienste für andere Benutzer und IT-Systeme mit der Rolle bereitgestellt werden. Einige Rollen (z. B. DNS-Server) haben nur eine Funktion, daher stehen für sie keine Rollendienste zur Verfügung. Andere Rollen (z. B. Remotedesktopdienste) verfügen über mehrere Rollendienste, die je nach Anforderungen installiert werden können.

Features

Features sind Programme, die die Funktionalität des Servers oder aber einer oder mehrerer Rollen unterstützen oder verbessern. Z. B. wird mit dem Feature Failover-Clusterunterstützung die Funktionalität weiterer Rollen (u. a. Dateidienste und DHCP-Server) verbessert, da Servercluster für eine höhere Redundanz und bessere Leistung zusammengeführt werden können. Das Feature Telnet-Client hingegen ermöglicht die Fernkommunikation über das Telnet-Protokoll.

Rollen, Rollendienste und Features müssen immer so sparsam wie möglich installiert werden, um die Komplexität und Angriffsoberfläche klein zu halten. Die Regel "ein Dienst pro Server" gilt auch hier sinngemäß, es sollte in der Regel nur eine für die Institution wesentliche Serverrolle pro Server installiert sein. Die Auswahl der zu installierenden Rollen, Rollendienste und Features sollte begründet und dokumentiert werden.

Server Core

Server Core ist eine minimale Installationsoption für Windows Server (inkl. 2012 und 2012 R2), die eine Serverumgebung mit beschränkter Funktionalität und geringerem Wartungsbedarf bereitstellt.

Seit Windows Server 2012 ist ein Wechsel zwischen Full Server und Server Core ohne Neuinstallation möglich.

Hauptunterschiede sind das Fehlen der vollständigen Windows-Shell und eine extrem begrenzte grafische Oberfläche (GUI), die sich auf ein Kommandoprompt mit PowerShell-Unterstützung beschränkt.

Verwalten lässt sich Server Core folgendermaßen:

- per PowerShell (lokal und remote)
- über eine Terminal-Server-Verbindung von einer Kommandozeile
- aus der Ferne über die Microsoft Management Console (MMC)
- aus der Ferne mit anderen Kommandozeilentools, die Fernverwaltung unterstützen

Da Server Core bezüglich der Angriffsfläche das Minimum und damit Optimum darstellt, sollte, wo immer möglich, die Server Core-Variante genutzt werden. Abweichungen sollten begründet sein. Dies fördert zudem die Zentralisierung der Verwaltung.

SYS.1.2.2.M3 Sichere Administration von Windows Server 2012

Sichere Passworte für lokale Administrationskonten

Es ist sicherzustellen, dass das Passwort für jedes lokale Administratorkonto nicht nur sicher ist, sondern zudem einzigartig. So wird es einem Angreifer erschwert, sich von einem kompromittierten IT-System zum nächsten lateral weiterzubewegen.

Mit dem bei Microsoft kostenlos verfügbaren Tool LAPS (Local Administrator Password Solution) ist es möglich, sichere lokale Administratorkonten automatisch per AD zu verwalten. Dessen Einsatz ist stark zu empfehlen, wenn nicht bereits eine Drittlösung hierfür bereitsteht.

Schulung von Administratoren

Um Windows Server 2012 (R2) sicher einrichten und betreiben zu können, müssen die zuständigen Administratoren über eine Reihe von Fähigkeiten und Kenntnissen verfügen, die teilweise sehr spezifisch für dieses Betriebssystem sind. Zum Allgemeinwissen des Administrators gehören etwa Grundregeln des Arbeitens auf Serversystemen wie

- nicht von Servern aus im WWW zu surfen,
- insbesondere keine möglicherweise unsicheren Seiten anzusteuern,
- Clientsysteme für den Download von Dateien wie etwa Treibern zu verwenden und
- für sämtliche nichtadministrativen Tätigkeiten einen Standardaccount zu verwenden.

Im Folgenden werden Spezifika von Windows Server 2012 (R2) vorgestellt, mit denen sich die Administratoren auskennen sollten. Notwendige Schulungen sollten vor Installation der Serversysteme durchgeführt werden.

Administrationsthemen

Die folgende Tabelle enthält eine Liste von Administrationsthemen mit Security-Relevanz. Administratoren von Windows Server 2012 (R2) sollten sich mit den genannten Themen und ihren Besonderheiten sowie jeweils geeigneten Tools bei Windows Server 2012 (R2) auskennen.

Thema	Aufgaben des Administrators
Zugriff	Verwalten des Zugriffs auf Netzressourcen
Auditing	Verwalten des Zugriffs auf Netzressourcen
Zertifikatsdienste	Verwalten einer Zertifizierungsstelle (CA) und andere Active Directory-Zertifikatsdienste-Aufgaben
Computer	Analysieren und Verwalten von Computerprozessen und Leistung
Anmeldeinformationen	Verwalten von Benutzerkonten, Gruppen und Anmeldeinformationen
Kryptografie	Verwalten von Zertifikaten und Verschlüsselung
Dateien	Übernehmen oder dauerhaftes Löschen von Dateien
Sicherheitsrichtlinien	Analysieren und Verwalten von Sicherheitsrichtlinien
Sicherheitsprinzipale	Ändern oder Erstellen neuer Sicherheitsprinzipale
Systemsicherheit	Diagnostizieren, Planen und Berichtigen der globalen Systemsicherheit

Darüber hinaus bietet Microsoft als Teil der Windows PowerShell Core Modules Sammlungen von PowerShell-Commandlets für Security-Aufgaben an. Administratoren sollten diese kennen, um sie für eine einfache und schlanke Sicherheitsverwaltung nutzen zu können:

- Windows PowerShell Security Cmdlets
- PowerShell Cmdlets for Active Directory
- PowerShell Cmdlets for Active Directory Rights Management Services
- PowerShell Cmdlets for AppLocker
- PowerShell Cmdlets for Group Policy
- PowerShell Cmdlets for Server Manager
- PowerShell Cmdlets for the Best Practice Analyzer

Benutzerkontensteuerung (UAC)

Die Benutzerkontensteuerung (User Account Control, UAC) wurde in Windows Vista eingeführt. Sie sorgt dafür, dass bei administrativen Aufgaben eine Rechteerhöhung erforderlich ist. Bis dahin hatten die meisten Anwender als Administratoren gearbeitet, mit entsprechender Anfälligkeit für Schadsoftware.

Wenn sich bei aktivierter UAC ein Administrator anmeldet, arbeitet er mit eingeschränkten Rechten. Erst nach Bestätigung in einem speziellen Dialogfeld erhält eine Anwendung administrative Berechtigungen. Im Hintergrund werden dafür Rechte erhöht, indem die Identität gewechselt wird. Die UAC ist damit die Grundlage für das Sandboxing von Programmen und Verzeichnissen unter Windows. Sie regelt die Vergabe von Privilegien an Prozesse und sie isoliert Prozesse und Fenster voneinander, die auf demselben Desktop mit unterschiedlichen Rechten laufen.

Mit Windows Server 2012 und Windows 7 wurde die UAC verfeinert, um die Verwaltung der Konfiguration und der Nachrichten zu erleichtern.

Die UAC stellt einen Kompromiss zwischen Sicherheit und Bequemlichkeit dar. Sie bietet kein vollständiges Sandboxing und kann auf verschiedene Arten umgangen werden, erhöht jedoch den Aufwand für Schadsoftware und ähnliche Bedrohungen bzw. kann helfen, deren Effekte einzugrenzen.

Eine noch stärkere Absicherung würde durch das Arbeiten mit komplett getrennten Konten samt wirklichem Kontowechsel für administrative Aufgaben erreicht. Dies wird bei hohem oder sehr hohem Schutzbedarf empfohlen. Die zweitsicherste Lösung ist die Nutzung getrennter Konten mit Rechteerhöhung für Standardnutzer durch Over-the-Shoulder-Abfrage (OTS). Zumindest sollte Arbeiten im Administratorbestätigungsmodus (Admin Approval Mode, AAM) aktiviert sein. Die Abschaltung der Benutzerkontensteuerung ist mit Windows Server 2012 gar nicht mehr möglich, aber auch eine automatische Rechteerhöhung ohne Nachfrage ist nicht zu empfehlen.

Allerdings ergibt sich bei vollständiger Trennung der Accounts das Problem, dass wenn sich Administratoren zunächst als Standardnutzer auf Servern anmelden können sollen, auch die Anmeldung aller Domänennutzer auf dem Server möglich ist. Dies ist nicht gewünscht, da sich so die Angriffsfläche deutlich erhöht. Entweder muss dies mit aufwändiger Konfiguration verhindert werden oder es kann auf die Alternative getrennter Admin-Systeme, sogenannte Privileged Access Workstations (PAWs), zurückgegriffen werden. Diese besonders geschützten dedizierten Systeme kommen in der Regel allerdings erst bei höherem Schutzbedarf infrage.

Achtung: Das vordefinierte Konto "Administrator" wird durch UAC niemals eingeschränkt. Unter Client-Betriebssystemen ab Vista hat dies normalerweise keine Auswirkungen, da dieses Konto nicht zum Login verwendet werden kann; hierfür werden stattdessen weitere Konten der Gruppe "Administratoren" angelegt. Windows Server (ab 2008) hingegen erzeugt bei der Installation keine zusätzlichen Konten und erlaubt die Anmeldung als "Administrator", ohne UAC. Das Konto "Administrator" sollte daher möglichst nicht zur regelmäßigen Systemverwaltung genutzt werden. Andere lokale oder Domänen-Konten, die "Administratoren"-Mitglieder sind, werden über UAC eingeschränkt.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Windows Server 2012".

SYS.1.2.2.M4 Sichere Konfiguration von Windows Server 2012

Im Folgenden werden diejenigen wichtigen Sicherheitsmechanismen, d. h. Techniken, die der Sicherheit dienen oder eine wesentliche Auswirkung auf diese haben,in Windows Server 2012 (R2) kurz vorgestellt, bei denen der Sicherheitsverantwortliche oder Administrator eine Wahl zu treffen hat. Nicht aufgeführt sind solche Mechanismen, bei denen sich nichts im Vergleich auf die Vorgängerversionen verändert hat oder keine Gestaltungsfreiheit in der Anwendung besteht.

Windows Server 2012 (R2) bringt eine Reihe von Ressourcen und Tools bereits mit, die für eine Absicherung verwendet werden können und sollten. Diese sollten sich mit Sicherheitsfunktionen anderer IT-Systeme und Drittherstellerprodukte sinnvoll ergänzen, idealerweise im Sinn einer gestaffelten Verteidigung (Defense-in-Depth) überdecken und niemals gegenseitig aushebeln oder schwächen.

Nicht mehrere wesentliche Funktionen pro **Server**

Mit der Forderung, dass nicht mehrere wesentliche Funktionen durch einen Server erfüllt werden sollen, wird eine grundlegende Aufteilung kritischer Serverfunktionalität auf verschiedenen Systeme angestrebt. Das im Unix-Bereich verbreitete "ein Dienst pro Server" passt hier nicht, da Dienst im engeren Sinn eher einen einzelnen Netzdienst beschreibt (z. B. Telnet). Hier geht es eher darum, funktional unabhängige Einheiten auch technisch voneinander unabhängig zu machen. Ein Webserver sollte beispielsweise nicht gleichzeitig als Terminalserver dienen, ein Fileserver nicht gleichzeitig als WSUS-Server. Bei Mehrschichtanwendungen wird in der Regel angestrebt, die einzelnen Schichten (etwa Datenbank / Geschäftslogik / Präsentation) in getrennte Server(-Cluster) abzubilden. Dies hat den Vorteil, dass das Netzes einfacher segmentiert werden und so besser dem Schutzbedarf und der Art der Bedrohungen angepasst sein kann. Außerdem ergeben sich Vorteile in der Wartung und Verwaltung.

S**ecurity Baseline** und SCM

Viele sicherheitsrelevante Einstellungen von Windows Server 2012 (R2) lassen sich am einfachsten über GPOs verwalten. Es empfiehlt sich, für alle Serversysteme oder für Serversysteme einer bestimmten Einsatzklasse eine sogenannte Baseline zu erstellen, also eine Vorlage, die optimale Sicherheitseinstellungen enthält, regelmäßig überprüft und fortgeschrieben wird und auf alle betriebenen Serversysteme ausgerollt wird.

Der Security Compliance Manager (SCM) ist ein kostenloses Tool von Microsoft, mit dem schnell GPOs erzeugt und verwaltet werden können und zudem Sicherheitsvorlagen für verschiedene Zwecke bereits mitbringt. Diese können dann mit verschiedenen Verfahren, wie z. B. Group Policy-Editor oder System Center Configuration Manager (SCCM) bzw. DCM (Desired Configuration Management, inzwischen umbenannt in Configuration Manager Compliance Settings), zentral ausgerollt werden. Auch eine Konfiguration von Stand-alone-Maschinen ist über das GPO Pack-Feature möglich, jedoch nur für die Ausnahme von Nicht-Domänenmitgliedern zu empfehlen.

Die konsequente Nutzung von SCM oder anderer Sicherheitsvorlagen und das zentrale Deployment von GPOs und/oder DCMs verbessern die Gleichförmigkeit und Nachvollziehbarkeit und helfen damit, Konfigurationsdrift zu verhindern und die Compliance zu erhöhen. Neben Betriebssystemeinstellungen können so auch viele Anwendungen verwaltet werden.

Insbesondere die im SCM verfügbaren Sicherheitsvorlagen enthalten für sehr viele Parameter bereits sicherere Einstellungen als die Grundeinstellung in Windows Server 2012 (R2). Häufig müssen diese allerdings noch auf den jeweiligen Einsatzzweck und die Gegebenheiten der Institution angepasst werden.

Falls die Institution nicht bereits über eine grundschutzkonforme Sicherheitsvorlage verfügt, sollte im SCM die Security Baseline für Windows Server 2012 bzw. R2 ausgewählt werden. Die gepackte .cab-Datei enthält die folgenden Komponenten:

- Windows Server 2012
  - AD Certificate Services Server Security
  - DHCP Server Security
  - DNS Server Security
  - Domain Controller Security Compliance
  - Domain Security Compliance
  - File Server Security
  - Hyper-V Security
  - Member Server Security Compliance
  - Network Policy and Access Services Security
  - Print Server Security
  - Remote Access Services Security
  - Remote Desktop Services Security
  - Web Server Security
- Windows Server 2012 R2
  - Domain Controller Security Compliance
  - Domain Security Compliance
  - Member Server Security Compliance
- Folgende Attachments liegen bei beiden jeweils bei:
  - Security Guide.docx: dieser enthält die Beschreibung der gewählten Einstellungen
  - CCE Reference.xlsm

Die Anpassung sollte auf der Grundlage der GPOs für die avisierte Rolle des Servers 2012 (R2) stattfinden. Alle Einstellungen sollten vor dem Ausrollen auf produktive Systeme gründlich getestet werden, da sonst leicht Fehlfunktionen auftreten können.

Es sollte nach jeder großen Änderung überprüft werden, ob die Einstellung erfolgreich geändert wurde und ob die Vorlage überhaupt auf die gewünschten Server angewandt wird, da hier viele Fehlerquellen lauern. Ein einfacher Weg dies zu tun ist die Ausführung des Group Policy Results Kommandozeilentools GPResult.exe auf dem Server.

Für weitere Informationen siehe auch Baustein APP.2.2 Active Directory.

Absicherung des Internet Explorers

Der Browser auf dem Server, im Fall von Windows Server zunächst der IE, stellt ein mögliches Einfallstor für Angriffe aus dem Internet dar. Er sollte daher besonders abgesichert werden, selbst wenn das wilde Surfen per Richtlinie organisatorisch verboten ist.

Enhanced Security Configuration

Bei Installation von Windows Server 2012 wird IE automatisch mit aktivierter Enhanced Security Configuration (ESC) installiert. Diese Konfiguration weist den in IE 10 definierten Zonen (Internet, Intranet, Trusted, Restricted) jeweils spezifische (höhere) Sicherheitslevel zu, z. B. "hoch" im Fall von Internet und Restricted Zone. Darüber hinaus enthält die Konfiguration eine Reihe von anderen Einstellungen, etwa zum Löschen der temporären Internetdateien beim Schließen des Browsers.

Dieser Modus hilft, die Angriffsfläche im Browser zu verringern und sollte daher beibehalten werden.

Enhanced **Protected Mode**

Enhanced Protected Mode (EPM), ebenfalls ab IE 10 verfügbar, ist eine Erweiterung des mit IE 7 auf Windows Vista eingeführten Protected Mode. Zu dessen Maßnahmen gegen die Installation von Software und Manipulation des Systems durch den Browser kamen weitere Beschränkungen im Bezug auf die Informationsabfluss aus dem Intranet hinzu

EPM lässt sich entweder in der Group Policy Management Console (GPMC) unter "Windows Components\Internet Explorer\Internet Control Panel\Advanced Page" oder in der Registry (computerweit) unter "HKLM\Software\Policies\Microsoft\Internet Explorer\Main!Isolation" konfigurieren.

SYS.1.2.2.M5 Schutz vor Schadsoftware

Bevor ein IT-System mit möglicherweise unsicheren Netzen verbunden wird sowie bevor Wechselmedien an dem IT-System angeschlossen werden, sollte auf jedem System mit Windows Server 2012 (R2) ein Virenschutzprogramm installiert werden, wenn nicht anderweitige Vorkehrungen gegen Schadprogramme getroffen werden. Dies zu planen und zu konfigurieren ist Gegenstand des Bausteins OPS.1.15 Schutz vor Schadprogrammen.

Bei Verwendung eines Virenschutzprogramms auf dem Server sollten die Signaturen mindestens täglich aktualisiert werden, zudem sollten regelmäßig alle Festplatten inklusive der Betriebssystempartition vollständig gescannt werden. Geeignete Alarme für die zuständigen Administratoren sollten bei allen Arten von Ereignissen in Bezug auf Schadsoftware konfiguriert sein.

Unabhängig vom gewählten Antivirusprodukt kann zunächst das in Windows Server 2012 (R2) integrierte Microsoft-Produkt Windows Defender verwendet werden, bis die finale Lösung zum Schutz vor Schadprogrammen aktiviert werden kann.

Windows Defender

Windows Defender war vor Windows Server 2012 eine reine Anti-Spyware-Lösung und stellt seitdem einen vollwertigen Virenschutz dar, ist allerdings für den Consumer-Bereich optimiert. Seit R2 ist Windows Defender auf Server Core standardmäßig aktiviert.

Windows Defender sollte aktiviert bleiben, bis eine alternative vollwertige Virenschutzlösung installiert wurde. Mehrere Antivirenprogramme (einschließlich Windows Defender) parallel dürfen nur betrieben werden, wenn die Empfehlungen beider Hersteller dies ausdrücklich erlauben, in der Regel ist dies nicht der Fall. Zudem erhöht jeder Virenscanner durch potentielle eigene Schwachstellen auch die Angriffsfläche des Servers.

SYS.1.2.2.M6 Sichere Authentisierung und Autorisierung in Windows Server 2012

Authentisierung und Autorisierung spielen als zwei grundlegende Sicherheitstechniken an verschiedenen Stellen in Windows Server 2012 (R2) wichtige Rollen. Folgende Prinzipien können dabei als allgemeine Leitlinien der Realisierung dienen:

- Beschränkung und Schutz privilegierter Domänenaccounts
  - Getrennte Accounts für Administration und andere Nutzung für Administratoren
  - Spezielle abgesicherte Admin-Workstations
  - Einschränkung der Konten, die sich interaktiv einloggen können
  - Beschränkung von Account Delegation-Rechten für administrative Accounts
- Beschränkung und Schutz lokaler Adminaccounts
  - Lokale Account-Beschränkungen für Remote-Zugriff
  - Kein Netz-Login für lokale Accounts
  - Individuelle Passwörter für lokale Admin-Accounts

Geschützte Benutzer

Mit R2 kam die domänenbezogene globale Sicherheitsgruppe "Geschützte Benutzer" (Protected Users) hinzu. Die Anmeldeinformationen der Mitglieder dieser Gruppe werden durch standardmäßig restriktivere Sicherheitseinstellungen zusätzlich geschützt.

Der nicht weiter konfigurierbare Schutz gilt für alle Geräten, auf denen Windows Server 2012 R2 und Windows 8.1 ausgeführt wird sowie auf Domänencontrollern in Domänen mit einem primären Windows Server 2012 R2 Domänencontroller.

Der Speicherfußabdruck von Anmeldeinformationen wird durch mehrere Einschränkungen signifikant reduziert:

- NTLM, Digestauthentifizierung oder CredSSP sind deaktiviert.
- Kerberos nutzt in der Vor-Authentifizierung nicht die schwächere DES- oder RC4-Verschlüsselung.
- Das Konto kann nicht mit der eingeschränkten und uneingeschränkten Kerberos-Delegierung delegiert werden. Das bedeutet, dass frühere Verbindungen mit anderen Systemen fehlschlagen, wenn der Benutzer Mitglied der Gruppe "Geschützte Benutzer" ist.
- Eine Ticket-Granting-Ticket-Lebensdauer von vier Stunden kann via Active Directory-Verwaltungscenter (ADAC) über Authentifizierungsrichtlinien und Silos konfiguriert werden, sodass sich der Benutzer alle vier Stunden erneut authentifizieren muss.

Alle menschlichen Benutzer sollten möglichst Mitglieder der Gruppe "Geschützte Benutzer" sein.

Achtung: Konten für Dienste und Computer sollten nicht Mitglieder von "Geschützte Benutzer" sein, da die Gruppe keinen lokalen Schutz bietet: Kennwort oder Zertifikat sind immer auf dem System verfügbar.

Gruppe "Managed Service Accounts"

Managed Service Accounts (MSA) sind eines der besonderen Features, die mit Windows Server 2008 R2 und Windows 7 hinzugekommen sind. Es handelt sich hierbei um Konten für Dienste (z. B. SQL Server oder Exchange) im Active Directory, die an einen bestimmten Rechner gebunden sind. Das Konto verfügt über sein eigenes komplexes Passwort und wird automatisch verwaltet. So kann ein MSA einfach und sicher Dienste auf einem bestimmten System ausführen, während die Möglichkeit, als ein bestimmter Benutzer-Principal auf Ressourcen im Netz zuzugreifen, gewahrt bleibt. Die Gruppe "Managed Service Account", die mit Windows Server 2012 geschaffen wurde, bietet dieselbe Funktionalität in der Domäne, jedoch zusätzlich mit der Möglichkeit, diese über mehrere Server zu erstrecken.

Wo immer möglich sollten für Dienstkonten MSA eingesetzt werden, sowie im Sinn einer einheitlichen Konfiguration und Beschränkung der Komplexität möglichst auch die Gruppe "Managed Service Account".

LSA-Schutz in Windows Server 2012 R2

Die Local Security Authority (LSA), die den Local Security Authority Server Service (LSASS)-Prozess umfasst, authentisiert Benutzer bei lokalen und Netzanmeldungen und setzt die lokalen Sicherheitspolicies durch. Windows 8.1 und Windows Server 2012 R2 bieten zusätzliche Schutzmechanismen dafür, die ein Auslesen von Speicher sowie eine Injektion von Code erschweren. Dies erhöht den Schutz für Credentials, die in der LSA gespeichert und verwaltet werden, etwa gegenüber Pass-the-Hash-Angriffen. Auch Smartcard-Daten inklusive PINs sind dort abgelegt.

Dazu ist in der Registry unter "HKEY_LOCAL MACHINE > SYSTEM > CurrentControlSet > Control > Lsa" ein DWORD (32-bit) des Namens "RunAsPPL" mit Inhalt "1" einzutragen und der Server neu zu starten. Alternativ geht dies auch über eine GPO (Computer Configuration > Windows Settings > Hive > **HKEY_LOCAL_MACHINE** > **SYSTEM\CurrentControlSet\Control\Lsa**).

Um die erfolgreiche Einrichtung zu überprüfen, sollte im Event Viewer unter Windows Logs > System nach folgendem WinInit-Event Ausschau gehalten werden: "LSASS.exe was started as a protected process with level: 4".

In Kombination mit Secure Boot ist der Schutz besonders sicher, da er in dem Fall in UEFI generell aktiviert ist, unabhängig vom Inhalt der Registry.

Dynamische Zugriffsregeln

In Windows Server 2012 wurde die Möglichkeit geschaffen, für die Autorisierung dynamische Zugriffsregeln für Dateien und Ordner zu definieren. Da diese einen wesentlich schlankeren und dadurch leichter zu pflegenden Regelsatz erlauben können, sollte ihr Einsatz geprüft und bevorzugt werden, wenn nicht andere, betriebliche Gründe dagegen sprechen.

SYS.1.2.2.M7 Sicherheitsprüfung von Windows Server 2012

Auch bei Windows Server 2012 (R2) sollte die tatsächlich effektiv vorhandene Sicherheit regelmäßig auditiert werden, da nur so eine vollständige Umsetzung der Maßnahmen verlässlich geprüft werden kann.

Tools zur Überprüfung der Sicherheitskonfiguration (Assessment Tools)

Neben den Standardmitteln technisches Konfigurationsaudit und Penetrationstest (siehe Baustein SYS.1.1 Allgemeiner Server) bringt Windows Server 2012 (R2) eine Reihe von Tools mit, mittels derer die Administratoren die Konfiguration überprüfen können. Diese sollten regelmäßig genutzt und die Ergebnisse dokumentiert sowie für die Planung der Verbesserung genutzt werden.

Microsoft Security Assessment Tool 4.0

Beim Security Assessment Tool handelt es sich um eine sogenannte Risikomanagement-Anwendung. Diese ist als zweiteiliger Fragebogen realisiert. Der erste, kürzere Fragebogen nennt sich Business Risk Profile und versucht zu messen, wie viel Risiko mit der Geschäftstätigkeit der Institution verbunden ist. Da im IT-Grundschutz vergleichbare Verfahren verwendet werden, kann hier auf eine Anwendung verzichtet werden. Der zweite Teil heißt "Assessment" und ist aufwändiger zu beantworten. Es entsteht eine Auswertung der Effektivität der Sicherheitsstrategie in den vier Themenbereichen Personal, Prozesse, Ressourcen und Technik, basierend auf Best Practices und Standards wie ISO 27001 und NIST-800.x. Zwar ist auch dies in der IT-Grundschutz-Vorgehensweise bereits abgedeckt, jedoch können die vom Tool generierten Empfehlungen insbesondere aufgrund der zusätzlichen Hinweise und Verweise auf Material von Microsofts Trustworthy Computing Group lohnenswerte Quellen darstellen.

Darüber hinaus besteht die Möglichkeit des anonymisierten Uploads von Ergebnissen im Austausch für den Download von Benchmarks. Im Zweifel sollte auf den Upload verzichtet werden, um die mögliche Weitergabe von internen Informationen zu unterbinden.

Microsoft Baseline Security Analyzer 2.3

Der Baseline Security Analyzer bietet eine effiziente Methode, um eine ganze Reihe häufiger, sicherheitsrelevanter Fehlkonfigurationen zu erkennen.

Zum einen wird auf fehlende sicherheitsrelevante Updates (und ausschließlich auf solche) geprüft, und zwar bei Windows, Windows-Komponenten wie Internet Explorer, IIS, anderen Microsoft-Produkten wie SQL Server und Office-Makroeinstellungen. Die Updates werden über den Windows Update Agenten abgefragt, der seit Windows 2000 Service Pack 3 auf allen Systemen vorhanden ist. Beim Test auf sogenannte unsichere Einstellungen ("less-secure settings"), auch als Vulnerability Assessment (VA) bezeichnet, wird gegen eine Datenbank von Registry- und Dateieinstellungen geprüft. Beispielsweise könnte ein VA ausgeben, dass die Berechtigungen in einem Verzeichnis unter /www/root zu lasch gewählt sind

Der Ausführende benötigt auf dem zu scannenden Server lokale Adminrechte, zudem müssen die administrativen Freigaben aktiviert sein.

Security Configuration Wizard

Seit Windows Server 2003 Service Pack 1 auf Windows Serversystemen vorhanden ist das Tool Security Configuration Wizard (SCW). Es dient dazu, das Serverprofil zu prüfen und Empfehlungen zur Verbesserung der Sicherheit zu generieren. Bei Windows Server 2012 (R2) findet sich der SCW im neuen Server Manager-Dashboard.

Allgemein anerkannte grundlegende Empfehlungen wie "unbenutzte Dienste deaktivieren" oder "unbenutzte Features deinstallieren" werden auch in diesem Baustein genutzt. Wie aber ist in der Praxis nachprüfbar, dass bei einer großen Anzahl von Servern mit möglicherweise dutzenden von Rollen auf dem Netzserver und vielen unterschiedlichen Gruppen von Fileservern, Webservern, Datenbanken etc. alle nach Security Best Practice konfiguriert sind?

SCW kann helfen die Angriffsfläche zu verkleinern, indem Policies generiert werden, die einen Server auf die minimale Funktionalität beschränken, die für seine Rolle(n) benötigt wird.

Generierte Policies lassen sich direkt anwenden oder, dies ist zu empfehlen, als XML-Datei abspeichern. Aus diesen lässt sich über die PowerShell via

scwcmd transform /p:TemplateMeinServer.xml /g:GPO-Hardening-MeinServer

eine Policy (GPO) erzeugen, die dann auf alle Server mit derselben Charakteristik angewandt werden kann. Wie immer sollten neue Einstellungen kritisch begutachtet und vor Ausrollen auf Produktivsysteme getestet werden. Die Chance ist, dass so eine stärkere Standardisierung der Policies entsteht und die Konfigurationsdrift abnimmt.

SYS.1.2.2.M8 Schutz der Systemintegrität

Secure Boot sollte aktiv sein. AppLocker sollte aktiviert und möglichst strikt konfiguriert sein.

Secure Boot

Bei Secure Boot handelt es sich um einen Sicherheitsstandard aus den Reihen der Computerhersteller. Das Verfahren versucht sicherzustellen, dass nur Software gebootet wird, die vom PC-Hersteller als vertrauenswürdig angesehen wird. Realisiert wird dies durch digitale Signaturen auf Softwarekomponenten sowie eine Datenbank, die der Hersteller des Computers pflegt.

Beim Start des PCs prüft die Firmware die Signatur jeder Komponente der Boot-Software einschließlich der Treiber und des Betriebssystems. Nur wenn alle Signaturen gültig sind, wird der Bootprozess vollendet, andernfalls kommen herstellerspezifische Notmaßnahmen zum Tragen.

Nicht möglich ist die Nutzung von Secure Boot bei alter, nicht kompatibler Hardware oder im für den Serverbetrieb in der Regel nicht sinnvollen Dual Boot-Modus sowie bei virtuellen Maschinen, die Secure Boot nicht unterstützen.

Heutzutage kann in aller Regel von ausreichender Hardware und Kompatibilität ausgegangen werden, sodass es keinen Grund gibt, den wertvollen Integritätsschutz, den Secure Boot anbietet, nicht zu nutzen.

AppLocker

AppLocker bietet richtliniengesteuerte Zugriffskontrolle für Anwendungen und andere ausführbare Dateien. Hiermit können bestimmte Anwendungen erlaubt, andere wiederum blockiert werden. Mit Windows Server 2012 kam die Funktion hinzu, Regeln für Anwendungspakete zu definieren, was die Konfiguration von AppLocker für Apps aus dem Windows Store erlaubt. Seit R2 gibt es die Möglichkeit, Laufzeitinformationen von Prozessen zu beobachten und im Sicherheitsprotokoll festzuhalten, die für die zielgenaue Einstellung von AppLocker verwendet werden können (Audit-Modus). Dies sollte genutzt werden, um Ausfälle bis hin um Aussperren der Administratoren aus dem System zu vermeiden.

AppLocker ist ein mächtiges Werkzeug, um die Ausführung schädlicher Software deutlich zu erschweren. Trotz diverser Erleichterungen bleibt jedoch immer noch ein erheblicher Konfigurationsaufwand, sodass sich der Einsatz von AppLocker vor allem empfiehlt, wenn hoher Integritätsbedarf besteht oder die Konfiguration eines Servers relativ statisch ist. Dies ist bei Serversystemen unter Windows 2012 (R2), die lediglich eine Rolle anbieten, nicht selten der Fall.

Software Restriction Policies

Software Restriction Policies (SRP) ist eine ältere Funktion, mittels derer Programme identifiziert werden können, die auf Computern in der Domäne laufen sollen. Auch diese kann wie AppLocker dazu genutzt werden, mit großer Flexibilität die erlaubte Software in der ganzen Institution zu kontrollieren. SRP wird benötigt, wenn auch für Betriebssysteme vor Windows Server 2008 R2 oder Windows 7 Softwarebeschränkungen konfiguriert werden sollen, die kein AppLocker unterstützen.

Wie AppLocker auch wird SRP über GPOs konfiguriert. Wenn sowohl SRP- als auch AppLocker-Policies in derselben Domäne durch Gruppenrichtlinien angewandt werden, so werden die SRP-Richtlinien auf Rechnern, die AppLocker unterstützen, durch die AppLocker-Richtlinien überstimmt.

Es sollten immer getrennte GPOs verwendet werden, um SRP und AppLocker zu konfigurieren, um Fehler auszuschließen und insbesondere die Fehlersuche zu erleichtern.

SYS.1.2.2.M9 Lokale Kommunikationsfilterung

Grundsätzlich werden zentrale Maßnahmen wie Segmentierung von Netzen, Zonenbildung und Paketfilterung im Unternehmens- und Behördenbereich in der Regel durch dedizierte aktive Netzkomponenten realisiert, die an geeigneten Stellen aufgestellt werden. Im Sinn einer gestaffelten Verteidigung (Defense-in-Depth) sollte jedoch bei höherem Schutzbedarf auch die lokale Firewall aktiviert werden.

Windows Server 2012 (R2) bringt für diesen Zweck eine lokale Firewall mit, die sogenannte "Windows Firewall mit Advanced Security (WFAS)". Diese sollte aktiviert und für eingehenden wie ausgehenden Verkehr möglichst strikt eingestellt sein.

Die WFAS kann durch GPOs verwaltet werden. Dies ist zu empfehlen, um die Konfiguration konsistent und zentral zu halten. Die Verwaltung der konkreten Firewallregeln ist außerhalb des Scopes dieses Bausteins. Hierfür ist der Baustein Firewall anzuwenden.

Ebenfalls durch die WFAS realisiert werden die nativen IPsec-Features von Windows Server 2012 (R2). Diese sollten verwendet werden, um die Identität und Integrität der Verbindung zu Remote-Systemen sicherzustellen, da dies mit Paketfilterfunktionen allein nicht möglich ist. Die sichere Konfiguration von IPsec-Verbindungen ist ebenfalls nicht Inhalt dieses Bausteins. Sie wird im Baustein VPN abgehandelt.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

SYS.1.2.2.M10 Festplattenverschlüsselung bei Windows Server 2012 (C)

Ein geeignetes Mittel zum Schutz der Vertraulichkeit von Daten im Ruhezustand, also nicht während des Transports, ist die Verschlüsselung von Festplatten und sonstigen Datenträgern. Dabei ist zu beachten, dass die Daten für die Bearbeitung entschlüsselt werden müssen (z. B. im Fall der Verschlüsselung des Bootmediums bereits während des Bootvorgangs) und grundsätzlich lesbar bleiben, bis das System heruntergefahren oder in den Ruhemodus versetzt wird. Da Serversysteme häufig rund um die Uhr laufen, ist der Schutz letztlich beschränkt, kann aber gegen physische Angriffe wie Diebstahl von Datenträgern gleichwohl hilfreich sein, wenn er mit geeigneten anderen Maßnahmen kombiniert wird. Windows bringt zu diesem Zweck das Tool BitLocker mit, das auch in Windows Server 2012 (R2) in allen Editionen verfügbar ist.

BitLocker unterstützt Geräteverschlüsselung auf x86- und x64-basierten Systemen, welche die Anforderungen des Windows Hardware Certification Kit (HCK) für ein TPM (Trusted Platform Module) und Secure Boot mit sogenannter "Connected Stand-by"-Funktion erfüllen. Die Geräteverschlüsselung schützt sowohl das Betriebssystem als auch weitere angeschlossene Festplatten. Grundsätzlich kann Geräteverschlüsselung mit einem Microsoft-Account oder einem Domänen-Account genutzt werden.

BitLocker unterstützt mit Windows Server 2012 (R2) die Algorithmen AES-128-CBC und AES-256-CBC. Zur Verschlüsselung mit BitLocker wird ein Key Protector benötigt, der vorhanden sein muss, um das Laufwerk entschlüsseln zu können. In der Standardkonfiguration sind dies ein TPM-Modul und ein zusätzlicher Wiederherstellungsschlüssel, mit dessen Hilfe das Laufwerk auch ohne das TPM-Modul entschlüsselt werden kann. Bei Enterprise-Umgebungen mit einem Active Directory kann der Wiederherstellungsschlüssel auch im Active Directory abgelegt werden.

Windows Server 2012

Bezüglich Vorgängerversionen haben sich die Möglichkeiten von BitLocker in Windows 8 und Server 2012 erweitert:

Installation

BitLocker kann nun Festplatten bereits während der Installation verschlüsseln. Dies ist zu empfehlen, da so das System nicht für gewisse Zeit im Klartext vorliegt.

Administratoren können dazu BitLocker vor der Installation vom Windows Preinstallation Environment (WinPE) aktivieren. Dies geschieht mit einem zufälligen Klartext-Schlüssel, der auf die frisch formatierte Festplatte angewendet wird, bevor der Setup-Prozess startet. Neu hinzugekommen ist auch die Option "Used Disk Space Only", bei der nur der bisher tatsächlich verwendete Speicher verschlüsselt wird. Dies benötigt an dieser Stelle in der Regel nur wenige Sekunden und behindert so den Installationsprozess nicht merklich.

Den BitLocker-Status einer Partition kann der Administrator im BitLocker-Control Panel oder auch im Windows Explorer prüfen. Wurde eine Festplatte während der Installation zunächst mit Klartext-Schlüssel verschlüsselt, wird der Status "Waiting For Activation" mit einem gelben Ausrufezeichen angezeigt. Dies bedeutet, dass für einen vollständigen Schutz der Partition der Schlüssel noch geschützt werden muss. Dafür fügt der Administrator über das Control Panel, das manage-bde-Tool oder die WMI-APIs einen geeigneten Schlüsselschutz hinzu.

Schlüsselschutz (Key Protector)

Für einen vollständigen BitLocker-Schutz muss der zufällige Verschlüsselungsschlüssel seinerseits geschützt werden. Hierfür gibt es verschiedene Varianten:

Speichermedium	Schlüsselschutz (Key Protector)
Betriebssystem	• • • •
andere Festplatte	• • •
Wechselfestplatte	• •

Used Disk Space Only

BitLocker bietet nun zwei Verschlüsselungsmethoden, "Used Disk Space Only" und "Full Volume Encryption". Ersteres arbeitet viel schneller während der Erstverschlüsselung, da zunächst nur die bereits genutzten Blöcke der Partition verschlüsselt werden. Die Vollverschlüsselung verschlüsselt immer alle Blöcke einschließlich des freien Speicherplatzes.

Folgende GPOs für BitLocker, die Used Drive Encryption bzw. Full Volume Encryption erzwingen, sind verfügbar unter \Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption

- Fixed Data Drives\Enforce drive encryption type on fixed data drives
- Operating System Drives\Enforce drive encryption type on operating system drives
- Removable Data Drives\Enforce drive encryption type on removable data drives

Ist hier nichts konfiguriert, kann der Administrator frei entscheiden, wenn er BitLocker aktiviert.

Bei normalen und hohen Vertraulichkeitsanforderungen genügt in der Regel die Teilverschlüsselung. Bei sehr hohen Vertraulichkeitsanforderungen sollte immer eine Vollverschlüsselung gewählt werden, da bereits die sich ändernde Datenmenge, die in dem Fall leicht ablesbar ist, Informationen über die Daten preisgeben kann (ein sogenannter Seitenkanalangriff). Auch für die Erreichung des Ziels Abstreitbarkeit ist eine Vollverschlüsselung zu empfehlen.

Wenn der erhöhte Zeitbedarf für die Vollverschlüsselung keine negative Auswirkung auf den Deploymentprozess hat, sollte grundsätzlich voll verschlüsselt werden.

PIN- und Passwortänderung für Standardnutzer

Diese Funktion erlaubt einem Standardnutzer, die BitLocker-PIN bzw. das Passwort auf Betriebssystempartitionen bzw. das BitLocker-Passwort auf Datenpartitionen selbst zu ändern, was helfen kann, Anfragen an den Support zu reduzieren.

Network Unlock

Diese Funktion ermöglicht, ein BitLocker-geschütztes System während des Bootvorgangs automatisch über das Netz zu entschlüsseln. Auch dies kann Anfragen beim Support vermeiden und trägt zur Benutzerfreundlichkeit bei.

Technisch handelt es sich bei Network Unlock um eine neue Option für den Schlüsselschutz. Benötigt wird dafür ein in der UEFI-Firmware implementierter DHCP-Treiber.

Betriebssystempartitionen, die mit TPM+PIN geschützt sind, verlangen die manuelle Eingabe der PIN beim Booten und Erwachen aus dem Ruhemodus (Hibernation), z. B. bei konfiguriertem Wake-on-LAN. Dies macht es aufwändig, etwa automatisiert Patches auszurollen. Network Unlock bietet eine Möglichkeit, die Rechner trotzdem ohne Interaktion hochzufahren.

Ähnlich wie bei TPM+StartupKey wird hier ein verschlüsselter Startup Key aus dem Netz heruntergeladen und mit Hilfe des TPMs entschlüsselt. Der Netzschlüssel ist auf einem Systemlaufwerk im Netz gespeichert und mit einem AES 256-Bit-Sessionkey sowie dem 2048-Bit-RSA-Publickey des Serverzertifikats verschlüsselt. Ist Network Unlock nicht verfügbar, wird wie gehabt der normale TPM+PIN-Eingabebildschirm angezeigt. Serverseitig wird die Verteilung eines RSA-Schlüsselpaars per Group Policy Management Console auf dem Server 2012 Domain Controller benötigt.

Unterstützung von Hardwareverschlüsselung

Mit Windows Server 2012 ist es möglich, auch andere, per Hardwareverschlüsselung verschlüsselte Festplatten in der BitLocker-Konsole zu verwalten, um eine gemeinsame Verwaltungsoberfläche zu schaffen.

Windows Server 2012 R2

Mit Windows 8.1 und Server 2012 R2 kamen folgende Erweiterungen der BitLocker-Funktionalität hinzu:

Anders als die bisherige BitLocker-Implementierung ist die sogenannte Geräteverschlüsselung (Device Encryption), die im Hintergrund ebenfalls auf BitLocker basiert, automatisch aktiviert, sodass das Gerät von Anfang an verschlüsselt wird. Dies geschieht folgendermaßen:

Während einer Neuinstallation von Windows Server 2012 R2 wird der Server für die erste Verwendung vorbereitet. Dabei werden auch die Geräteverschlüsselung initialisiert und der Datenträger des Betriebssystems sowie die anderen Festplatten zunächst mit einem im Klartext gespeicherten Schlüssel verschlüsselt. Die Sicherheit der Daten zu diesem Zeitpunkt entspricht einer BitLocker-Verschlüsselung im Standby-Modus (Suspended), bei der der Schlüssel im Klartext auf der Festplatte vorliegt.

Falls der Server nicht zu einer Domäne hinzugefügt wird, wird ein Microsoft-Account benötigt, dem administrative Rechte auf dem Server eingeräumt wurden. Sobald der Administrator sich mit dem Microsoft-Account anmeldet, wird der Klartextschlüssel gelöscht, ein Wiederherstellungsschlüssel in den Microsoft-Account (online) hochgeladen und der TPM-Schutz erstellt. Sollte der Wiederherstellungsschlüssel später benötigt werden (z. B. bei einem Schaden des TPM), kann der Administrator diesen über ein Zweitgerät und das Microsoft-Konto wieder beziehen.

Meldet sich der Benutzer über einen Domänenaccount an, wird der Klartextschlüssel erst in dem Moment gelöscht, wenn der Server die Domäne betreten hat und der dann erzeugte Wiederherstellungsschlüssel erfolgreich in die Active Directory Domain Services gesichert wurde. Die GPO "Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives" muss aktiviert und die Option "Do not enable BitLocker until recovery information is stored in AD DS for operating system drives" sollte ausgewählt sein. Erst danach aktiviert sich der TPM-Schutz und schließt so die Geräteverschlüsselung ab.

Im Einsatz in Behörden und Unternehmen sollte der Wiederherstellungsschlüssel im AD gespeichert und auf die Online-Variante mit dem Microsoft-Konto verzichtet werden, da im letzteren Fall keine Kontrolle darüber besteht, was mit diesem Schlüssel geschieht.

FIPS-Unterstützung für das Recovery-Passwort

Seit Windows Server 2012 R2 existiert ein FIPS-Modus, der es erlaubt, BitLocker kompatibel mit dem US-amerikanischen öffentlichen Krypto-Standard (Federal Information Processing Standard) zu betreiben.

BitLocker auf virtuellen Maschinen

Die Verschlüsselung von virtuellen Maschinen bietet sich an, wenn entweder das Hostsystem nicht verschlüsselt werden kann oder soll oder aber der Vertraulichkeitsbedarf der Daten in der VM höher ist oder diese aus anderen Gründen vom Hostsystem abgeschirmt werden sollen. Auch hier gilt, dass Festplattenverschlüsselung (FDE: Full Disk Encryption) keinen wirksamen Schutz gegen Auslesen von Daten im laufenden Betrieb, d. h. mit entschlüsselten Datenträgern, darstellt. Als Zusatzmaßnahme kann daher organisatorisch festgelegt werden, dass verschlüsselte VMs erst dann entschlüsselt werden dürfen, wenn sie benötigt werden und nach Benutzung möglichst schnell wieder heruntergefahren werden müssen.

Da virtuelle Maschinen nicht über ein TPM verfügen, müssen folgende zwei Schritte ausgeführt werden, bevor BitLocker (das auf dem Server installiert sein muss) aktiviert werden kann:

1. In der GPO "Computer Configuration/Administrative Templates/Windows Components/BitLocker Drive Encryption/Operating System Drives" muss "Require additional authentication at startup" auf "Enable" und "Allow BitLocker without a compatible TPM" konfiguriert sein (z. B. mit dem lokalen Gruppenrichtlinieneditor gpedit.msc).

2. Nach einem Neustart der VM ist im Control Panel BitLocker zu aktivieren.

SYS.1.2.2.M11 Angriffserkennung bei Windows Server 2012 (CIA)

Oft stellt sich bei der Sicherheitvorfallsbehandlung heraus, dass die Protokollierung unzureichend war, um den Vorfall aufzuklären und Gegenmaßnahmen zielgerichtet planen zu können. Häufige Fehler sind:

- fehlendes zentrales Logging,
- fehlendes Logging von Mitgliedsservern und Endpunkten (nur Domaincontroller),
- Unübersichtlichkeit durch zu viele Daten im Protokoll,
- fehlende Aufzeichnung zentraler Ereignisse,
- zu schnelles Überlaufen (Rolling / Rotating) der Protokolle.

Z. B. werden zentrale Events wie Logins standardmäßig nur auf dem System selbst geloggt. Der AD protokolliert seinerseits nur die Ticketerstellung, hat aber kein Bild von der Session als solcher (inklusive deren Anfang und Ende).

Als Mindestanforderung sollten die folgenden Ereignisse von allen Systemen protokolliert und ausgewertet werden:

- das Löschen von Sicherheits-Logs,
- Änderungen an kritischen Gruppen wie Domänenadministratoren,
- Änderungen an lokalen Admingruppen,
- das Anlegen und Löschen lokaler Benutzer,
- die Installation neuer Dienste, vor allem auf Domänencontrollern (ein mögliches Anzeichen für Schadsoftware oder laterale Bewegungen von Angreifern).

Der erste Schritt zu einer Angriffserkennung ist die zentrale Sammlung aller relevanten Ereignisdaten. Eigens dafür entwickelte Systeme wie SIEM (Security Incident und Event Management) sind in der Regel teuer und aufwändig einzurichten und zu betreiben. Sie sind nicht Thema dieses Bausteins. Jedoch lässt sich bereits mit Windows Server-Bordmitteln Wesentliches erreichen.

Nutzung des Windows Event Frameworks (WEF)

Mit dem Windows Event Framework (WEF) verfügt Windows über eine bereits integrierte Lösung, die mindestens als Komplement für ein SIEM eingesetzt werden kann. Wichtige Basisfunktionen einer Eventüberwachung können sogar komplett mit WEF realisiert werden.

Event Forwarding, also die gezielte automatische Weiterleitung von Events, kann die Sichtbarkeit kritischer Events deutlich erhöhen, insbesondere die von dezentralen Servern oder auch Clients, die keinen Agenten eines proprietären Monitoringsystems installiert haben. Die Auswahl, welche Events zentral geloggt werden sollen, ist außerhalb dieses Bausteins und als Teil eines übergreifenden Loggingkonzepts zu sehen (siehe Baustein OPS1.1.7 Protokollierung).

WEF lässt sich mit GPOs konfigurieren. Events können im nativen .evtx-Format exportiert werden. Dieses ist XML-basiert und damit leicht auswertbar.

Im Push-Modus leiten Systeme bestimmte Ereignisse automatisch an den sogenannten Collector (#Server) weiter. Somit ist es für Administratoren, die nicht Sicherheitsverantwortliche sind, möglich, für die von ihnen verantworteten Systeme zusätzliche Events zu konfigurieren.

Für die Einrichtung wird lediglich ein Windows Server benötigt und eine GPO. Außerdem muss dem Netzdienst (lediglich dem lokalen auf dem jeweiligen System) das Leserecht am Protokoll eingeräumt werden und der WinRM-Dienst muss auf allen zu beobachtenden Systemen gestartet sein. Er braucht nicht (auto-)konfiguriert zu werden, was ihn im lauschenden, sprich eher angreifbaren Zustand belassen würde. Werden lediglich kritisch Events geloggt, so ist nicht mit sehr großen Logdateien zu rechnen.

Auf dem Collector wird die Autokonfiguration über den Befehl "winrm qc" in einem administrativen Prompt aufgerufen. Automatisches Starten des WinRM-Dienstes sollte auf Nachfrage aktiviert werden, das ebenfalls abgefragte automatische Öffnen der Firewall lässt sich noch sicherer per GPO erledigen. Nun können im Eventviewer unter "Subscriptions" eingehende Events eingesehen werden.

Anschließend können per GPO die weiterzuleitenden Events definiert werden. Systeme, die die GPO anwenden, werden beim Windows Event Collector nachfragen, ob Subskriptionen für sie vorliegen und nur in diesem Fall die gewünschten Events senden.

Es ist durchaus möglich, die Gesamtheit aller Security Events der Domäne im WEF einzusammeln. Dies kann sinnvoll sein, wenn kein anderes zentrales Loggingsystem vorhanden ist und trotzdem forensische Untersuchungen möglich sein sollen. Ansonsten besteht die Stärke des WEF hauptsächlich in der gezielten Sammlung und Filterung kritischer Ereignisse. So kann auch ein SIEM, das sämtliche Ereignisse aufzeichnet, am besten ergänzt werden: das SIEM für die Vollständigkeit, WEF für die Sichtbarkeit, auch in Bereiche der Umgebung, die nicht vom SIEM abgedeckt sind. Das SIEM kann Ereignisse aus diesen dann wiederum beim Collector abholen und somit noch besser die einheitliche Sicht auf alles bereitstellen.

Sperrung nach missglückten Entschlüsselungsversuchen

Benutzerkonten können mit einer Schwelle versehen sein, wie viele Anmeldeversuche möglich sind, bevor der Account gesperrt ist. Dies ist ein Standardverfahren, um Brute-Force-Angriffe zu behindern. Gleichzeitig besteht die Gefahr, dass Sperren absichtlich provoziert werden, um Denial-of-Service zu erreichen.

Da Datenträgerverschlüsselung eine Erweiterung des Zugriffsschutzes auf die Daten auf Festplatten darstellt, die ebenfalls per Brute Force angegriffen werden kann, ist hier eine vergleichbare Maßnahme möglich:

Seit Windows 8 und Server 2012 ermöglicht die Policy "\Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Machine account lockout threshold" ein automatisches Sperren von Partitionen nach einer definierten Anzahl vergeblicher Loginversuche im Sinn der Vernichtung des primären Key Protectors. Danach lässt sich das Volume nur noch per Wiederherstellungsschlüssel entschlüsseln. Dieser muss von einem autorisierten Benutzer im sogenannten "Device Lockout-Modus", in den das System automatisch rebootet, eingegeben werden, um wieder Zugriff zu erhalten. Es zählen fehlerhafte Loginversuche sowohl auf per Strg-Alt-Entf gesperrten Systemen als auch bei passwortgeschützten Bildschirmschonern.

Der Schwellwert kann zwischen 4 und 999 gewählt werden (1-3 werden automatisch als 4 interpretiert), 0 schaltet die Sperrung ab. Der Wert sollte mit der Schwelle für die normale Accountsperre korrelieren und jedenfalls nicht niedriger als diese sein, damit nach einer normalen Accountsperre noch ein normales Entsperren des Accounts veranlasst werden kann.

SYS.1.2.2.M12 Redundanz und Hochverfügbarkeit (A)

Wenn besonders hohe Verfügbarkeitsanforderungen an ein System bestehen, das unter Windows Server 2012 (R2) betrieben wird, so ergeben sich mögliche Maßnahmen im Wesentlichen aus der jeweiligen Anwendung. Bei einem Fileserver wird ein verteiltes Dateisystem eine Lösungsvariante darstellen, bei einem Active Directory der Einsatz mehrerer Domaincontroller und bei einem Webserver z. B. Load Balancing. Für das Thema Hochverfügbarkeit sei daher vor allem auf die jeweiligen Anwendungsbausteine verwiesen.

Darüber hinaus gibt es jedoch einige Maßnahmen, die auf Betriebssystemebene von Windows Server 2012 (R2) umgesetzt werden können, um die Verfügbarkeit zu erhöhen.

Failover Cluster

Mehrere Windows-Server können in einem Verbund betrieben werden. Analog zu den Server-Rollen, die auf einzelnen Systemen laufen, gibt es auch diverse Cluster-Rollen, die in einem Failover-Cluster betrieben werden können. Dabei ist immer jeweils einer der Knoten des Clusters verantwortlich für den Betrieb der Rolle. Fällt der Knoten aus oder verliert er die Konnektivität, übernimmt einer der anderen Knoten. Die Ausfallsicherheit kann so erhöht werden, da im Fehlerfall ein anderes System den Betrieb übernimmt. Die Liste der Rollen, die direkt auf einem Cluster ausgeführt werden können, ist relativ eingeschränkt. Allerdings können auch virtuelle Maschinen auf einem Failover Cluster betrieben werden, so dass ganze Systeme, die kritische Dienste zur Verfügung stellen, als virtuelle Maschine hochverfügbar gemacht werden können.

Network Load Balancing

Mit der Funktion Network Load Balancing können zwei oder mehr Windows Server Netzdienste über TCP/IP unter einer gemeinsamen Adresse anbieten. Die Server und die Dienste sind unabhängig voneinander und teilen keine Ressourcen. Netzanfragen an die gemeinsame Adresse werden auf die Server im Verbund verteilt.

NIC-Teaming

NIC-Teaming (von Network Interface Card), auch bekannt als Load Balancing/Failover (LBFO) ermöglicht es, mehrere Netzschnittstellen in sogenannte Teams zusammenzufassen um

a.) Bandbreitenkapazitäten zu bündeln und/oder

b.) im Fall eines Versagens einer Schnittstelle oder Verbindung einen Failover (Rückfall) für den Netzverkehr zu haben.

Seit Windows Server 2012 ist diese Technik nativ im Betriebssystem verfügbar.

Da das Thema NIC-Teaming vielfältig ist und stark vom konkreten Einsatzszenario abhängt, können in diesen Umsetzungshinweisen nur allgemeine Hinweise gegeben werden. Für Details zu NIC-Teaming in Windows Server 2012 (R2) bietet Microsoft daher einen "NIC Teaming User Guide" an.

Grundfunktion von NIC-Teaming

Netzwerkkarten der gleichen Geschwindigkeit lassen sich ohne Zusatzwerkzeuge zu Teams zusammenfassen, soweit die Hersteller die Funktion unterstützen. Mit Bluetooth- oder WLAN-Adaptern ist dies nicht möglich. Die Konfiguration erfolgt im Server-Manager oder per PowerShell, auch über das Netz.

Das LBFO in Windows Server 2012 lässt sich nicht mit NIC-Teaming anderer Hersteller kombinieren. Treten in so einem Fall Störungen auf, lässt sich die Teamkonfiguration mit der PowerShell folgendermaßen löschen:

Get-NetLbfoTeam | Remove-NetLbfoTeam

Kommt Virtualisierung mit Hyper-V zum Einsatz, so muss der Teamvorgang vor der Erstellung von virtuellen Switches in Hyper-V durchgeführt werden, da sonst die physische Netzverbindung nicht mehr für den Teamvorgang verfügbar ist. Darüber hinaus sind hier weitere Besonderheiten zu beachten.

NIC-Teaming-Architektur

Es existieren verschiedene Architekturen, in denen NIC-Teaming verwendet werden kann. Bei Switch-unabhängigem Teaming weiß der Switch nichts von Teamzugehörigkeit, die NICs können auch an verschiedenen Switches angeschlossen sein, müssen dies jedoch nicht. Beim Switch-abhängigen Teaming, bei dem das gesamte Team am selben physischen Switch hängen muss, sind Netzwerkkarten und Switch für das Teaming konfiguriert. Dies kann statisch geschehen (eine Funktion, die typischerweise von Server-geeigneten Switchen unterstützt wird) oder dynamisch vereinbart werden über das Protokoll IEEE 802.1ax (LACP: Link Aggregation Control Protocol).

Algorithmen zur Verteilung des Datenverkehrs

Um die mögliche kombinierte Bandbreite auch nutzen zu können, ist es notwendig, den Datenverkehr sinnvoll auf die Netzwerkkarten zu verteilen. In der Regel erfolgt dies nach Adress-Hashing, einem Verfahren, das Pakete anhand ihrer Adressdaten pseudozufällig auf die Adapter verteilt. Beim Einsatz von Virtualisierung kann eine viel feingranularere Verteilung erreicht werden, wenn zusätzlich der virtuelle Hyper-V-Switchport mit in den Verteilungsalgorithmus einbezogen wird.

Je nach Setup und Anforderungen bieten unterschiedliche Kombinationen aus Architektur und Verteilungsalgorithmus verschiedene Vor- und Nachteile.

Unterschiede zwischen Windows Server 2012 und 2012 R2

Die hauptsächlichen Unterschiede in Bezug auf NIC-Teaming betreffen

- die Ergänzung des dynamischen Load Balancing-Modus (s. o.) und
- verbesserte Interoperabilität und Leistungsfähigkeit in Zusammenhang mit Hyper-V Netzvirtualisierung (NVGRE).

BranchCache

BranchCache ist eine Technik zur Optimierung der Nutzung von Übertragungskapazitäten im WAN, z. B. bei der Anbindung von Außenstellen. Um Bandbreite zu sparen, kopiert BranchCache Inhalte von zentralen Servern und speichert diese in der Außenstelle (englisch branch office) zwischen (sogenanntes Caching), sodass sie bei erneutem Zugriff nicht mehr übertragen werden müssen.

BranchCache basiert auf tiefliegenden Funktionen des Windows Fileservers. So werden Dateien in kleine Abschnitte eingeteilt, um Duplikate finden und eliminieren zu können. Insbesondere kleinere Änderungen in großen Dateien führen so nicht zur kompletten Neuübertragung.

Die Konfiguration kann auch für größere Institutionen durch einen einzelnen kleinen Satz von GPOs erfolgen.

Mit Windows Server 2012 (R2) erfolgt die Speicherung des Caches inzwischen verschlüsselt, sodass zumindest bei normalen Vertraulichkeitsanforderungen auf eine weitere Verschlüsselung etwa der Datenträger verzichtet werden kann.

In vorherigen Versionen wurden Serverzertifikate benötigt, was einen komplexen PKI-Betrieb voraussetzte. Inzwischen werden diese nicht mehr benötigt, da Verschlüsselung und Authentisierung anders gelöst sind.

SYS.1.2.2.M13 Starke Authentifizierung bei Windows Server 2012 (CI)

Es sollte ein rollenbasiertes Administrations-Modell für die Administration unterschiedlicher Serverfunktionen entworfen und umgesetzt werden. Für kritische Dienste sollte eine Zwei-Faktor-Authentifizierung implementiert sein.

Rollenbasiertes Administrationskonzept

Die Unterscheidung in Administratoren und normale Benutzer ist wichtig, allerdings relativ grob. Sie missachtet, dass es in der Realität verschiedene Arten administrativer Aufgaben oder, allgemeiner gesprochen, hierarchischer und teilweise auch überlappender Rollen und Verantwortlichkeiten gibt. Um das Prinzip des Least Privilege konsequenter durchzusetzen, ist daher ein feingranulareres rollenbasiertes Administrationskonzept zu entwickeln. Dies ist insbesondere für größere Institutionen sinnvoll und realistisch.

Ein solches Administrationskonzept kann nicht allein mit Blick auf Windows Server 2012 (R2) aufgestellt werden. Vielmehr sind unterschiedliche Rollen (verschiedene Arten von Domain Controllern, Mitgliedsserver, Clientsysteme etc.) zu betrachten. Dieser Versuch wird im Baustein APP.2.2 Active Directory unternommen.

Smartcards

Smartcards eignen sich als schwer zu fälschende mobile Sicherheitsmerkmale, etwa in der Zwei-Faktor-Authentifizierung oder für Signaturen. Mit Windows Server 2012 wurde die Nutzung von Smartcards im Sinn der stärkeren Integration in eine größere Anzahl von Anwendungen verbessert. Zudem kam die Möglichkeit hinzu, sogenannte virtuelle Smartcards zu verwenden.

Virtuelle Smartcards

Virtuelle Smartcards ermöglichen Multi-Faktor-Authentifizierung in vielen Arten von Infrastrukturen auch in dem Fall, dass Benutzer keine physische Karte mit sich führen. Hierfür wurde der Prozess vereinfacht, beliebige Geräte mit TPM als virtuelles Smartcard-Gerät zu registrieren, unabhängig davon, ob sie Domänenmitglieder sind und wie ihre Hardware ansonsten beschaffen ist. Dies setzt die Hürde für den Einsatz von Smartcards als weiteres Authentifizierungsmerkmal deutlich herab.

Windows Biometric Framework

Auch das Windows Biometric Framework (WBF), ein Satz an Diensten und Schnittstellen für biometrische Devices, wurden erweitert. Fast User Switching und die Synchronisation von Passwörtern mit Fingerabdrücken sind nun möglich.

Es ist jedoch zu beachten, dass biometrische Daten einige Nachteile haben, die sie als Identifikations- und Authentifizierungsmerkmale aus Sicherheitssicht weitgehend unbrauchbar machen. Neben der Tatsache, dass viele biometrische Merkmale weltweit nicht eindeutig sind, sind sie häufig relativ leicht zu fälschen und können vor allem, einmal bekannt geworden, nicht geändert werden.

SYS.1.2.2.M14 Herunterfahren verschlüsselter Server und virtueller Maschinen (CI)

Wenn Festplatten verschlüsselt sind, um die Vertraulichkeit oder Integrität von Daten zu schützen, steht idealerweise der Schlüssel zur Entschlüsselung nicht permanent bereit, sondern erfordert eine Interaktion eines Administrators oder zumindest eine protokollierte technische Anfrage im Netz bzw. am AD. Ansonsten kann ein Angreifer oder Innentäter die Daten im laufenden Betrieb auslesen bzw. manipulieren. Dafür muss BitLocker bzw. die Geräteverschlüsselung in einem Modus aktiviert sein, der nicht ausschließlich auf dem TPM basiert, und der zusätzliche Schlüsselschutz (Key Protector),etwa ein USB-Key, sollte nicht permanent gesteckt sein. Dies erhöht zwar den Aufwand im Betrieb, stellt jedoch eine deutlich höhere Hürde für Angreifer dar.

3 Weiterführende Informationen

3.1 Wissenswertes

Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Windows Server 2012" finden sich unter anderem in folgenden Veröffentlichungen:

[ADRL] AD Reading Library

(Active Directory Security), mit weiterführender Literatur des AD Security Blogs, https://adsecurity.org/page_id=41, zuletzt abgerufen am 24.08.2018

[LAPS1] Local Administrator Password Solution

Microsoft Technet, https://technet.microsoft.com/en-us/mt227395.aspx, zuletzt abgerufen am 24.08.2018

[PAYNE] Windows Event Forwarding for everyone

Microsoft Technet, Blog, Jessica Payne, November 2015, https://blogs.technet.microsoft.com/jepayne/2015/11/23/monitoring-what-matters-windows-event-forwarding-for-everyone-even-if-you-already-have-a-siem/, zuletzt abgerufen am 24.08.2018

[TN730960] Security Tools to Administer Windows Server 2012

Microsoft Technet, März 2013, https://technet.microsoft.com/en-us/library/jj730960.aspx, zuletzt abgerufen am 24.08.2018

[TN831360] Secure Windows Server 2012 R2 and Windows Server 2012

Micorosoft TechNet, November 2013, https://technet.microsoft.com/en-us/library/hh831360.aspx, zuletzt abgerufen am 24.08.2018

[TN831778] Security and Protection

Microsoft TechNet, Februar 2014, https://technet.microsoft.com/en-us/library/hh831778.aspx, zuletzt abgerufen am 24.08.2018

[TN832031] Secure Windows

Für Windows 8/8.1 (gilt größtenteils auch für Windows Server 2012 / 2012 R2), März 2014, https://technet.microsoft.com/en-us/library/hh832031.aspx, zuletzt abgerufen am 24.08.2018

SYS.2: Desktop-Systeme

Umsetzungshinweise zum Baustein SYS.2.1 Allgemeiner Client

1 Beschreibung

1.1 Einleitung

Als "Allgemeiner Client" wird ein IT-System mit einem beliebigen Betriebssystem bezeichnet, das die Trennung von Benutzern zulässt. Es sollten mindestens eine Administrator- und eine Benutzer-Umgebung eingerichtet werden können. Typischerweise ist ein solches IT-System vernetzt und wird als Client in einem Client-Server-Netz betrieben. Das IT-System kann auf einer beliebigen Plattform betrieben werden. Dabei kann es sich beispielsweise um einen PC mit oder ohne Festplatte, um ein mobiles oder stationäres Gerät, aber auch um eine Unix-Workstation oder einen Apple Mac handeln. Das IT-System verfügt in der Regel über Laufwerke für auswechselbare Datenträger, weitere Schnittstellen für den Datenaustausch sowie andere Peripheriegeräte.

1.2 Lebenszyklus

Planung und Konzeption

Für die sichere Nutzung von IT-Systemen müssen vorab die Rahmenbedingungen festgelegt werden. Dabei müssen die Sicherheitsanforderungen für die bereits vorhandenen IT-Systeme sowie die geplanten Einsatzszenarien von Anfang an mit einbezogen werden (siehe SYS.2.1.M10 Planung des Einsatzes von Clients). Schon vor der Beschaffung der Clients und Software sollte eine Sicherheitsrichtlinie für die Clients erstellt werden (siehe SYS.2.1.M9 Festlegung einer Sicherheitsrichtlinie für Clients).

Beschaffung

Für die Beschaffung von Clients, die typischerweise in größeren Mengen erfolgt, müssen ausgehend von den Einsatzszenarien Kriterien für die Auswahl geeigneter Produkte formuliert werden (siehe hierzu SYS.1.1.M11 Beschaffung eines Client). Auch bei der Beschaffung von Einzelsystemen ist es wichtig, dass der Client zur vorhandenen Struktur passt, damit nicht für ein einzelnes IT-System wegen dessen Besonderheiten ein unangemessen hoher Aufwand bei Integration und Betrieb entsteht.

Falls Hard- oder Software nicht die festgelegten Sicherheitsanforderungen erfüllen, sind weitere Maßnahmen erforderlich. Diese können organisatorischer Art sein (beispielsweise durch Regelungen, dass der Client ausschließlich hinter verschlossener Bürotür betrieben werden darf) oder es können in speziellen Fällen Zusatzkomponenten beschafft werden, um die identifizierten Mankos auszugleichen.

Bei besonders hohen Anforderungen an die Verfügbarkeit der Clients ist für diese der Einsatz einer Unterbrechungsfreien Stromversorgung (USV) empfehlenswert (siehe SYS.2.1.M39 Unterbrechungsfreie und stabile Stromversorgung). Dabei kann es sich beispielsweise um eine "Einzelplatz-USV" handeln, falls die hohen Anforderungen nur für einzelne Clients gelten, oder aber um einen eigenen entsprechend abgesicherten Stromkreis ("rote Steckdose").

Umsetzung

Um Risiken durch Fehlbedienung oder absichtlichen Missbrauch der IT-Systeme auszuschließen, sind eine sorgfältige Auswahl der Betriebssystem- und Softwarekomponenten, eine sichere Installation und sorgfältige Konfiguration wichtig. Die dabei zu treffenden Maßnahmen sind in hohem Grade abhängig von dem eingesetzten Betriebssystem. Näheres dazu findet sich deswegen in spezifischen Bausteinen, beispielsweise in SYS.2.3 Client unter Linux oder SYS.2.3 Client unter Windows 10.

Der Grundstein für die Sicherheit wird bereits bei der Vorbereitung der Installation gelegt. Vor der Installation sollte festgelegt werden, welche Komponenten des Betriebssystems und welche Anwendungsprogramme und Tools installiert werden sollen. Die getroffenen Entscheidungen müssen so dokumentiert werden, dass gegebenenfalls nachvollzogen werden kann, wie die IT-Systeme konfiguriert und mit welcher Software ausgestattet wurden (siehe SYS.2.1.M15 Sichere Installation und Konfiguration von Clients).

Betrieb

Eine der wichtigsten Sicherheitsmaßnahmen beim Betrieb heutiger Client-Systeme ist es, die IT-Systeme durch die Installation und permanente Aktualisierung eines Virenscanners (siehe dazu auch SYS.2.1.M6 Einsatz von Viren-Schutzprogrammen) zu schützen. Daneben ist eine regelmäßige Datensicherung (siehe auch SYS.2.1.M4 Regelmäßige Datensicherung) eine grundlegende Voraussetzung dafür, dass Hardwaredefekte und Programm- oder Benutzerfehler nicht zu gravierenden Datenverlusten führen.

Aussonderung

Bei der Aussonderung eines Clients muss zunächst sichergestellt werden, dass alle Benutzerdaten gesichert oder auf ein Ersatzsystem übertragen werden. Anschließend muss dafür gesorgt werden, dass keine sensitiven Daten auf den Festplatten des Clients zurück bleiben. Dazu genügt es nicht, die Platten einfach neu zu formatieren, sondern sie müssen mindestens einmal vollständig überschrieben werden. Es ist zu beachten, dass die Daten nicht wirklich von den Festplatten entfernt werden, wenn sie nur logisch gelöscht oder mit den Mitteln des installierten Betriebssystems neu formatiert werden. Mit geeigneter Software können Daten, die auf diese Weise gelöscht wurden, wieder rekonstruiert werden, oft sogar ohne großen Aufwand. Nach der Aussonderung eines Clients müssen Bestandsverzeichnisse und Netzpläne aktualisiert werden. Vertiefende Informationen hierzu sind in SYS.2.1.M27 Geregelte Außerbetriebnahme eines Clients zu finden.

Notfallvorsorge

Das notwendige Maß an Notfallvorsorge für einen allgemeinen Client ist stark vom individuellen Einsatzszenario abhängig. Oft wird als Notfallvorsorge für einen Client ausreichend sein, regelmäßig die Daten zu sichern und einen bootfähigen Datenträger für Notfälle zu erstellen (siehe SYS.1.1.M38 Einbindung in die Notfallplanung). Für Clients mit besonderen Anforderungen an die Verfügbarkeit kann es sinnvoll sein, weitere Maßnahmen zu ergreifen, beispielsweise ein Austauschsystem bereit zu halten.

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Allgemeiner Client" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

SYS.2.1.M1 Benutzerauthentisierung

Die Identifikations- und Authentikationsmechanismen von IT-Systemen bzw. IT-Anwendungen müssen so gestaltet sein, dass Benutzer eindeutig identifiziert und authentisiert werden. Die Identifikation und Authentisierung muss vor jeder anderen Interaktion zwischen IT-System und Benutzer erfolgen. Weitere Interaktionen dürfen nur möglich sein, nachdem die Benutzer sich erfolgreiche identifiziert und authentisiert haben. Die Authentisierungsinformationen müssen so gespeichert sein, dass nur autorisierte Benutzer darauf Zugriff haben (sie prüfen oder ändern können). Bei jeder Interaktion muss das IT-System die Identität des Benutzers feststellen können.

Es gibt verschiedene Techniken, über die die Authentizität eines Benutzers nachgewiesen werden kann. Die bekanntesten sind:

- PINs (Persönliche Identifikationsnummern),
- Passwörter,
- Token wie z. B. Zugangskarten sowie
- Biometrie.

Für sicherheitskritische Anwendungsbereiche sollte starke Authentisierung verwendet werden, hierbei werden zwei oder mehr Authentisierungstechniken kombiniert, wie Passwort plus Transaktionsnummern (Einmalpasswörter) oder plus Chipkarte. Daher wird dies auch häufig als Zwei-Faktor-Authentisierung bzw. Mehr-Faktor-Authentisierung bezeichnet. Alle eingesetzten Authentisierungstechniken müssen sich auf dem Stand der Technik befinden.

Passwörter

Werden in einem Client Passwörter zur Authentisierung verwendet, so ist die Sicherheit der Zugangs- und Zugriffsrechteverwaltung des IT-Systems entscheidend davon abhängig, dass die Passwörter korrekt gebraucht werden. Dafür sollte eine Richtlinie zum Passwortgebrauch erstellt und veröffentlicht werden. Außerdem sollten die IT-Benutzer regelmäßig, z.B. bei Team-Meetings, darauf hingewiesen werden.

Wenn Passwörter zur Authentikation eingesetzt werden, sollte das IT-System Mechanismen bieten, die folgende Bedingungen erfüllen:

- Es wird gewährleistet, dass jeder Benutzer individuelle Passwörter benutzt (und diese auch selbst auswählen kann).
- Es wird überprüft, dass alle Passwörter den definierten Vorgaben genügen (z. B. Mindestlänge, keine Trivialpasswörter). Die Prüfung der Passwortgüte sollte individuell regelbar sein. Beispielsweise sollten vorgegeben werden können, dass die Passwörter mindestens ein Sonderzeichen enthalten müssen oder bestimmte Zeichenkombinationen verboten werden.
- Das IT-System generiert Passwörter, die den definierten Vorgaben genügen. Das IT-System muss die so erzeugten Passwörter dem Benutzer anbieten.
- Der Passwortwechsel sollte von den IT-Systemen regelmäßig initiiert werden. Die Lebensdauer eines Passwortes sollte einstellbar sein.
- Die Wiederholung alter Passwörter beim Passwortwechsel sollte vom IT-System verhindert werden (Passwort-Historie).
- Bei der Eingabe sollte das Passwort nicht auf dem Bildschirm angezeigt werden.
- Nach der Installation bzw. der Neueinrichtung von Benutzern sollte das Passwort-System einen Passwort-Wechsel nach der Erst-Anmeldung erzwingen.

Vertiefende Informationen zur Authentisierung sind in ORP.4 Identitäts- und Berechtigungsmanagement zu finden.

SYS.2.1.M2 Rollentrennung

Grundsätzlich kann zwischen Kennungen für Benutzer- und Administratoren unterschieden werden. Nur Administratoren verwalten die IT-Systeme, während normale Benutzerkennungen nur die Rechte besitzen, um ihre arbeitsplatzspezifischen Aufgaben erfüllen zu können. Normale Benutzerkennungen dürfen keine Administrationsrechte besitzen, damit das Betriebssystem und die Konfiguration der Clients vor versehentlicher, fahrlässiger oder vorsätzlicher Modifikation durch die Benutzer geschützt werden.

Falls Benutzer nur bestimmte administrative Aufgaben wahrnehmen müssen, ist es oftmals nicht erforderlich, ihnen alle mit einem eigenen Login verbundenen Rechte oder sogar Systemadministrator-Rechte zu geben. Beispiele sind bestimmte Tätigkeiten der routinemäßigen Systemverwaltung, wie die Erstellung von Backups oder das Einrichten eines neuen Benutzers, die mit einem Programm menügesteuert durchgeführt werden, oder Tätigkeiten, für die ein Benutzer nur ein einzelnes Anwendungsprogramm benötigt. Insbesondere bei Aushilfskräften und externen Dienstleistern muss darauf geachtet werden, dass diese nur die Dienste verwenden und nur auf die Daten zugreifen dürfen, die sie tatsächlich benötigen. Wenn ihre Tätigkeit beendet ist, sind deren Accounts zu deaktivieren und alle Zugangsberechtigungen zu entfernen.

Wenn möglich, sollte für die Benutzer eine eingeschränkte Benutzerumgebung geschaffen werden. Sie kann zum Beispiel unter Unix durch eine Restricted Shell (rsh) und eine Beschränkung der Zugriffspfade mit dem Unix-Kommando chroot realisiert werden. Eine weitere Möglichkeit besteht darin, einzelne Anwendungsprogramme, wie Web-Browser, im sogenannten Kiosk-Modus auszuführen, so dass nur ein beschränkter Zugriff besteht.

Werden an Benutzerkennungen besonders weitgehende Rechte vergeben, so sollte dies möglichst restriktiv erfolgen. Hierbei sollte zum einem der Kreis der privilegierten Benutzer möglichst eingeschränkt werden und zum anderen nur die für die Durchführung der Arbeit benötigten Rechte vergeben werden. Für alle Aufgaben, die ohne erweiterte Rechte durchgeführt werden können, sollten auch privilegierte Benutzer unter Kennungen mit Standard-Rechten arbeiten.

SYS.2.1.M3 Aktivieren von Autoupdate-Mechanismen

Viele Produkte verfügen über automatische Update-Mechanismen (Autoupdate), die die Anwender darüber informieren, wenn Patches oder Updates vorhanden sind. Häufig bieten diese auch die Option, die Updates sofort über das Internet herunterzuladen und zu installieren. Generell müssen die vorhandenen Autoupdate-Mechanismen aktiviert werden, sofern nicht andere Mechanismen wie regelmäßige manuelle Wartung oder ein zentrales Softwareverteilungssystem für Updates eingesetzt werden. In der Regel enthalten heute alle Betriebssysteme und verfügbaren Standardsoftwarepakete solche Mechanismen. Die Funktionsweise des Update-Mechanismus ist je nach Version, Installationsmodus und Hersteller unterschiedlich ausgeprägt.

Ein Software-Update-Mechanismus sollte die folgenden Anforderungen erfüllen:

- Die lokalen Update-Clients müssen die Authentizität des Update-Servers prüfen.
- Updateinformationen sowie die Updates selbst dürfen durch die lokalen Update-Clients vom Update-Server nur verschlüsselt abgerufen werden.
- Die lokalen Update-Clients müssen vor der Durchführung eines Updates die vom Update-Server erhaltenen Daten auf deren Integrität prüfen, z. B. mittels Zertifikaten.
- Der Updatevorgang sollte von den lokalen Update-Clients so protokolliert werden, dass die sicherheitskritischen Aktionen nachvollzogen und die Protokolle zentral verarbeitet werden können.
- Updates sollten die Konfigurationen der zu aktualisierenden Software grundsätzlich nicht ändern, falls (z. B. aus Sicherheitsgründen) dennoch erforderlich, aber darauf in geeigneter Weise darauf hinweisen.
- Updates sollten rückgängig gemacht werden können und so den vor dem Update verwendeten Zustand der Software wiederherstellen (z. B. im Fall von Kompatibilitätsproblemen).
- Die Software sollte von den lokalen Update-Clients auch ohne eine Verbindung zum Internet aktualisiert werden können.
- Es sollte möglich sein, einen Update-Server innerhalb des eigenen Datennetzes betreiben zu können und so Update-Clients zentral zu verwalten und Updates zu verteilen.
- Die lokalen Update-Clients sollten mit den geringsten für das jeweilige Update erforderlichen Rechten betrieben werden können.
- Die lokalen Update-Clients sollte eine Möglichkeit anbieten, automatisch auf verfügbare Updates zu prüfen.
- Das Updateverhalten der lokalen Update-Clients sollte konfigurierbar sein (u. A. Zeitpunkte zur Prüfung und Durchführung von Updates).

Üblicherweise suchen IT-Produkte mit Autoupdate bei jedem Start der IT-Systeme oder bei jeder Einwahl in das Internet auf einem öffentlichen Updateserver nach neuen Versionen oder Softwarepaketen. Produkte bieten verschiedene Möglichkeiten, den Autoupdate-Mechanismus zu konfigurieren. Wenn neue IT-Komponenten in Betrieb genommen werden, sollte immer auch überprüft werden, ob und welche Update-Mechanismen diese haben und wie diese konfiguriert werden können. Dabei sollten auch kontrolliert werden, welche Daten vom Autoupdate-Mechanismus zum Hersteller übertragen werden. Es sollte zunächst grundsätzlich geklärt werden, wie mit diesen Mechanismen umgegangen wird. Danach sollte festgelegt werden, wie die Update-Funktionen konkret in den verschiedenen Produkten konfiguriert werden. Im Folgenden wird ein Überblick über verschiedene Varianten dieser Mechanismen gegeben.

Das komplette Deaktivieren wird nicht von jeder Software angeboten. Falls die Institution die unkontrollierte Kommunikation von IT-Komponenten mit der Außenwelt unterbinden will, müssen hierfür Paketfilter eingesetzt werden.

Wird eine Abfrage von einem öffentlichen Update-Server nicht gewünscht, lassen sich viele Softwareprodukte auf andere Internet-Adressen als die des Herstellers, beispielsweise interne, umlenken.

Einige Hersteller bieten Software für den Eigenbetrieb von Update-Servern oder Update-Spiegelservern an, dabei wird der Update-Server in der Institution lokal installiert (z. B. Windows Server Update Services WSUS). Der Update-Server kommuniziert dann direkt mit dem Hersteller und lädt die gewünschten Aktualisierungen direkt vom Hersteller. Der Vorteil dieser Lösung ist, dass die von der Aktualisierung betroffenen IT-Systeme einer Institution nicht selber mit dem Update-Server des Herstellers kommunizieren müssen, sondern nur mit dem lokal installierten. Dadurch kann der Datenverkehr nach Außen auf ein Mindestmaß reduziert werden. Bei vielen Produkten für Update-Servern lassen sich die gewünschten Einstellungen komfortabel über eine grafische Benutzeroberfläche (GUI) vornehmen. Allerdings gibt es auch Produkte, bei denen die notwendigen Einstellungen, um lokale Update-Server zu verwenden oder die Abfrage von einem öffentlichen Updateserver zu unterbinden, verborgen oder nur per Paketfilter bzw. Firewall zu unterbinden sind.

Falls öffentliche Update-Server genutzt werden sollen, so ist zunächst die Authentizität des Update-Servers zu prüfen. Außerdem sollte untersucht werden, ob Zeitintervalle oder Ereignisse zur Steuerung der Update-Abfrageaktion eingestellt werden können. Die Einstellungen müssen dann entsprechend der festgelegten Änderungsstrategie vorgenommen werden.

Es sollte geprüft werden, wie die Kommunikation mit Update-Servern auf das geringst mögliche Maß beschränkt werden kann. Außerdem muss entschieden werden, ob die direkte Kommunikation mit dem Hersteller als einzige Alternative oder parallel zur internen Kommunikation (Parallelkonfiguration) betrieben werden soll.

Eine Parallelkonfiguration ist häufig sinnvoll für mobile Nutzer, die nicht immer innerhalb des Behörden- oder Unternehmensnetzes kommunizieren. Bei mobilen IT-Systemen kann es beispielsweise wichtiger sein, unterwegs einen aktuellen Patch einzuspielen, wenn dieser eine gefährliche Sicherheitslücke schließt, als auf die Freigabe vom Änderungsmanagement zu warten. Es kann jedoch auch gewünscht werden, dass sämtliche Software-Änderungen ausschließlich durch die interne freigegebene Softwareverteilung erfolgen.

Bei Autoupdate-Mechanismen ist unter anderem noch zu beachten, ob die Änderungen vom Hersteller nur auf ein internes IT-System geladen werden und die Installation der Änderung danach dem Benutzer überlassen wird, oder ob diese nach dem Herunterladen sofort automatisch installiert werden.

Außerdem muss festgelegt werden, wie damit umgegangen werden soll, wenn durch ein Update das IT-System neu gestartet werden muss. Es kann entschieden werden, das IT-System sofort neu zu starten, es kann aber auch oft festgelegt werden, dass derartige Updates erst installiert werden, wenn das IT-System sowieso planmäßig runter gefahren wird.

SYS.2.1.M4 Regelmäßige Datensicherung

Zur Vermeidung von Datenverlusten müssen regelmäßige Datensicherungen durchgeführt werden. In den meisten Clients können diese weitgehend automatisiert erfolgen. Es sind Regelungen zu treffen, welche Daten von wem wann gesichert werden.

Es müssen mindestens die Daten regelmäßig gesichert werden, die nicht aus anderen Informationen abgeleitet werden können.

Es wird empfohlen, ein Datensicherungskonzept zu erstellen, hierfür sollten die Anforderungen des Baustein OPS.1.1.5 Datensicherung berücksichtigt werden

Hinweis: Auch wenn Benutzer alle Arbeitsergebnisse auf zentralen Servern speichern sollen, werden sich immer wieder geschäftsrelevante Daten auf Clients finden, solange diese eine Möglichkeit dafür bieten. Daher müssen auch Clients in das Datensicherungskonzept der Institution einbezogen werden.

Abhängig von der Menge und Wichtigkeit der laufend neu gespeicherten Daten und vom möglichen Schaden bei Verlust dieser Daten ist folgendes festzulegen:

- Zeitintervall
  Beispiele: täglich, wöchentlich, monatlich
- Zeitpunkt
  Beispiele: nachts, freitags abends
- Anzahl der aufzubewahrenden Generationen
  Beispiel: Bei täglicher Komplettsicherung werden die letzten sieben Sicherungen aufbewahrt, außerdem die Freitag-Abend-Sicherungen der letzten zwei Monate.
- Umfang der zu sichernden Daten
  Am einfachsten ist es, Partitionen bzw. Verzeichnisse festzulegen, die bei der regelmäßigen Datensicherung berücksichtigt werden. Eine geeignete Differenzierung kann die Übersichtlichkeit vergrößern sowie Aufwand und Kosten sparen helfen.Beispiel: selbst erstellte Dateien und individuelle Konfigurationsdateien
- Speichermedien (abhängig von der Datenmenge)
  Beispiele: Bänder, DVDs oder Blu-rays, Festplatten, USB-Sticks
- Vorherige Löschung der Datenträger vor Wiederverwendung (z. B. bei Bändern oder Kassetten)
- Zuständigkeit für die Durchführung (Administrator, Benutzer)
- Zuständigkeit für die Überwachung der Sicherung, insbesondere bei automatischer Durchführung (Fehlermeldungen, verbleibender Platz auf den Speichermedien)
- Dokumentation der erstellten Sicherungen (Datum, Art der Durchführung der Sicherung sowie gewählte Parameter, Beschriftung der Datenträger)

Wegen des großen Aufwands können Komplettsicherungen in der Regel höchstens einmal täglich durchgeführt werden. Die seit der letzten Sicherung erstellten Daten können nicht wieder eingespielt werden. Daher und zur Senkung der Kosten sollten zwischen den Komplettsicherungen regelmäßig differentielle oder inkrementelle Sicherungen durchgeführt werden. Hinweise zu den verschiedenen Arten von Datensicherungen finden sich in den Umsetzungshinweisen des Bausteins OPS.1.1.5 Datensicherung.

Eine differentielle oder inkrementelle Sicherung kann häufiger erfolgen, zum Beispiel sofort nach Erstellung wichtiger Dateien oder mehrmals täglich. Die Vereinbarkeit mit dem laufenden Betrieb ist sicherzustellen.

Für eingesetzte Software ist separat zu entscheiden, ob sie von der regelmäßigen Datensicherung erfasst werden muss. Dies hängt beispielsweise davon ab, wie aufwendig es, den Client neu zu installieren und Patches und Updates einzuspielen. Unter Umständen ist es ausreichend, Sicherungskopien von den Originaldatenträgern anzufertigen.

Es muss regelmäßig getestet werden, ob die Datensicherung auch wie gewünscht funktioniert, vor allem, ob gesicherte Daten problemlos zurückgespielt werden können.

Alle Benutzer sollten über die Regelungen zur Datensicherung informiert sein, um gegebenenfalls auf Unzulänglichkeiten (zum Beispiel zu geringes Zeitintervall für ihren Bedarf) hinweisen oder individuelle Ergänzungen vornehmen zu können (zum Beispiel zwischenzeitliche Spiegelung wichtiger Daten auf der eigenen Platte). Auch die Information der Benutzer darüber, wie lange die Daten wiedereinspielbar sind, ist wichtig. Werden zum Beispiel bei wöchentlicher Komplettsicherung nur zwei Generationen aufbewahrt, bleiben in Abhängigkeit vom Zeitpunkt des Verlustes nur zwei bis drei Wochen Zeit, um die Wiedereinspielung vorzunehmen.

Falls bei vernetzten Clients nur die Netzfreigaben gesichert werden, ist sicherzustellen, dass die zu sichernden Daten regelmäßig von den Benutzern oder automatisch dorthin überspielt werden, besser ist es, wenn alle Daten ausschließlich auf den Netzlaufwerken abgelegt werden. Bei größeren Änderungen an IT-Systemen oder des Informationsverbunds muss der Datensicherungsprozess entsprechend angepasst werden.

Vertrauliche Daten sollten vor der Sicherung möglichst verschlüsselt werden, dabei müssen die Daten auch nach einem längeren Zeitraum entschlüsselt werden können (siehe CON.1 Kryptokonzept).

Der Ausdruck von Daten auf Papier ist keine angemessene Art der Datensicherung.

SYS.2.1.M5 Bildschirmsperre [Benutzer]

Unter einer Bildschirmsperre wird die Möglichkeit verstanden, die auf dem Bildschirm aktuell gezeigten Informationen zu verbergen sowie den Rechner vor unbefugtem Zugriff zu schützen. Eine Bildschirmsperre muss nur durch eine erfolgreiche Benutzerauthentikation, also z. B. eine Passwortabfrage, deaktiviert werden können, damit bei einer kürzeren Abwesenheit des IT-Benutzers ein Zugriffsschutz für das IT-System gewährleistet wird.

Die Bildschirmsperre sollte sich sowohl manuell vom Benutzer aktivieren lassen, als auch nach einem vorgegebenen Inaktivitäts-Zeitraum automatisch gestartet werden. Alle Benutzer sollten dafür sensibilisiert sein, dass sie die Bildschirmsperre aktivieren, wenn sie den Arbeitsplatz für eine kurze Zeit verlassen. Bei längeren Abwesenheiten sollten Benutzer sich abmelden.

Der Zeitraum, nach dem sich eine Bildschirmsperre wegen fehlender Benutzereingaben aktiviert, sollte gewisse Grenzen weder unter- noch überschreiten. Der Zeitraum sollte nicht zu knapp gewählt werden, damit die Bildschirmsperre nicht bereits nach kurzen Denkpausen anspringt. Dieser Zeitraum darf aber auf keinen Fall zu lang sein, damit die Abwesenheit des Benutzers nicht von Dritten ausgenutzt werden kann. Eine sinnvolle Vorgabe ist eine Zeitspanne von 15 Minuten. Es sollten Vorgaben für die Einstellung der Wartezeit gemacht werden, die die Sicherheitsanforderungen der jeweiligen IT-Systeme und deren Einsatzumgebung berücksichtigen.

Fast alle Betriebssysteme enthalten Bildschirmsperren. Bei deren Nutzung muss darauf geachtet werden, die Passwortabfrage zu aktivieren.

SYS.2.1.M6 Einsatz von Viren-Schutzprogrammen

Zum Schutz vor Schadprogrammen können unterschiedliche Wirkprinzipien genutzt werden. Programme, die IT-Systeme nach sämtlichen bekannten Schadprogrammen durchsuchen, haben sich in der Vergangenheit als mögliches Mittel in der Schadprogramm-Prävention erwiesen. Entsprechend der in OPS1.1.4 Schutz vor Schadprogrammen beschriebenen Anforderungen sollten daher Viren-Schutzprogramme eingesetzt werden.

Regelmäßige Untersuchung des gesamten Datenbestands

Auch wenn das Viren-Schutzprogramm bei jedem Dateizugriff eine Prüfung auf Schadprogramme durchführt, ist eine regelmäßige Untersuchung aller Dateien auf Clients und Datei-Servern sinnvoll. So können auch Schadprogramme gefunden werden, für die es noch keine Erkennungssignatur gab, als sie gespeichert wurden. In derartigen Fällen muss beispielsweise untersucht werden, ob das Schadprogramm vor seiner Entdeckung bereits vertrauliche Daten gesammelt, Schutzfunktionen deaktiviert oder Code aus dem Internet nachgeladen hat.

Aus Performance-Gründen sollte eine vollständige Prüfung des Datenbestands in Zeiten durchgeführt werden, in denen die IT-Ressourcen nicht stark beansprucht werden. Ideal ist es, wenn die Software die Auslastung des Clients überwacht und dessen "Arbeitspausen" automatisch für die Überprüfung nutzt. Auf den Clients könnte das Viren-Schutzprogramm z. B. auch mit dem Start des Bildschirmschoners gekoppelt werden. Auch bei starker Auslastung empfiehlt es sich, regelmäßig eine vollständige Prüfung des Datenbestands durchzuführen.

Datenaustausch und Datenübertragung

Daten, die versendet werden sollen, müssen unmittelbar vor dem Versand auf Schadprogramme geprüft werden. Analog müssen empfangene Daten unmittelbar nach dem Empfang auf Schadprogramme geprüft werden. Diese Überprüfungen sind sowohl beim Zugriff auf Datenträger als auch bei der Datenübertragung über Kommunikationsverbindungen erforderlich. Die Überprüfungen sollten so weit wie möglich automatisiert werden.

Erkennung von Schadprogrammen auch in komprimierten Dateien

Das Viren-Schutzprogramm sollte Schadprogramme auch in komprimierten Dateien finden, wobei alle gängigen Komprimierungsfunktionen und Archivformate unterstützt werden sollten. Schadprogramme in geschachtelten Archivdateien sollten ebenfalls gefunden werden.

Schutz vor unerlaubter Deaktivierung oder Änderung

Die Viren-Schutzprogramme auf den Clients und Endgeräten müssen so konfiguriert sein, dass die Benutzer keine sicherheitsrelevanten Änderungen an den Einstellungen der Viren-Schutzprogramme vornehmen können. Insbesondere muss sichergestellt sein, dass die Benutzer die Viren-Schutzprogramme nicht deaktivieren können.

SYS.2.1.M7 Protokollierung

Die am Client mögliche Protokollierung ist in einem sinnvollen Umfang zu aktivieren. In regelmäßigen Abständen muss der IT-Betrieb die Protokolldateien der Clients überprüfen. Es sollten alle sicherheitsrelevanten Ereignisse protokolliert werden. Dabei sind insbesondere folgende Vorkommnisse von Interesse:

- falsche Passworteingabe für eine Benutzer-Kennung bis hin zur Sperrung der Benutzer-Kennung bei Erreichen der Fehlversuchsgrenze,
- Versuche von unberechtigten Zugriffen,
- Daten, aus denen die Netzauslastung und -überlastung ermittelt werden kann.

Wie viele Ereignisse darüber hinaus protokolliert werden, hängt unter anderem vom Schutzbedarf der jeweiligen IT-Systeme ab. Je höher deren Schutzbedarf ist, desto mehr sollte protokolliert werden.

Da die Protokoll-Dateien mit der Zeit sehr umfangreich werden können, sollten die Auswertungsintervalle so kurz gewählt werden, dass eine sinnvolle Auswertung möglich ist. Um eine sinnvolle Auswertung zu ermöglichen, sollte jeder Protokoll-Eintrag Benutzer-Kennung bzw. Prozessnummer, Kennzeichnung des Endgeräts, Datum und Uhrzeit enthalten.

Es ist zu prüfen, welche gesetzlichen oder vertraglichen Aufbewahrungsfristen für Protokoll-Dateien beachtet werden müssen. Damit Aktionen lange Zeit nachvollzogen werden können, kann eine Mindestspeicherdauer vorgeschrieben sein, aus Datenschutzgründen kann es auch eine Löschungspflicht geben.

Gerade bei einer Vielzahl von Clients sollten die Protokolldaten zentral zusammengeführt und ausgewertet werden. Hierfür wird empfohlen, einen zentralen Protokollierungsserver einzusetzen, siehe OPS.1.1.6 Protokollierung.

SYS.2.1.M8 Absicherung des Boot-Vorgangs

Wenn von Wechselmedien gebootet oder Fremdsoftware installiert wird, können nicht nur Sicherheitseinstellungen umgangen werden, sondern das IT-System kann auch mit Schadprogrammen infiziert werden. Zusätzlich können Schadprogramme auch in den Bootvorgang eingreifen. Diesen Gefahren sollten die Verantwortlichen durch geeignete organisatorische oderund technische Sicherheitsmaßnahmen entgegenwirken. Hierfür bieten sich verschiedene Vorgehensweisen an, die konkret in den Umsetzungshinweisen des Bausteins SYS.3.4 Mobile Datenträger beschrieben sind:

- Ausbau von Laufwerken
- Verschluss von Laufwerken
- Deaktivierung von Laufwerken im BIOS bzw. Betriebssystem
- Kontrolle der Schnittstellennutzung
- Verschlüsselung (ausschließlicher Zugriff auf verschlüsselte Datenträger)
- Richtlinien für die Nutzung

Unabhängig davon, für welche Vorgehensweise sich die Institution entscheidet, ist zu verhindern, dass Inhalte von mobilen Datenträgern automatisch ausgeführt werden, wenn diese angeschlossen werden. Hierzu sind die entsprechenden Autorun- und Autoplay-Funktionen des Betriebssystems zu deaktivieren.

Um den Bootvorgang kryptographisch abzusichern, sollten bei Systemen mit UEFI-Firmware die Option SecureBoot aktiviert und die Schlüsseldatenbanken gemäß den Vorgaben der Institution konfiguriert werden. Es sollte mindestens überprüft und dokumentiert werden, welchen Schlüsseln vertraut wird. Diese Konfiguration sollte so gesichert werden, dass sie nicht abgeschaltet werden kann. Der Zugriff auf die Konfigurationsoberfläche der Firmware sollte mindestens mit Passwort gesichert sein.

Damit die Sicherheitsmaßnahmen akzeptiert und beachtet werden, müssen die Benutzer über die Gefährdung informiert und sensibilisiert werden.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Allgemeiner Client".

SYS.2.1.M9 Festlegung einer Sicherheitsrichtlinie für Clients

Die Sicherheitsvorgaben für alle Clients ergeben sich aus der institutionsweiten Sicherheitsrichtlinie. Ausgehend von der allgemeinen Richtlinie müssen die Anforderungen für den gegebenen Kontext konkretisiert werden und in einer Sicherheitsrichtlinie für die jeweilige Gruppe von Clients zusammengefasst werden. In diesem Zusammenhang ist zu prüfen, ob neben der institutionsweiten Sicherheitsleitlinie weitere übergeordnete Vorgaben wie IT-Richtlinien, Passwortrichtlinien oder Vorgaben zur Internet-Nutzung zu berücksichtigen sind.

Die Sicherheitsrichtlinie muss allen Anwendern und anderen Personen, die an der Beschaffung und dem Betrieb der Clients beteiligt sind, bekannt sein und Grundlage für deren Arbeit sein. Wie bei allen Richtlinien sind ihre Inhalte und ihre Umsetzung im Rahmen einer übergeordneten Revision regelmäßig zu prüfen.

Die Sicherheitsrichtlinie sollte das generell zu erreichende Sicherheitsniveau spezifizieren und grundlegende Festlegungen treffen. Um die Übersichtlichkeit zu verbessern, kann es sinnvoll sein, für verschiedene Einsatzgebiete gesonderte Sicherheitsrichtlinien zu entwickeln.

Als erstes sollte die allgemeine Konfigurations- und Administrationsstrategie ("Liberal" oder "Restriktiv") festgelegt werden, da die weiteren Entscheidungen von dieser Festlegung wesentlich abhängen.

Für Clients mit normalem Schutzbedarf kann eine relativ liberale Strategie gewählt werden, was in vielen Fällen die Konfiguration und Administration vereinfacht. Generell ist es aber auch in diesen Fällen empfehlenswert, die Strategie nur "so liberal wie nötig" auszulegen.

Bei Clients mit einem hohen Schutzbedarf wird grundsätzlich eine restriktive Strategie empfohlen. Für Clients mit höherem Schutzbedarf bezüglich eines der drei Grundwerte sollte unbedingt eine restriktive Konfigurations- und Administrationsstrategie umgesetzt werden.

Nachfolgend sind einige Punkte aufgeführt, die berücksichtigt werden sollten:

- Regelungen für die Arbeit der Benutzer der Clients:
  - Soll ein Client nur von jeweils einem einzelnen Benutzer genutzt werden, oder ist ein Betrieb mit wechselnden Benutzern vorgesehen?
  - Dürfen Benutzer bestimmte Konfigurationseinstellungen selbst ändern (beispielsweise Bildschirmhintergrund, Bildschirmschoner oder ähnliches) oder werden alle Einstellungen zentral vorgegeben?
  - Dürfen Benutzer auf bestimmte Bereiche der IT-Systeme keinen Zugriff haben? Diese Vorgaben haben in der Regel sowohl Auswirkungen auf die Rechtevergabe im IT-System selbst als auch auf die Vorgaben für die Installation und Grundkonfiguration.
  - Welche Informationen dürfen die Benutzer lokal auf den Clients abspeichern? Generell sollten alle geschäftsrelevanten Informationen zentral auf einem Server abgelegt werden, auf dem sie regelmäßig gesichert werden. Andernfalls muss dafür gesorgt werden, dass alle Informationen der Benutzer, die lokal auf den Clients abgespeichert sind, im Datensicherungskonzept des Clients berücksichtigt werden.
  - Sind die Benutzer gehalten, den Client abends herunterzufahren und auszuschalten, oder muss er rund um die Uhr in Betrieb sein?Für das Ausschalten von Clients bei Arbeitsschluss sprechen beispielsweise Brandschutz und Stromersparnis. Darüber hinaus sind etwa Festplatten, die in Clients eingesetzt werden, meist nicht für einen Dauerbetrieb geeignet. Ein durchgehender Betrieb der Clients kann dennoch erwünscht sein, beispielsweise wenn über Nacht automatische Datensicherungen erstellt werden.
- Regelungen für die Arbeit des IT-Betriebs und Revisoren:
  - Nach welchem Schema werden Administrationsrechte vergeben? Welcher Administrator darf welche Rechte ausüben und wie erlangt er diese Rechte?
  - Über welche Zugangswege dürfen Administratoren und Revisoren auf die IT-Systeme zugreifen?
  - Welche Vorgänge und Ereignisse müssen dokumentiert werden? In welcher Form wird die Dokumentation erstellt und gepflegt?
  - Gilt für bestimmte Änderungen ein Vier-Augen-Prinzip?
- Vorgaben für die Installation und Grundkonfiguration:
  - Welche Installationsmedien werden zur Installation verwendet?
  - Soll ein zentraler Authentisierungsdienst genutzt werden oder erfolgt die Benutzerverwaltung und -authentisierung nur lokal?
- Regelungen zur Benutzer- und Rollenverwaltung, Berechtigungsstrukturen (Ablauf und Methoden der Authentisierung und Autorisierung, Berechtigung zu Installation, Update, Konfigurationsänderungen etc.). Nach Möglichkeit sollte ein Rollenkonzept für die Administration erarbeitet werden. Es dürfen keine Sammelkennungen, die verschiedene Benutzer mit derselben Kennung nutzen, verwendet werden.
  - Falls bei der Planung für die Clients festgelegt wurde, dass Teile des Dateisystems verschlüsselt werden sollen, so sollte an dieser Stelle festgelegt werden, wie dies zu geschehen hat (siehe auch SYS.2.1.M25 Verschlüsselung der Clients).
  - Beim Einsatz verschlüsselter Dateisysteme sollte hierfür ein eigenes Konzept erstellt und die Details der Konfiguration besonders sorgfältig dokumentiert werden, da im Fall von Problemen (Verlust des Schlüssels oder der Passphrase zum Schlüssel, inkorrekte Konfiguration oder ähnliches) die Daten auf den verschlüsselten Dateisystemen sonst vollständig verloren sein können.
  - Regelungen zu Erstellung und Pflege von Dokumentation
- Vorgaben für den sicheren Betrieb:
  - Welcher Benutzerkreis darf sich auf den IT-Systemen anmelden?
  - Wie können sich die Benutzer gegenüber dem IT-System authentisieren? Generell sollte auf eine automatische Anmeldung, bei der die Benutzer ohne eine aktive Authentisierung beim Hochfahren des Clients angemeldet werden, verzichtet werden.
  - Erhalten Benutzer Zugriff auf ein oder mehrere LANs oder das Internet? Welche Protokolle dürfen verwendet werden? Bei Clients, die als Arbeitsplatzrechner in einer Institution genutzt werden, ist es in der Regel nicht notwendig und oft auch nicht wünschenswert, dass normale Benutzer über das Netz auf einen anderen Arbeitsplatzrechner zugreifen.
  - Auf welche Ressourcen dürfen die Benutzer zugreifen?
  - Es müssen Vorgaben für die Passwortnutzung erstellt werden (Passwortregeln, Regeln und Situationen für Passwortänderungen, gegebenenfalls Hinterlegung von Passwörtern).
  - Wie wird der Startvorgang des IT-Systems ("Booten") gegen Manipulation abgesichert? Nur Administratoren sollten die Clients von Laufwerken oder externen Speichermedien boo-

Anhand der oben genannten Punkte kann eine Checkliste erstellt werden, die bei Audits oder Revisionen hilfreich sein kann.

Die Verantwortung für die Sicherheitsrichtlinie liegt beim Sicherheitsmanagement. Änderungen und Abweichungen hiervon dürfen nur in Abstimmung mit dem Sicherheitsmanagement erfolgen.

Bei der Erstellung einer Sicherheitsrichtlinie ist es empfehlenswert, so vorzugehen, dass zunächst ein Maximum an Forderungen und Vorgaben für die Sicherheit der IT-Systeme aufgestellt wird. Diese können anschließend den tatsächlichen Gegebenheiten angepasst werden. Idealerweise wird so erreicht, dass alle notwendigen Aspekte berücksichtigt werden. Für jede im zweiten Schritt verworfene oder abgeschwächte Vorgabe sollte der Grund für die Nicht-Berücksichtigung dokumentiert werden.

In Bezug auf Regelungen für die Benutzer sollte jedoch beachtet werden, dass diese nur so weit sinnvoll sind, wie sie im normalen Arbeitsalltag anwendbar sind, aber auch wie sie überwacht und durchgesetzt werden können. Beispielsweise ist es bei Zugriffsbeschränkungen nicht zielführend, den Benutzern nur in der Sicherheitsrichtlinie den Zugriff auf bestimmte Verzeichnisse zu verbieten, diese aber nicht auch durch eine entsprechende Rechtevergabe tatsächlich vor dem Zugriff zu schützen. Zugriffsbeschränkungen, die bei der Erstellung der Sicherheitsrichtlinie festgelegt wurden, sollten daher immer so weit wie möglich über entsprechende Vorgaben für die Installation und Konfiguration der Clients umgesetzt werden.

Während die Sicherheitsrichtlinie für Clients formuliert wird, ist es auch wichtig, eine Balance zwischen Sicherheit (indem die Funktionalität eingeschränkt und Benutzerrechte restriktiv vergeben werden) und Benutzerfreundlichkeit zu finden. Werden die Benutzer durch Regelungen, die für sie nicht transparent sind und die eventuell sogar als Schikane empfunden werden, zu sehr eingeschränkt, so kann sie dies im Gegenzug dazu verleiten, diese Beschränkungen mit besonderer Kreativität zu umgehen.

Dies unterscheidet die Sicherheitsrichtlinie für Clients von den entsprechenden Richtlinien etwa für Server oder aktive Netzkomponenten, bei denen in der Regel nur technisch versierte Anwender und Administratoren angesprochen sind, denen viele Einschränkungen eher plausibel gemacht werden können.

SYS.2.1.M10 Planung des Einsatzes von Clients

Eine grundlegende Voraussetzung dafür, dass Clients sicher betrieben werden können, ist ein angemessenes Maß an Planung im Vorfeld.

Die Planung des Einsatzes kann in mehreren Schritten nach dem Prinzip des Top-Down-Entwurfs erfolgen: Ausgehend von einem Grobkonzept für das Gesamtsystem werden konkrete Planungen für Teilkomponenten in spezifische Teilkonzepten festgelegt. Die Planung betrifft dabei nicht nur Aspekte, die klassischerweise mit dem Begriff Sicherheit verknüpft werden, sondern auch normale betriebliche Aspekte, die Anforderungen im Bereich der Sicherheit nach sich ziehen.

Im Grobkonzept sollten beispielsweise folgende typische Fragestellungen behandelt werden:

- Welche Aufgaben sollen die Clients erfüllen? Auf welche Dienste muss von den Clients zugegriffen werden können? Gibt es besondere Anforderungen an die Verfügbarkeit der IT-Systeme oder an die Vertraulichkeit oder Integrität der gespeicherten oder verarbeiteten Daten?
- Sollen in den IT-Systemen bestimmte Hardware-Komponenten eingesetzt werden? Dies kann beispielsweise für die Auswahl des Betriebssystems wichtig sein.
- Welche Anforderungen an die Hardwareausstattung (CPU, Arbeitsspeicher, Kapazität der Festplatten, Kapazität des Netzes etc.) ergeben sich aus den allgemeinen Anforderungen?
- Handelt es sich bei dem Netz, in dem die Clients eingesetzt werden sollen, um einen homogenen oder heterogenen Rechnerverbund?
- Dienen die Clients als Ersatz für vorhandene IT-Systeme? Sollen von den alten IT-Systemen Datenbestände oder Hardware-Komponenten übernommen werden?
- Sollen auf den Clients weitere Betriebssysteme mittels Multiboot installiert werden?

Es wird empfohlen, ein oder mehrere generische Anforderungsprofile (beispielsweise "Allgemeiner Büro-PC", "Entwicklungsrechner" oder "Administrations-Client") zu erstellen, die bei konkreten Planungen als Grundlage dienen können.

Die folgenden Teilkonzepte sollten bei der Planung berücksichtigt werden:

- Authentisierung und Benutzerverwaltung: Welche Arten der Benutzerverwaltung und Benutzer-Authentisierung sollen genutzt werden? Werden Benutzer nur lokal verwaltet oder soll ein zentrales Verwaltungssystem genutzt werden? Sollen die IT-Systeme auf einen zentralen, netzbasierten Authentisierungsdienst zugreifen oder wird nur eine lokale Authentisierung benötigt?
- Benutzer- und Gruppenkonzept: Ausgehend vom institutionsweiten Benutzer-, Rechte- und Rollenkonzept müssen entsprechende Regelungen für die Clients erstellt werden (siehe ORP.4 Identitäts- und Berechtigungsmanagement).
- Administration: Wie sollen die IT-Systeme administriert werden? Werden alle Einstellungen lokal vorgenommen oder werden die Clients in ein zentrales Administrations- und Konfigurationsmanagement integriert?
- Partitions- und Dateisystem-Layout: In der Planungsphase sollte eine erste Abschätzung des benötigten Festplattenplatzes durchgeführt werden. Zur einfacheren Administration und Wartung ist es empfehlenswert, so weit wie möglich das Betriebssystem (Systemprogramme und -konfiguration), die Anwendungsprogrammen und -daten (beispielsweise Datenbank-Server und Daten) und gegebenenfalls die Benutzerdaten voneinander zu trennen. Verschiedene Betriebssysteme bieten hierfür unterschiedliche Mechanismen an (Aufteilung in Laufwerke unter Windows, Mountpoints unter Unix). Oft kann es sinnvoll sein, bestimmte Daten sogar auf einer eigenen Festplatte oder einem eigenen Festplattensystem zu speichern. Dies erlaubt es beispielsweise, bei einer Neuinstallation oder einem Update des IT-Systems die Daten auf den anderen Partitionen ohne Umkopieren zu übernehmen.

In der Planungsphase sollte die vorgesehene Aufteilung der Partitionen und deren Größe dokumentiert werden.

- Falls auf den Clients Daten mit hohem Schutzbedarf bezüglich der Vertraulichkeit gespeichert werden, so wird der Einsatz verschlüsselter Dateisysteme dringend empfohlen (siehe auch SYS.2.1.M25 Verschlüsselung der Clients). Dabei brauchen nicht notwendigerweise alle Dateisysteme verschlüsselt zu werden, sondern es wird oft ausreichend sein, für den Teil des Dateisystems eine Verschlüsselung vorzusehen, auf dem die Daten selbst gespeichert werden, sowie für den Teil, in dem die Daten zwischengespeichert werden können (Auslagerungsdatei/-partition oder temporäre Verzeichnisse). Es muss bei allen Varianten sichergestellt sein, dass kein Schlüsselmaterial im Klartext gespeichert wird, da dies den Schutz aushebelt. Dies wird durch eine entsprechende Planung des Partitions- und Dateisystemlayouts erleichtert.
- Bei höheren Anforderungen am Schutzbedarf bezüglich der Vertraulichkeit der Daten, die auf den Clients gespeichert sind, kann es erforderlich werden, die IT-Systeme mit einem Verschlüsselungsprogramm auszustatten, das die gesamte Festplatte verschlüsselt und bereits vor dem Start des Betriebssystems eine Benutzer-Authentisierung (beispielsweise über eine Chipkarte) durchführt ("Pre-Boot-Authentication").
- Netzdienste und Netzanbindung: In Abhängigkeit von den Sicherheitsanforderungen der Daten, auf die von den Clients aus zugegriffen werden muss, muss die Netzanbindung der Clients geplant werden.
- Abhängig vom festgelegten Einsatzzweck der Clients wird außerdem eventuell der Zugriff auf weitere Dienste im Netz benötigt. Dies muss bereits im Rahmen der Planung berücksichtigt werden, damit nicht zu einem späteren Zeitpunkt Schwierigkeiten beispielsweise durch zu geringe Übertragungskapazitäten oder Probleme mit zwischengeschalteten Sicherheitsgateways entstehen.
- Monitoring: Falls besondere Anforderungen an die Verfügbarkeit der Clients bestehen, so kann ein Monitoring-System eingesetzt werden. Dafür wird auf einem Server ein Monitoring-Daemon installiert, dem ein lokal auf dem Client installierter Agent die zu überwachenden Daten sendet, beispielsweise zur Systemauslastung oder zum verbleibenden freien Speicherplatz. Bei Problemen kann zum Beispiel automatisch ein Alarm generiert werden (siehe auch SYS.1.1.M26 Systemüberwachung).
- Protokollierung: Auch bei Clients spielt die Protokollierung eine wichtige Rolle, beispielsweise bei der Diagnose und Behebung von Störungen oder bei der Erkennung und Aufklärung von Angriffen. In der Planungsphase sollte entschieden werden, welche Informationen mindestens protokolliert werden sollen, und wie lange die Protokolldaten aufbewahrt werden sollen. Außerdem muss festgelegt werden, ob die Protokolldaten lokal auf den IT-Systemen oder auf einem zentralen Protokollierungsserver im Netz gespeichert werden sollen. Vertiefende Informationen sind in dem Baustein OPS.1.1.6 Protokollierung zu finden
- Sinnvollerweise sollte bereits in der Planungsphase festgelegt werden, wie und zu welchen Zeitpunkten Protokolldaten ausgewertet werden sollen.
- Hochverfügbarkeit: Falls an die Verfügbarkeit der Clients besondere Anforderungen gestellt werden, so sollte bereits in der Planungsphase überlegt werden, wie diese Anforderungen erfüllt werden können.

Alle Entscheidungen, die in der Planungsphase getroffen wurden, müssen so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können. Dabei ist zu beachten, dass meist andere Personen neben dem Autor diese Informationen auswerten müssen. Daher ist auf passende Strukturierung und Verständlichkeit zu achten.

SYS.2.1.M11 Beschaffung von Clients

Für die Beschaffung von Clients, die typischerweise in größeren Mengen erfolgt, müssen ausgehend von den Einsatzszenarien Kriterien für die Auswahl geeigneter Produkte formuliert werden. Werden Clients beschafft, ist es wichtig, dass die IT-Systeme zur vorhandenen Struktur passen, damit nicht für ein einzelnes IT-System wegen dessen Besonderheiten ein unangemessen hoher Aufwand bei Integration und Betrieb entsteht. Vertiefende Informationen sind OPS.1.2.6 Beschaffung, Ausschreibung und Einkauf zu finden.

SYS.2.1.M12 Kompatibilitätsprüfung von Software

Vor einer beabsichtigten Beschaffung von Software sollte deren Kompatibilität zum eingesetzten Betriebssystem in der vorliegenden Konfiguration geprüft und die Kompatibilitätsprüfung in das Freigabeverfahren der Software aufgenommen werden. Ist vom Hersteller der Software oder aus anderen Fachkreisen keine sichere Information zur Kompatibilität vorhanden, so sollte die Kompatibilität in einer Testumgebung geprüft werden. Vor einer beabsichtigten Hardwareänderung oder bei einer Betriebssystemmigration sollte auch die Treibersoftware für alle betreffenden Komponenten auf Kompatibilität zum Betriebssystem gewährleistet werden.

SYS.2.1.M13 Zugriff auf Ausführungsumgebungen mit unbeobachtbarer Codeausführung

Die Nutzung von Ausführungsumgebungen mit unbeobachteter Codeausführung, wie z. B. Intel Software Guard Extensions (SGX), sollte in der Firmware des Clients im (UEFI)-Setupmenü deaktiviert werden. Die Einstellung wird von den verschiedenen Herstellern unterschiedlich benannt. Sie befindet sich zumeist in den Sicherheitseinstellungen.

Es sollte berücksichtigt werden, dass sich die Ausführungsumgebungen mit unbeobachteter Codeausführung teilweise nicht mehr abschalten lassen. Es sollte daher z. B. durch regelmäßiges Patchen sichergestellt sein, dass die dort vorhandenen Schwachstellen zeitnah behoben werden und somit nur das IT-System und der jeweilige Hersteller der Ausführungsumgebung vollen Zugriff auf diese Bereiche haben.

SYS.2.1.M14 Updates und Patches für Firmware, Betriebssystem und Anwendungen

Häufig werden Fehler in Produkten bekannt, die dazu führen können, dass die Informationssicherheit des Informationsverbundes, wo diese betrieben werden, beeinträchtigt wird. Entsprechende Fehler können Hardware, Firmware, Betriebssysteme und Anwendungen betreffen. Diese Schwachstellen müssen so schnell wie möglich behoben werden, damit sie nicht durch interne oder externe Angreifer ausgenutzt werden können. Dies ist ganz besonders wichtig, wenn die betreffenden IT-Systeme mit dem Internet verbunden sind. Die Hersteller von Betriebssystem- oder Software-Komponenten veröffentlichen in der Regel Patches oder Updates, die auf dem jeweiligen IT-System installiert werden müssen, um den oder die Fehler zu beheben.

Die Systemadministratoren sollten sich daher regelmäßig über bekannt gewordene Schwachstellen informieren.

Wichtig ist, dass Patches und Updates, wie jede andere Software, nur aus vertrauenswürdigen Quellen bezogen werden dürfen. Für jedes eingesetzte IT-System oder Softwareprodukt muss bekannt sein, wo Sicherheitsupdates und Patches erhältlich sind. Außerdem ist es wichtig, dass Integrität und Authentizität der bereits installierten Produkte oder der einzuspielenden Sicherheitsupdates und Patches überprüft werden (siehe Abschnitt "Verwendung von vertrauenswürdigen Installationsmedien"), bevor ein Update oder Patch installiert wird. Vor der Installation sollten sie außerdem mit Hilfe eines Computer-Virenschutzprogramms geprüft werden. Dies sollte auch bei solchen Paketen gemacht werden, deren Integrität und Authentizität verifiziert wurde.

Sicherheitsupdates oder Patches sollten schnell, jedoch nicht voreilig eingespielt werden, sondern müssen getestet werden, bevor sie eingespielt werden. Falls sich ein Konflikt mit anderen kritischen Komponenten oder Programmen herausstellt, kann ein solches Update sonst zu einem Ausfall der IT-System führen. Nötigenfalls muss ein betroffenes IT-System so lange durch andere Maßnahmen geschützt werden, bis die Tests abgeschlossen sind.

Bevor ein Update oder Patch installiert wird, sollte die Daten auf dem IT-System gesichert werden, damit der Originalzustand nach Problemen wieder hergestellt werden kann. Dies gilt insbesondere dann, wenn aus Zeitgründen oder mangels eines geeigneten Testsystems nicht ausführlich getestet werden kann.

In jedem Fall muss dokumentiert werden, wann, von wem und aus welchem Anlass Patches und Updates eingespielt wurden. Wenn Schwachstellen gekannt werden, muss sich aus der Dokumentation der aktuelle Patchlevel der IT-Systeme jederzeit schnell ermitteln lassen, um schnell Klarheit darüber zu erhalten, ob die IT-Systeme dadurch gefährdet sind.

Falls festgestellt wird, dass ein Sicherheitsupdate oder Patch mit einer anderen wichtigen Komponente oder einem Programm inkompatibel ist oder Probleme verursacht, so muss sorgfältig überlegt werden, wie weiter vorgegangen wird. Wird entschieden, dass auf Grund der aufgetretenen Probleme ein Patch nicht installiert wird, so ist diese Entscheidung auf jeden Fall zu dokumentieren. Außerdem muss in diesem Fall klar beschrieben sein, welche Maßnahmen ersatzweise ergriffen wurden, damit die Schwachstelle nicht ausgenutzt werden kann. Eine solche Entscheidung darf nicht von den Administratoren alleine getroffen werden, sondern sie muss mit den Vorgesetzten und dem ISB abgestimmt sein.

Verwendung von vertrauenswürdigen Installationsmedien

Durch unvorsichtiges Ausführen von Programmen, die aus "unsicheren" Quellen stammen, kann beträchtlicher Schaden entstehen. Schadsoftware (so genannte Malware) kann beispielsweise Programme zum Ausspähen von Passwörtern, Trojanische Pferde oder Backdoors auf einem Client installieren, oder ganz einfach Daten beschädigen oder löschen.

Typische Quellen für solche Schadsoftware sind beispielsweise Programme, die sich als Bildschirmschoner, Virenscanner oder sonstige Hilfsprogramme ausgeben, und per E-Mail unter gefälschten Absenderadressen an sehr viele Empfänger verschickt werden. Oft laden auch unvorsichtige Anwender die Programme aus dem Internet herunter und installieren sie ohne Überprüfung.

Software sollte grundsätzlich nur aus bekannten Quellen installiert werden, besonders dann, wenn sie nicht auf Datenträgern geliefert, sondern beispielsweise aus dem Internet heruntergeladen wurde. Dies gilt besonders für Updates oder Patches, die normalerweise nicht mehr auf Datenträgern ausgeliefert werden. Die meisten Hersteller und Distributoren bieten zu diesem Zweck kryptographische Prüfsummen an, die zumindest eine Prüfung der Integrität eines Paketes erlauben. Die Prüfsummen werden dabei meist auf den (transportverschlüsselten) Webseiten der Hersteller veröffentlicht oder auch per (signierter) E-Mail verschickt. Um die Integrität eines heruntergeladenen Programms oder einer Archivdatei zu verifizieren, wird dann die veröffentlichte Prüfsumme mit einer von einem entsprechenden Programm lokal erzeugten Prüfsumme verglichen.

Falls zu einem Softwarepaket Prüfsummen angeboten werden, so sollten diese vor der Installation des Paketes überprüft werden.

Mit Prüfsummen kann die Authentizität nicht verifiziert werden. Daher werden in vielen Fällen für Programme oder Pakete digitale Signaturen angeboten. Die zur Überprüfung der Signatur benötigten öffentlichen Schlüssel sind wiederum meist auf den Webseiten des Herstellers oder von Public-Key-Servern verfügbar. Häufig werden die Prüfsummen mit einem der Programme PGP oder GnuPG erzeugt.

Ergibt die Prüfung, dass es sich um eine gültige Signatur des jeweiligen Herstellers handelt, ist das Paket vertrauenswürdiger als ein Paket, dass über Prüfsumme verfügt. Das bei Linux-Distributionen verbreitete Paketverwaltungssystem RPM (Redhat Package Manager) hat ebenso wie das Paketverwaltungssystem APT/DPKG bei Debian-basierten Distributionen bereits eine integrierte Überprüfungsfunktionalität.

Manchmal führen selbst die eingebauten Software-Updatemechanismen des jeweiligen Betriebssystems oder der Anwendungssoftware keine kryptographischen Prüfsummenvergleiche durch. Software ohne diese Prüfungen sollte nicht verwendet werden. Wenn möglich, sollte allerdings für jedes Softwarepaket die Prüfsumme verifiziert werden, bevor es eingespielt wird.

Ferner können die Prüfsummen oft nicht automatisch verglichen werden, da die hierfür erforderlichen Checksummen, Signaturen oder Zertifikate von den Herstellern nicht auf eine einheitliche Weise bereitgestellt werden. Daher müssen sie häufig manuell über die Prüfsummen von den Herstellerseiten oder durch eine Anpassung der URLs in der Patch- und Änderungssoftware verglichen werden.

Falls zu einem Softwarepaket digitale Signaturen verfügbar sind, sollten diese auf jeden Fall überprüft werden, bevor das Paket installiert wird.

Ein prinzipielles Problem bei der Verwendung digitaler Signaturen stellt die Verifikation der Authentizität des verwendeten Schlüssels selbst dar. Trägt der öffentliche Schlüssel keine Signatur einer bekannten vertrauenswürdigen Person oder Organisation (etwa eines Trustcenters), so bieten die mit dem entsprechenden privaten Schlüssel erzeugten Signaturen keine wirkliche Sicherheit, dass das Softwarepaket tatsächlich vom Entwickler, Hersteller oder Distributor stammt. Daher sollten die öffentlichen Schlüssel, sofern sie nicht zertifiziert sind, möglichst aus einer anderen Quelle als das Softwarepaket selbst bezogen werden, beispielsweise von einer DVD des Herstellers, von einem anderen Spiegelserver, auf dem das Paket ebenfalls heruntergeladen werden kann, oder von einem Public Key Server.

Um Prüfsummen und digitalen Signaturen zu überprüfen, müssen die entsprechenden Programme lokal vorhanden sein. Die Administratoren sollten über die Bedeutung und Aussagekraft von Prüfsummen und digitalen Signaturen informiert sein. Außerdem müssen die Administratoren genügend Zeit haben, die entsprechenden Programme im Arbeitsalltag einzusetzen und sich mit der Bedienung vertraut zu machen.

Patches und Änderungen sollten aus verschiedenen Gründen nicht per E-Mail bezogen werden. Die Herkunft von E-Mails ist ohne Einsatz zusätzlicher Sicherheitsmechanismen schwer festzustellen und die Empfängeradressen in den Institutionen sind oft Verteilerlisten, deren Adresse leicht zu erraten ist. Patches und Änderungen können außerdem mittlerweile sehr umfangreich sein. Viele Unternehmen und Behörden haben die Größe von E-Mail-Anhängen beschränkt und verbieten es unter Umständen, ausführbare Anhänge anzunehmen. Ferner werden durch die großen Datenmengen die E-Mail-Systeme unnötig belastet. Daher kann eine rechtzeitige Verfügbarkeit der Software-Änderungen, welche besonders bei Sicherheitspatches kritisch sein kann, via E-Mail nicht ausreichend gewährleistet werden.

Des Weiteren bieten einige Hersteller an, Änderungen und Patches dem Kunden direkt auf Datenträgern zuzusenden. Auch in diesem Fall sollten die Patches und Änderungen möglichst anhand von Prüfsummen oder digitalen Signaturen verifiziert werden, denn Absender-Angaben auf Postsendungen und Hersteller-Logos auf CDs und DVDs lassen sich leicht fälschen.

Ein weiterer Aspekt zur Prüfung der Echtheit der Aktualisierung können vom Hersteller veröffentlichte Nachrichten auf seiner Webseite, per Newsletter oder über ähnliche Kanäle sein. Einige Hersteller haben Zyklen und Zeitpunkte etabliert, zu denen systematisch Informationen über Änderungen veröffentlicht werden.

SYS.2.1.M15 Sichere Installation und Konfiguration von Clients

Nachdem die Planung eines neuen Clients abgeschlossen und eine Sicherheitsrichtlinie erstellt wurde, kann mit der Installation des Clients begonnen werden.

Die Installation und Konfiguration des IT-Systems sollte nur von autorisierten Personen (Administratoren oder vertraglich gebundene Dienstleister) durchgeführt werden. Administratoren für IT-Systeme und deren Vertreter müssen sorgfältig ausgewählt werden. Sie müssen regelmäßig darüber belehrt werden, dass die Befugnisse nur für die erforderlichen Administrationsaufgaben verwendet werden dürfen. Da Administratoren hinsichtlich der Funktionsfähigkeit der eingesetzten Hard- und Software eine Schlüsselrolle innehaben, muss auch beim Ausfall von Administratoren die Weiterführung der Tätigkeiten gewährleistet sein. Hierzu müssen die benannten Vertreter über den aktuellen Stand der Systemkonfiguration verfügen sowie Zugriff auf die für die Administration benötigten Passwörter, Schlüssel und Sicherheitstoken haben.

Es ist empfehlenswert, zunächst ein kurzes Installationskonzept entsprechend den funktionalen Anforderungen aus der Planung und den Vorgaben der Sicherheitsrichtlinie zu erstellen. Prinzipiell ist es vorteilhaft, die Installation in zwei Phasen vorzunehmen: Zunächst wird ein Grundsystem installiert und konfiguriert, anschließend werden die weiteren benötigten Anwendungen eingerichtet. Die Installationsprogramme der meisten Betriebssysteme unterstützen diese Vorgehensweise mehr oder weniger gut.

Die beschriebenen Schritte brauchen nicht notwendigerweise alle für jeden Client erneut durchgeführt zu werden. Dies könnte sogar insofern kontraproduktiv sein, als die ständige Wiederholung die Gefahr von Fehlern erhöht. Es wird daher empfohlen, die beschriebenen Schritte einmal besonders sorgfältig auf einem Referenz-System durchzuführen, die nötigen Konfigurationen genau zu dokumentieren und so ein angepasstes Installationskonzept für das betreffende Betriebssystem zu erhalten (siehe SYS.2.1.M27 Einrichten einer Referenzinstallation für Clients). Dabei muss beachtet werden, dass dieses Installationskonzept auch bei Änderungen am Betriebssystem, die kein komplett neues Release darstellen (Service-Packs, Update-Releases oder ähnliches) überprüft und gegebenenfalls angepasst werden muss.

Installation

Während der Installation und der späteren Konfiguration sollten zumindest die wichtigen Schritte so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können. Beispielsweise kann eine Checkliste für die Installation erstellt werden, auf der durchgeführte Schritte abgehakt und vorgenommene Einstellungen vermerkt werden können. Eine entsprechende Dokumentation ist für eine Fehleranalyse oder spätere Neuinstallation hilfreich. Dabei sollte beachtet werden, dass neben dem Autor auch weitere, auf diesem Gebiet eventuell weniger spezialisierte, Administratoren auf die Dokumentation zurückgreifen müssen. Daher ist es wichtig, dass die Dokumentation gut strukturiert und verständlich ist.

Wird der Client von Datenträgern wie DVDs oder anderen Speichermedien installiert, wird empfohlen, die Installation und Grundkonfiguration offline oder zumindest in einem sicheren Netz (Installations- oder Administrationsnetz) durchzuführen. Generell sollte verhindert werden, dass andere IT-Systeme während der Installation auf das zu installierende IT-System zugreifen können. Dies ist wichtig, weil während der Installation meist noch keine Passwörter vergeben und keine Schutzmechanismen aktiv sind, aber eventuell schon Zugriffe möglich sind. Falls die Installation mehrerer IT-Systeme teilweise über das Netz erfolgen soll (beispielsweise Nachladen von Paketen), so wird empfohlen, einen Installationsserver im Administrationsnetz zu nutzen.

Insbesondere beim Betriebssystem selbst ist es wichtig, dass die installierte Version aus einer vertrauenswürdigen Quelle stammt. Dies ist besonders wichtig, wenn beispielsweise CD -Images aus dem Internet heruntergeladen wurden. In diesem Fall sollte unbedingt geprüft werden, ob digitale Signaturen der Pakete verfügbar sind, die zur Verifikation von Integrität und Authentizität der Pakete verwendet werden können. Pakete und CD-Images, für die keine digitalen Signaturen oder wenigstens Prüfsummen existieren, sollten möglichst nicht eingesetzt werden (siehe auch SYS.2.1.M13 Updates und Patches für Firmware, Betriebssystem und Anwendungen).

Bei der Einrichtung der Festplattenpartitionen muss das in der Planungsphase erstellte Konzept umgesetzt werden. Wenn ein verschlüsseltes Dateisystem eingesetzt werden soll, so muss es meist initialisiert werden, bevor Daten hineinkopiert werden können, denn oft lässt sich ein Dateisystem nicht im Nachhinein verschlüsseln.

Sofern dies nicht bereits automatisch geschehen ist, sollte spätestens beim Abschluss der Grundinstallation auch die Protokollierung der Systemereignisse aktiviert werden. Die Protokolldaten können bei Problemen bei der weiteren Installation und Konfiguration wertvolle Informationen liefern.

Konfiguration

Die Grundeinstellungen, die vom Hersteller oder Distributor eines Betriebssystems vorgenommen werden, sind meist nicht auf Sicherheit optimiert, sondern auf eine einfache Installation und Inbetriebnahme sowie oft darauf, dass jeder Anwender möglichst einfach auf möglichst viele Features des Betriebssystems zugreifen kann. Beim Einsatz von IT-Systemen (egal, ob als Client oder Server) in Behörden oder Unternehmen ist dies oft nicht wünschenswert.

Der erste Schritt bei der Grundkonfiguration muss daher sein, die Grundeinstellungen zu überprüfen und nötigenfalls entsprechend den Vorgaben der Sicherheitsrichtlinie anzupassen. Die Grundkonfiguration ist naturgemäß relativ stark vom eingesetzten Betriebssystem abhängig. Aus diesem Grund sind in den betriebssystemspezifischen Bausteinen entsprechende detailliertere Empfehlungen enthalten.

Ziele einer sicheren Grundkonfiguration sollten sein, dass

- die Clients gegen "einfache" Angriffe über das Netz abgesichert ist,
- kein normaler Benutzer durch reine Neugierde oder gar zufällig Zugriff auf sensitive Daten erlangen kann, die nicht für ihn bestimmt sind,
- kein normaler Benutzer beim normalen Arbeiten mit den Clients durch reine Bedienungsfehler oder Leichtsinn ("Was passiert eigentlich, wenn ich diese Datei lösche?") schwerwiegenden Schaden an den IT-Systemen oder an den Daten anderer Benutzer verursachen kann, und dass
- auch für die Arbeiten der Systemadministratoren die Auswirkungen kleinerer Fehler so weit wie möglich begrenzt sind.

Die Einstellungen, die im Rahmen der Grundkonfiguration überprüft und angepasst werden sollten, betreffen insbesondere die folgenden Bereiche:

- Einstellungen für Systemadministratoren
  Die Kennungen, unter denen Systemadministratoren arbeiten, sollten besonders stark abgesichert werden. Dies betrifft beispielsweise die Einstellungen für die Benutzerumgebung wie

-
  - Suchpfade für Programme und Dateien,
  - Umgebungsvariablen und die
  - Konfiguration bestimmter Programme.

Diese Einstellungen sollten überprüft und gegebenenfalls angepasst werden. Außerdem sollten die Einstellungen für die Benutzerverzeichnisse von Systemadministratoren so gewählt werden, dass normale Benutzer keinen Zugriff darauf haben.

- Einstellungen für die Systemverzeichnisse und -dateien
  Bei der Grundkonfiguration muss überprüft werden, ob die Berechtigungen für Systemverzeichnisse und -dateien den Vorgaben der Sicherheitsrichtlinie entsprechen. Auf einem Server sollten für die Berechtigungen der Systemverzeichnisse und -dateien relativ restriktive Einstellungen gewählt werden.
- Einstellungen für Benutzerkennungen und Benutzerverzeichnisse
  Im Rahmen der Grundkonfiguration sollte überprüft werden, welche Standardeinstellungen für Benutzerkennungen und Benutzerverzeichnisse gelten. Die Einstellungen müssen gegebenenfalls entsprechend der Sicherheitsrichtlinie angepasst werden. Dies betrifft im Wesentlichen dieselben Parameter wie für Systemadministrator-Kennungen, für normale Benutzer können aber unter Umständen andere Einstellungen sinnvoll sein.
- Einstellungen für den Zugriff auf das Netz
  Im Rahmen der Grundkonfiguration sollten auch die Einstellungen für den Zugriff auf das Netz sowie wichtige externe Dienste getroffen und dokumentiert werden. Dies betrifft beispielsweise (sofern nicht bereits bei der Installation geschehen):
  - Vergabe der IP-Adresse und Konfiguration der grundlegenden Netzparameter oder Konfiguration des Zugriffs auf einen Server, der automatisch, beispielsweise über DHCP (Dynamic Host Configuration Protocol) Netzeinstellungen verteilt. Für Server wird allerdings von der Verwendung von DHCP abgeraten.
  - Konfiguration des Zugriffs auf einen DNS-Server und gegebenenfalls andere Namensdienste und die
  - Konfiguration des Zugriffs auf verteilte Dateisysteme, Datenbanken oder sonstige externe Dienste.
- Zusätzlicher Schutz durch einen lokalen Paketfilter
  Clients mit hohem Schutzbedarf sollten zusätzlich zum Schutz durch die institutionsweiten Sicherheitsgateways oder Paketfilter, die das interne Netz segmentieren, mit einem lokalen Paketfilter (siehe SYS.2.1.M28 Einrichtung lokaler Paketfilter) oder einer Personal Firewall abgesichert werden. Entsprechende Funktionalitäten sind in praktisch allen modernen Betriebssystemen vorhanden.
- Deaktivierung von "Call Home"-Funktionen
  Einige Betriebssysteme und Anwendungen senden Informationen, beispielsweise über aufgetretene Fehler oder über die Systemkonfiguration , direkt an den Hersteller, damit dieser zukünftig das Produkt an die Bedürfnisse der Anwender anpassen kann. Hierfür wird eine Datenverbindung über Datennetze, wie dem Internet, zu den Servern des Herstellers aufgebaut. Eine solche Form des Datenabflusses kann kritisch sein, vor allem, wenn die Anwender nicht über die Häufigkeit und Inhalte der Datenweitergabe informiert werden.Generell sollte dieser oft unerwünschte Informationsaustausch unterbunden werden. Ob und wie Informationen versendet werden, kann in der Regel den Lizenzvereinbarungen der eingesetzten Software entnommen werden.Viele Applikationen bieten die Möglichkeit, diese "Call Home"-Funktion zu deaktivieren. Nur in begründeten Ausnahmefällen sollte diese aktiviert bleiben. Nach Updates sollte überprüft werden, ob die "Call Home"-Funktion weiterhin deaktiviert ist.Durch lokale Paketfilter oder dem zentralen Sicherheitsgateway (Firewall) kann ebenfalls der Verbindungsaufbau mit dem Hersteller unterbunden werden. Beispielsweise könnten auf Grundlage der Zieladressen oder der Portnummern die Datenverbindungen abgewiesen werden. Hierbei ist zu beachten, dass die Berücksichtigung aller Applikationen aufwändig ist und automatische Update-Funktionen, falls benötigt, dann oft nicht mehr zur Verfügung stehen.
- Deaktivieren nicht benötigter Schnittstellen
  In einer Grundkonfiguration sind üblicherweise alle vorhandenen oder auch potentiell nachrüstbaren Schnittstellen aktiviert. Häufig werden nicht alle davon benötigt und sollten daher entfernt oder deaktiviert werden. Einige dieser Schnittstellen können auch potentielle Sicherheitsprobleme mit sich bringen, denen durch geeignete organisatorische oder technische Sicherheitsmaßnahmen entgegengewirkt werden muss. Schnittstellen, deren Nutzung kontrolliert werden sollte, sind beispielsweise Bluetooth, WLAN, Firewire, eSATA (externer SATA-Festplattenanschluss) und Thunderbolt.
- Verzeichnisbasierte Ausführungskontrolle
  Bei aktuellen Betriebssystemen ist eine verzeichnis- oder partitionsbasierte Ausführungskontrolle möglich. Dabei werden die Ausführungsrechte für alle Dateien in einem Verzeichnis und allen Unterverzeichnissen unterbunden. Beispielsweise kann dies auf windowsbasierten Betriebssystemen durch entsprechende Gruppenrichtlinien mit "Richtlinien für Softwareeinschränkung" erreicht werden. Auf Linux-Systemen kann die Festplatte zweckdienlich partitioniert und mit pas-

Es sollte dokumentiert werden, welche Einstellungen im Rahmen der Grundkonfiguration überprüft wurden, sowie ob und gegebenenfalls wie sie geändert wurden. Die Dokumentation muss so beschaffen sein, dass im Notfall auch eine andere Person als der eigentliche Administrator ohne vorherige Kenntnis der IT-Systeme anhand der Dokumentation nachvollziehen kann, was getan wurde. Im Idealfall sollte es möglich sein, alleine mit Hilfe der Dokumentation die IT-Systeme wiederherzustellen.

SYS.2.1.M16 Deaktivierung und Deinstallation nicht benötigter Komponenten und Kennungen

Oft wird im Rahmen der Standardinstallation eines Betriebssystems eine größere Anzahl von Benutzerkennungen, Programmen, Diensten und sonstige Komponenten eingerichtet, die für den Betrieb nicht in jedem Fall notwendig sind. Daher sollte im Rahmen der Grundkonfiguration geprüft werden, welche Benutzerkonten wirklich gebraucht werden. Nicht benötigte Benutzerkennungen sollten entweder gelöscht oder zumindest so deaktiviert werden, so dass unter der betreffenden Kennung keine Anmeldung am IT-System möglich ist.

Die Standardinstallation eines Betriebssystems enthält oft eine Reihe von Programmen und Diensten, die normalerweise nicht benötigt werden und die gerade deswegen eine Quelle von Sicherheitslücken sein können. Dies gilt insbesondere für Netzdienste. Nach der Installation sollte deswegen überprüft werden, welche Dienste und Anwendungen auf den IT-Systemen installiert und aktiviert sind. Nicht benötigte Dienste sollten deaktiviert oder ganz deinstalliert werden. Außerdem SOLLTEN nicht benötigte Laufzeitumgebungen, Interpretersprachen und Compiler deinstalliert werden.

Die Überprüfung auf laufende Dienste kann einerseits lokal mit den Mitteln des installierten Betriebssystems und bei Netzdiensten andererseits von außen durch einen Portscan von einem anderen System aus erfolgen. Durch eine Kombination beider Methoden kann weitgehend ausgeschlossen werden, dass die IT-Systeme noch weitere ungewollte Netzdienste anbietet.

Neben Diensten sollte ebenfalls alle nicht benötigten regelmäßigen bzw. auf Ereignis zu startenden Aufgaben (Tasks) entfernt werden.

SYS.2.1.M17 Einsatzfreigabe

Bevor Clients im produktiven Betrieb eingesetzt und bevor sie an ein produktives Netz angeschlossen werden, sollte der Einsatz freigegeben werden, dies ist zu dokumentieren. Die Einsatzfreigabe basiert auf einer Prüfung der Installations- und Konfigurationsdokumentation und der Funktionsfähigkeit der IT-Systeme in einem Test. Sie erfolgt durch eine in der Institution dafür autorisierte Stelle.

Vertiefende Informationen hierzu sind in OPS.1.1.7 Softwaretests- und Freigaben zu finden.

Falls festgestellt wird, dass ein Sicherheitsupdate oder Patch mit einer anderen wichtigen Komponente oder einem Programm inkompatibel ist oder Probleme verursacht, so muss sorgfältig überlegt werden, wie weiter vorgegangen wird. Wird entschieden, dass auf Grund der aufgetretenen Probleme ein Patch nicht installiert wird, so ist diese Entscheidung auf jeden Fall zu dokumentieren. Außerdem muss in diesem Fall klar beschrieben sein, welche Maßnahmen ersatzweise ergriffen wurden, damit die Schwachstelle nicht ausgenutzt werden kann. Eine solche Entscheidung darf nicht von den Administratoren alleine getroffen werden, sondern sie muss mit den Vorgesetzten und dem ISB abgestimmt sein.

SYS.2.1.M18 Nutzung von TLS [Benutzer]

Das bei der Web-Nutzung am häufigsten verwendete Sicherheitsprotokoll ist SSL/TLS (Secure Socket Layer/Transport Layer Security), weitere Informationen sind in [TR02102], [RFC5246] und [RFC5246] zu finden. Die erste Version des SSL-Protokolls (SSL v1.0) wurde von Netscape entwickelt. Neuere Versionen sind unter der Bezeichnung TLS in verschiedenen RFCs standardisiert. SSL/TLS wird von allen aktuelleren Browsern unterstützt. Mit SSL/TLS können Verbindungen abgesichert werden:

- durch Verschlüsselung der Verbindungsinhalte,
- durch Überprüfung der Vollständigkeit und Korrektheit der übertragenen Daten,
- durch Prüfung der Identität des Servers und
- optional durch Prüfung der Identität der Client-Seite.

Zu Beginn einer neuen mit SSL/TLS abgesicherten Kommunikationsverbindung findet ein sogenannter Handshake zwischen Client und Server statt. Hierbei verständigen sich Client und Server über die kryptographischen Algorithmen, die für Schlüsselaustausch, Verschlüsselung und Integritätssicherung eingesetzt werden. Außerdem einigen sich Client und Server über die SSL-Version, die verwendet wird. Zusätzlich sendet der Server sein X.509-Zertifikat an den Client. Optional kann auch der Client dem Server sein X.509-Zertifikat übermitteln, falls dies vom Server angefordert wird. Mit Hilfe eines asymmetrischen Verschlüsselungsverfahrens wird anschließend ein symmetrischer Schlüssel sicher ausgetauscht. Für die Verschlüsselung der eigentlichen Datenübertragung wird nun ein symmetrisches Verfahren benutzt, weil hiermit dies große Datenmengen schneller verschlüsselt werden können. Bei jeder Transaktion wird ein anderer symmetrischer Schlüssel als "Session Key" ausgehandelt, mit dem dann die Verbindung verschlüsselt wird.

Ein Benutzer kann Webseiten, die eine SSL/TLS-gesicherte Datenübertragung ermöglichen, beispielsweise daran erkennen, dass die Internet-Adresse um ein "s" erweitert ist (https://www...). Zusätzlich werden solche Webseiten bei den meisten gängigen Browsern auch besonders gekennzeichnet, beispielsweise durch ein angezeigtes Symbol (Schlüssel, Vorhängeschloss etc.) oder durch eine farbliche Markierung der Internet-Adresse.

Die Nutzung von SSL/TLS ist nicht auf HTTP-Clients und -Server beschränkt. Auch Protokolle wie SMTP, FTP, IMAP oder LDAP können durch SSL/TLS kryptographisch abgesichert werden, allerdings setzt dies voraus, dass die betreffenden Clients und Server diese Sicherheitsfunktion jeweils unterstützen.

SSL/TLS besteht aus zwei Schichten. Auf der oberen Schicht arbeitet das SSL/TLS Handshake Protokoll. Dieses dient dem Client und dem Server dazu, sich gegenseitig zu authentisieren sowie dazu, für den anschließenden Datenverkehr einen Schlüssel und einen Verschlüsselungsalgorithmus auszuhandeln. Die untere Schicht, das SSL/TLS Record Protokoll, das die Schnittstelle zur TCP-Schicht bildet, ver- und entschlüsselt den eigentlichen Datenverkehr. Da SSL/TLS für den Zugriff auf TCP auf der Socket-Schnittstelle aufsetzt und diese durch eine sicherheitserweiterte Version ersetzt, ist es auch für andere Dienste verwendbar.

Versionsnummer

Es existieren mehrere SSL/TLS-Protokollversionen, wie SSL v2, SSL v3, TLS v1.0, TLS v1.1 und TLS v1.2. SSL v1 wurde nicht veröffentlicht. Um eine sichere Verbindung zwischen Client und Server zu gewährleisten, sollte mindestens TLS 1.2 verwendet werden.

TLS 1.1 bietet ausreichende Sicherheit, aber im Vergleich zu TLS 1.2 weist es jedoch einige Schwächen auf, z. B. sind in TLS 1.1 noch Cipher-Suites vorhanden, die auf IDEA und DES basieren, in TLS 1.2 nicht mehr.

TLS 1.0 kann in bestehenden Client-Anwendungen übergangsweise weiter eingesetzt werden, falls eine sofortige Migration zu TLS 1.1 oder vorzugsweise TLS 1.2 nicht möglich ist und geeignete Maßnahmen gegen Chosen-Plaintext-Angriffe (z. B. BEAST) auf die CBC-Implementierung getroffen werden. Generell sollte jedoch eine Migration zu TLS 1.2 schnellstmöglich erfolgen. SSL v2 und SSL v3 dürfen nicht mehr eingesetzt werden, siehe hierzu auch den BSI-Migrationsleitfaden zum Mindeststandard TLS 1.2 (siehe [MIGLFTLS]).

Algorithmen und Schlüssellängen

Bei SSL/TLS können verschiedene kryptographische Algorithmen mit verschiedenen Schlüssellängen eingesetzt werden. Beim Verbindungsaufbau einigen sich Client und Server auf die in der Sitzung verwendeten Verfahren.

Durch die Auswahl der Produkte (Browser, Webserver, Plug-In etc.) und geeignete Konfiguration ist sicherzustellen, dass bei der SSL/TLS-geschützten Kommunikation ausschließlich Algorithmen und Schlüssellängen eingesetzt werden, die dem Stand der Technik und den Sicherheitsanforderungen der Institution entsprechen. Darüber hinaus sollten die verwendeten Cipher-Suites Perfect Forward Secrecy (PFS) unterstützen. Weitere Hinweise zu Algorithmen und Schlüssellängen finden sich im Baustein CON.1 Kryptokonzept.

Zertifikate

Es ist schwierig, bei der Datenkommunikation über offene Netze die Identität der Kommunikationspartner zu überprüfen, da nicht sichergestellt ist, dass Namensangaben korrekt sind. Bei SSL/TLS erfolgt die Überprüfung der Identität des Kommunikationspartners über so genannte Zertifikate. Zertifikate enthalten deren öffentliche Schlüssel sowie eine Bestätigung einer weiteren Instanz über die korrekte Zuordnung des öffentlichen Schlüssels zu dessen "Besitzer", hier also ein Server oder Client. Der Wert eines Zertifikates hängt also nicht zuletzt davon ab, wie vertrauenswürdig diese Bestätigungsinstanz (auch Trustcenter oder Zertifizierungsstelle genannt) ist. Die Echtheit des Zertifikates lässt sich wiederum mit dem öffentlichen Schlüssel der Bestätigungsinstanz überprüfen.

Gängige Betriebssysteme und Anwendungsprogramme, wie Browser, enthalten bereits bei der Installation SSL/TLS-Zertifikate einiger Zertifizierungsstellen. Diese Zertifizierungsstellen haben sehr unterschiedliche Sicherheitsleitlinien und Bedingungen, unter denen sie Zertifikate erteilen. Bevor sicherheitskritische Informationen über eine SSL/TLS-geschützte Verbindung übertragen werden, sollte deshalb die Sicherheitsrichtlinie der jeweiligen Zertifizierungsstellen geprüft werden.

Bei der Aufnahme eines neuen Zertifikates sollte darauf geachtet werden, dieses erst nach Überprüfung des "Fingerprints" zu aktivieren. Der Fingerprint ist eine hexadezimale Zahl, die zusammen mit dem Zertifikat übermittelt wird. Zusätzlich sollte sie auf einem anderen Weg übermittelt und verglichen werden, da diese die Korrektheit des Zertifikats sicherstellen soll.

In der Vergangenheit ist es bereits vorgekommen, dass Zertifizierungsstellen kompromittiert und dadurch Hunderte gefälschte Zertifikate ausgestellt wurden, darunter auch solche für Online-Informationsdienste, Online-Portale, andere Zertifizierungsstellen und Anonymisierungsdienste. Durch Widerrufslisten und Validierungsprotokolle wie OCSP (Online Certificate Status Protocol) können gefälschte, manipulierte oder veraltete Zertifikate allerdings zeitnah als ungültig erklärt werden. Daher sollte die Validierung von Zertifikaten in Anwendungsprogrammen wie Browsern und E-Mail-Clients aktiviert werden. Dabei ist OCSP der Verwendung von Zertifikatswiderruflisten (Certificate Revocation Lists, CRLs) vorzuziehen, da OCSP zeitnahe Aktualisierungen über das Internet erlaubt.

Kann ein Zertifikat nicht validiert werden, beispielsweise weil der OSCP-Server nicht erreicht oder auf die Widerrufslisten nicht zugegriffen werden kann, dann gibt es aus Sicht des Clients zwei Möglichkeiten: Er kann die Verbindung beenden oder ein eventuell manipuliertes oder ungültiges Zertifikat akzeptieren. Die Entscheidung, was in solchen Fällen zu tun ist, sollte mit den Sicherheitsrichtlinien der Institution in Einklang stehen.

Session Renegotation und TLS-Kompression

Mittels der sogenannten Session Renegotiation (Session-Neuverhandlung) können sowohl Client als auch Server die Parameter einer bestehenden HTTPS-Sitzung neu aushandeln. Aufgrund eines Fehlers in der Spezifikation des TLS-Protokolls (siehe [RFC5246]) ist es einem Man-in-the-Middle-Angreifer möglich, die Session Renegotiation zu missbrauchen, um beliebige Inhalte in eine existierende HTTPS-Sitzung einzufügen. Mittlerweile wurde das TLS-Protokoll erweitert (siehe [RFC5746]) und dieser Designfehler behoben. Clientseitig sollte die Session Renegotiation deaktiviert werden.

TLS bietet die Möglichkeit, die übertragenen Daten vor der Verschlüsselung zu komprimieren. Dies kann dazu führen, dass Seitenkanalangriffe auf die Verschlüsselung über die Länge der verschlüsselten Daten, durchgeführt werden. Ein Beispiel hierfür ist CRIME (Compression Retro Info-leak Made Easy), ein 2012 vorgestellter Seitenkanal-Angriff, der das Ziel hat, eine HTTPS-Sitzung zu übernehmen. Um dies zu verhindern, sollte die TLS-Kompression deaktiviert werden.

Hinweis: Beim Einsatz von SSL/TLS ist zu beachten, dass verschlüsselte Daten hinsichtlich aktiver Inhalte und Schadprogramme nicht zentral, also z. B.am Sicherheitsgateway, überprüft werden können. Dies muss bei der Sicherheitskonzeption berücksichtigt werden, damit keine Sicherheitslücken entstehen. Weitere Empfehlungen hierzu finden sich unter anderem im Baustein OPS1.1.4 Malware-Schutz.

SYS.2.1.M19 Restriktive Rechtevergabe

Grundsätzlich sollten Berechtigungen immer restriktiv vergeben werden, so dass Benutzer genau auf die Dienste und Daten zugreifen können, die sie für ihre Aufgaben benötigen. Besonders wichtig ist dies bei Systemdateien bzw. -verzeichnissen.

Systemdateien bzw. -verzeichnisse sind Dateien und Verzeichnisse, für die der IT-Betrieb zuständig ist. Diese sind entweder für alle Benutzer von Bedeutung oder sie dienen Administrationszwecken.Auf Systemdateien sollte möglichst nur der IT-Betrieb Zugriff haben. Editorprogramme oder Compiler dürfen nicht genutzt werden, wenn sie nicht für die Aufgabenerfüllung erforderlich sind. Der Kreis der zugriffsberechtigten Administratoren sollte möglichst klein gehalten werden. Auch Verzeichnisse dürfen nur die notwendigen Privilegien für die Benutzer zur Verfügung stellen. Die Vergabe von Zugriffsrechten auf Systemdateien sollte grundsätzlich restriktiv und nur in Übereinstimmung mit den hausinternen Sicherheitsrichtlinien erfolgen.

Systemdateien sollten getrennt von Applikationsdaten und Benutzerdateien gespeichert werden. Dies sorgt für eine bessere Übersicht und erleichtert es, Datensicherungen zu erstellen und den hierauf Zugriff korrekt zu schützen.

Der Zugriff auf Systemdateien sollte immer protokolliert werden. Nicht benötigte Systemdateien sollten von den IT-System entfernt werden, damit sie nicht für Angriffe missbraucht werden können und auch nicht ständig auf Integrität kontrolliert werden müssen.

Bei der restriktiven Vergabe von Zugriffsrechten reicht es nicht aus, nur die Rechte eines Programms zu überprüfen. Zusätzlich muss auch die Rechtevergabe aller Programme überprüft werden, die von diesem Programm aus aufgerufen werden.

Die Integrität aller Systemdateien und -verzeichnisse, sowie die Korrektheit der Zugriffsrechte sollte nach Möglichkeit regelmäßig verifiziert werden. Für viele Betriebssysteme gibt es dafür Tools, mit denen solche Prüfungen schnell und zuverlässig durchgeführt werden können.

SYS.2.1.M20 Schutz der Administrationsschnittstellen

Es gibt unterschiedliche Zugriffsmöglichkeiten, um Clients zu administrieren. Abhängig von der genutzten Zugriffsart müssen eine Reihe von Sicherheitsvorkehrungen getroffen werden. Bei größeren Netzen ist es empfehlenswert und oft unumgänglich, die Clients in ein zentrales Netzmanagement-System einzubinden, da sonst eine sichere und effiziente Administration nicht gewährleistet werden kann. Die zur Administration verwendeten Methoden sollten in der Sicherheitsrichtlinie festgelegt und die Administration nur entsprechend der Sicherheitsrichtlinie durchgeführt werden.

Es wird empfohlen, für die verschiedenen Administrationstätigkeiten eine Übersicht zu erstellen, welche Arbeiten auf welchem Weg durchgeführt werden können. Vor allem ist es wichtig festzuhalten, ob bestimmte Tätigkeiten auf einem bestimmten Weg normalerweise nicht durchgeführt werden dürfen.

- Lokale Administration
  Die Administration von Clients direkt durch Zugriff über die Konsole ist nur für eine kleine Zahl von Rechnern handhabbar und wird in Umgebungen mit einer größeren Anzahl von Clients meist einen Ausnahmefall darstellen. Muss der IT-Betrieb ausnahmsweise doch lokal an einem Client arbeiten, ist es beispielsweise wichtig, dass der Administrator bei der Authentisierung über ein Passwort darauf achtet, dass dieses nicht ausgespäht werden kann. Gegebenenfalls sollte überlegt werden, für solche Arbeiten Einmalpasswörter oder ähnliches zu verwenden.
- Administration mit Hilfe eines Bootmediums
  Für bestimmte Administrationsarbeiten, die lokal an einem Client vorgenommen werden sollen kann es vorteilhaft sein, ein externes Boot-Medium einzusetzen, von dem der Client gestartet wird (siehe auch SYS.2.1.M4 Regelmäßige Datensicherung). Dies bietet den Vorteil, dass der Administrator sich einer "sauberen" Systemumgebung sicher sein kann. Allerdings hat diese Methode auch eine Reihe von Nachteilen, beispielsweise einen höheren Aufwand. Außerdem ist es auf diese Weise meist nicht möglich, bestimmte Fehlermeldungen, die im laufenden Betrieb auftreten, nachzuvollziehen.
- Remote-Administration
  Clients werden häufig von Administrationsrechnern aus über das Netz administriert. Um zu verhindern, dass dabei Authentisierungsinformationen der Administratoren abgehört oder gar von einem Angreifer manipuliert werden, sollte die Administration nur über sichere Protokolle (beispielsweise nicht über Telnet, sondern über SSH erfolgen. Eine ungesicherte Remote-Administration über externe (unsichere) Netze hinweg darf in keinem Fall erfolgen. Dies muss bereits bei der Festlegung der Sicherheitsrichtlinie berücksichtigt werden. Auch im internen Netz sollten soweit möglich keine unsicheren Protokolle verwendet werden.
- Administration über ein zentrales Managementsystem
  Falls für die Administration ein zentrales Managementsystem genutzt werden soll, so müssen für diesen Zugangsweg analoge Vorüberlegungen angestellt werden, wie für die Remote-Administration. Zusätzlich ist es wichtig, dass das zentrale Managementsystem selbst entsprechend sicher konfiguriert und administriert wird.

Routinetätigkeiten bei der Administration

Es wird empfohlen, für die üblichen Routinetätigkeiten des IT-Betriebs entsprechend der Sicherheitsrichtlinie Hinweise für die Administration zu erstellen. Dies umfasst beispielsweise Tätigkeiten wie

- Anlegen und Löschen von Benutzern,
- Installation und Deinstallation von Programmen,
- Einspielen von Sicherheitsupdates und Patches,
- Einspielen sonstiger Updates und Patches oder
- Regelmäßiger Integritätscheck mit entsprechenden Tools.

SYS.2.1.M21 Verhinderung der unautorisierten Nutzung von Rechnermikrofonen und Kameras

Viele IT-Systeme sind mit Mikrofonen und teilweise auch mit Kameras ausgestattet. Mikrofone und Kameras von vernetzten Client können von denjenigen benutzt werden, die Zugriffsrechte auf die entsprechende Gerätedatei haben. Für ein Mikrofon wäre das unter Unix zum Beispiel /dev/audio für die Soundkarte oder /dev/video für eine Kamera. Unter Windows bestimmen die Zugriffsrechte auf die entsprechenden Schlüssel der Registrierung (HKEY_LOCAL_MACHINE\HARDWARE\.), wer das Rechnermikrofon oder die Rechnerkamera aktivieren kann. Diese Rechte sind daher sorgfältig zu vergeben. Der Zugriff auf die Gerätedatei sollte nur möglich sein, solange jemand lokal an dem IT-System arbeitet. Wenn vorhandene Mikrofone oder Kameras nicht genutzt und damit nicht missbraucht werden sollen, müssen diese, wenn möglich, ausgeschaltet, deaktiviert oder physikalisch vom Gerät getrennt werden.

Falls das Mikrofon bzw. die Kamera in den Client fest eingebaut ist und nur durch Software ein- und ausgeschaltet werden kann, müssen die Zugriffsrechte so gesetzt sein, dass kein Unbefugter sie benutzen kann. Dies kann z. B. erfolgen, indem unter Unix allen Benutzern die Leserechte auf die Gerätedateien /dev/audio, /dev/video bzw. unter Windows die Zugriffsrechte auf die entsprechenden Schlüssel der Registrierung entzogen werden. Dadurch ist ausgeschlossen, dass ein normaler Benutzer das Mikrofon oder die Kamera benutzen kann, er kann aber weiterhin Audio- oder Video-Dateien abspielen. Kameras können auch einfach abgedeckt werden, beispielsweise mit einem geeigneten Aufkleber.

Bei IT-Systemen mit Mikrofon bzw. Kamera ist zu prüfen, ob Zugriffsrechte und Eigentümer bei einem Zugriff auf die Gerätedatei verändert werden. Falls dies der Fall ist oder falls gewünscht ist, dass jeder Benutzer Mikrofon oder Kamera benutzen kann und es nicht nur in Einzelfällen durch den IT-Betrieb freigegeben werden soll, muss der Administrator ein Kommando zur Verfügung stellen, das

- nur aktiviert werden kann, wenn jemand an dem IT-System angemeldet ist,
- nur durch diesen Benutzer aktiviert werden kann und
- die Zugriffsberechtigungen dem Benutzer nach dem Abmelden wieder entzieht.

Solange der Zugriff auf das Mikrofon oder die Kamera durch kein sicheres Kommando geregelt wird, müssen diese physikalisch vom Client oder der Client vom Netz getrennt werden.

Clients mit eingebautem Mikrofon oder Kamera sollten während einer vertraulichen Besprechung aus dem Raum entfernt werden oder zumindest ausgeschaltet werden. Bei einem Laptop sollten alle eventuell vorhandenen Verbindungen zu Kommunikationsnetzen, die nicht benötigt werden, getrennt werden. In den meisten Fällen ist es hierzu am einfachsten, das entsprechende Kabel auszustecken.

SYS.2.1.M22 Abmelden nach Aufgabenerfüllung [Benutzer]

Wird ein IT-System oder eine IT-Anwendung von mehreren Benutzern verwendet und besitzen die einzelnen Benutzer unterschiedliche Zugriffsrechte auf dort gespeicherte Daten oder Programme, so kann der erforderliche Schutz mittels einer Zugriffskontrolle nur dann erreicht werden, wenn jeder Benutzer sich nach Aufgabenerfüllung am IT-System oder der IT-Anwendung abmeldet. Ist es einem Dritten möglich, an einem IT-System oder in einer IT-Anwendung unter der Identität eines anderen weiterzuarbeiten, so ist jegliche sinnvolle Zugriffskontrolle unmöglich. Daher sind alle Benutzer zu verpflichten, sich nach Aufgabenerfüllung vom IT-System beziehungsweise von der IT-Anwendung abzumelden. Aus technischen Gründen (z. B. damit alle offenen Dateien geschlossen werden) sollten auch dann Regelungen für die Abmeldung von IT-Systemen und IT-Anwendungen getroffen werden, wenn keine Zugriffskontrolle realisiert ist.

Ist absehbar, dass nur eine kurze Unterbrechung der Arbeit erforderlich ist, kann an Stelle des Abmeldens auch die manuelle Aktivierung der Bildschirmsperre erfolgen (siehe auch SYS.2.1.M5 Bildschirmsperre). Bei längerer Abwesenheit sollte die Bildschirmsperre automatisch aktiviert werden.

Einige IT-Systeme und IT-Anwendungen bieten die Möglichkeit, einen Zeitraum vorzugeben, nach dessen Ablauf ein Benutzer bei Inaktivität automatisch vom IT-System abgemeldet wird. Es sollte überlegt werden, ob dieses Verfahren benutzt wird, da es auch zu Datenverlusten führen kann. Eine automatische Abmeldung kann z. B. bei PC-Pools mit starkem Publikumsverkehr eingesetzt werden, da hier ein angemeldeter Benutzer den Arbeitsplatz mit Hilfe der Bildschirmsperre unberechtigterweise blockieren kann.

Je nach Arbeitsplatzumgebung ist abzuwägen, welche Vorkehrungen für kurzfristige Abwesenheiten von Benutzern zu treffen sind. So sollte eine automatische Aktivierung der Bildschirmsperre bei Mehr-Benutzer-Systemen schneller erfolgen als bei solchen für einen Benutzer, also z. B. bereits nach fünf Minuten.

SYS.2.1.M23 Nutzung von Client-Server-Diensten

Der Informationsaustausch zwischen gleichberechtigten IT-Systemen wird oft als "Client-to-Client" oder oft als"Peer-to-Peer" bezeichnet. Jedes IT-System kann hierbei Dienste anbieten oder nutzen. Über die hierfür aufgebaute Kommunikationsverbindung können sich mehrere IT-Systeme Ressourcen dezentral untereinander teilen. Somit werden die typischen Funktionen eines Servers und eines Clients auf einem IT-System vereint.

Oft werden entsprechende Anwendungen genutzt, um folgende Dienste anderen IT-Systemen bereitzustellen:

- Nutzung von Druckern, die lokal an einem IT-System angeschlossen sind, durch Benutzer an anderen IT-Systemen,
- Zugriff auf Speicherbereiche der im IT-System eingebauten oder lokal angeschlossenen Festplatten ("File Sharing"),
- Direktkommunikation über Kurzmitteilungen ("Messaging") und
- Internettelefonie.

Vorteile von Client-to-Client-Diensten

Im Gegensatz zu einer servergestützten Architektur haben Client-to-Client-Dienste zahlreiche Vorteile:

- Ein dedizierter Server verursacht in der Anschaffung und im Betrieb zusätzliche Kosten.
- Fällt der zentrale Server aus, stehen die Ressourcen nicht mehr zur Verfügung ("Single Point of Failure"). Fällt bei Client-to-Client-Diensten ein Client aus, können im Allgemeinen genügend andere Clients einspringen.
- Geographisch benachbarte Clients können effizienter Informationen direkt untereinander austauschen, als wenn hierfür ein Server benutzt wird, der sich weit entfernt befindet.
- Server benötigen eine höhere Bandbreite, mehr CPU-Leistung und umfangreicheren Festplatten- und Arbeitsspeicher als Clients. Diese Anforderungen können in Client-to-Client-Netzen auf die Clients verteilt und dort ungenutzte Ressourcen verwendet werden.
- Freigegebene Informationen liegen oft auf mehreren Clients gleichzeitig und damit redundant vor.

Die Nutzung von Client-to-Client-Diensten hat allerdings auch eine Vielzahl von Nachteilen, die in vielen Fällen auf der fehlenden Zentralisierung zurückzuführen sind. Beispielsweise können die ausgetauschten Informationen nicht zentral auf Schadsoftware untersucht werden.

Architektur

Je nach Anforderungen können Client-to-Client-Dienste nur in einem lokalen Netz oder im gesamten Internet genutzt werden. Die Anzahl der IT-Systeme, die sich untereinander diese Ressourcen teilen können, reichen von nur wenigen, ausgewählten Clients bis zu einer unüberschaubaren Menge von unbekannten Clients. Generell kann aber zwischen zwei Arten von Client-to-Client-Diensten unterschieden werden:

- Lokale Client-to-Client-Dienste
  Bei lokalen Client-to-Client-Diensten können einzelne Clients anderen Clients in einem LAN Ressourcen freigeben. Diese Freigaben können oft direkt vom Betriebssystem verwaltet werden. Ein Beispiel hierfür ist die Datei- und Druckerfreigabe in Windows-Betriebssystemen.Der Zugriff dieser Dienste kann oft über Passwörter oder eine Auswahl an IP-Adressen eingeschränkt werden. In der Regel werden diese Dienste nicht über das lokale Netz hinaus genutzt und werden am Sicherheitsgateway (Firewall) abgewiesen.Da für diese Dienste kein eigener Server benötigt wird, können Kosten für die Beschaffung von Hard- und Software eingespart werden.
- Öffentliche Client-to-Client-Dienste
  Um Informationen mit Anwendern, die keinen Zugriff auf das LAN haben, auszutauschen, können öffentliche Client-to-Client-Dienste eingesetzt werden. Hierfür müssen in der Regel zusätzliche Applikationen auf dem jeweiligen IT-System installiert werden, damit diese die von anderen Clients bereitgestellten Dienste nutzen zu können. Da bei Client-to-Client-Diensten direkt zwischen zwei oder mehreren IT-Systemen Informationen ausgetauscht werden, sind für einen Verbindungsaufbau zusätzliche Informationen nötig, wie diese IT-Systeme erreichbar sind. Aus diesem Grund sollte es besonders bei großen Client-to-Client-Netzen eine Übersicht geben, auf welchem Client welche Ressourcen bereitgestellt werden.
  Prinzipiell werden folgende Typen unterschieden:
  - Zentrale Client-to-Client-Dienste
    Die installierte Applikation baut eine Verbindung zu einem Server auf, der Informationen zu anderen Clients verwaltet. Hierfür muss vorher die Applikation des Clients Informationen über die Ressourcen, die er bereitstellen möchte, an den Server übertragen. Erst nach diesem Schritt kann in der Regel ein IT-System auf Informationen über die anderen angemeldeten Clients zugreifen. Hierzu gehören beispielsweise die IP-Adresse, der Benutzer und die bereitgestellten Inhalte. Mit Hilfe dieser Informationen kann eine direkte Verbindung zu dem entfernten Client aufgebaut und dessen Ressourcen genutzt werden.Fällt der zentrale Server aus, stehen die Kontaktinformationen der angeschlossenen IT-Systeme nicht mehr zur Verfügung und die Clients können keine Datenverbindung mehr untereinander aufbauen. Dies hat den Ausfall des gesamten Client-to-Client-Netzes zur Folge.
  - Dezentrale Client-to-Client-Dienste:
    Bei dezentralen Client-to-Client-Diensten wird kein zentraler Server, der die angeschlossenen Benutzer verwaltet, benötigt. Die IT-Systeme der Benutzer dieser Dienste bauen untereinander Datenverbindungen auf, um Informationen über die bereitgestellten Ressourcen auszutauschen. Hierbei können nicht nur die Ressourcen der IT-Systeme, mit denen direkt eine Verbindung aufgebaut wird, durchsucht werden, sondern auch Informationen über andere Clients, die hiermit wiederum eine Datenverbindung aufgebaut haben, abgerufen werden. Da jeder Client mit mehreren Clients eine Verbindung aufbauen kann, entsteht ein Netz, über das jeder Client Informationen zu den bereitgestellten Ressourcen anderer Clients abrufen kann.Diese dezentralen Client-To-Client-Dienste setzen voraus, dass die Applikation mit einem Client aufgebaut werden muss, der Bestandteil dieses Netzes ist, um ebenfalls Mitglied des Netzes werden zu können. Die hierfür benötigten Kontaktinformationen müssen vorher bekannt sein. Da viele Netze von einer großen Menge von angeschlossenen IT-Systemen profitieren, werden diese Kontaktinformationen oft auf Webseiten veröffentlicht.
  - Hybride Client-to-Client-Dienste
    Hybride Client-to-Client-Dienste sind mit zentralen Client-to-Client-Diensten vergleichbar, mit dem Unterschied, dass mehrere voneinander unabhängige Server eingesetzt werden können. Wie bei zentralen Client-to-Client-Diensten übermitteln die Clients einem Server die Ressourcen, die sie bereitstellen und Kontaktinformationen, wie sie erreicht werden können. Die Server wiederum teilen diese Informationen weiteren Servern mit. Bei Bedarf können die Clients auf die Ressourcen anderer Clients zugreifen, die nicht vom selben Server verwaltet werden.

Alternativen für den Einsatz von Client-to-Client-Diensten

Nur bei wenigen Diensten ist eine Client-to-Client-Kommunikation zwischen IT-Systemen zwingend erforderlich. Beispielsweise können Ressourcen auch zentral von Servern bereitgestellt werden. Erst durch einen Einsatz von Servern können Vorgaben zentral umgesetzt werden, beispielsweise dass nur berechtigte Personen auf die Informationen zugreifen dürfen. Folgende Dienste, die typischerweise über Client-to-Client-Netze verteilt werden können, können zentralisiert bereitgestellt werden:

- Bereitstellung von Druckern
  Wenn mehrere Personen in einem LAN Zugriff auf Drucker benötigen, können diese zentral im Netz bereitgestellt werden. Hierfür eignet sich der Einsatz netzfähiger Drucker oder die Verwaltung über Druckserver (siehe SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte).
- File-Sharing
  Statt Speicher auf mehreren Clients im LAN freizugeben, können die Informationen zentral auf einem Dateiserver abgelegt werden. Sollen nur die Benutzer innerhalb eines LANs auf den Server zugreifen dürfen, können beispielsweise Samba-Server (siehe APP.3.4 Samba) oder NFS-Server (siehe SYS.1.3 Server unter Unix) die Informationen bereitstellen., allgemeine Empfehlungen sind in APP3.3 Fileserver zu finden. Sollen auch externe Benutzer auf die Informationen zugreifen dürfen, könnten die Informationen auf einen extern erreichbaren Webserver (siehe APP.3.2 Webserver) abgelegt werden.
- Messaging
  Wenn es nötig ist, Kurzmitteilungen zu versenden und nicht auf E-Mail zurückgegriffen werden soll, ist zu überlegen, einen Instant Messaging Server, wie beispielsweise Jabber, zu betreiben. Über diesen Server könnten die Nachrichten zentralisiert auf Schadsoftware überprüft werden.
  Auch die Kommunikation mit externen Gesprächspartnern kann mit Hilfe eines zentralen Instant Messaging Server, der von der Institution betrieben wird und sowohl von intern als auch von extern erreichbar ist, erfolgen. Vertiefende Informationen sind in APP.1.5 Instant Messaging zu finden
- VoIP (Voice over Internet Protocol) und Internettelefonie
  VoIP-Lösungen, wie im Baustein NET.4.2 VoIP beschrieben, unterscheiden zwischen der Signalisierung und dem Medientransport. Für die Signalisierung werden oft Server vorausgesetzt, auf denen die Teilnehmer verwaltet werden. Nachdem über die Signalisierung ein Gespräch zwischen zwei oder mehreren Benutzern eingeleitet wurde, werden bei vielen Lösungen die Sprachinformationen direkt zwischen den Benutzern ausgetauscht. Diese Art von Client-to-Client ist in einem LAN sinnvoll und sollte genutzt werden.
  Über die Grenzen eines LANs hinweg sollte Client-to-Client nicht zur Telefonie genutzt werden, beispielsweise sollte eine Institution keine solche Kommunikation zulassen, um mit externen Gesprächspartner zu kommunizieren ("Internettelefonie"). Auch in diesem Fall sollte sowohl die Signalisierung als auch der Medientransport auf einem Konzentrator, ähnlich einem Proxy, gebündelt werden. Auf dieser Weise wird der direkte Verbindungsaufbau einzelner Clients auf externe Gesprächspartner, die sich beispielsweise im Internet befinden können, vermieden.

Empfehlungen für den Einsatz von lokalen Client-to-Client-Diensten

Wenn möglich, sollten statt Freigaben über Client-to-Client-Dienste dedizierte Server zum Informationsaustausch genutzt werden. In Ausnahmefällen ist aber auch der Einsatz von Client-to-Client-Lösungen nötig, wie beispielsweise bei VoIP. Daher ist festzulegen:

- welche Client-to-Client-Dienste genutzt und
- welche Informationen ausgetauscht

werden dürfen. Wenn erforderlich, sind die Benutzer für die Nutzung von Client-to-Client-Diensten zu schulen. Es ist darauf zu achten, dass sich die Client-to-Client-Dienste nur auf das LAN beschränken.

Empfehlungen für den Einsatz von öffentlichen Client-to-Client-Diensten

Generell muss der unkontrollierte Informationsfluss aus einem LAN unterbunden werden. Hierzu gehören auch direkte Client-to-Client-Verbindungen von Clients zu IT-Systemen, die sich nicht im LAN befinden. Durch die fehlende Zentralisierung können unkontrolliert Informationen das LAN verlassen (z. B. vertrauliche Informationen) oder hinein gelangen (z. B. Schadsoftware). Durch folgende Maßnahmen kann die Nutzung von öffentlichen Client-to-Client-Diensten verhindert werden:

- Lokale Paketfilter
  Durch den Einsatz lokaler Paketfilter kann die Kommunikation der Clients auf wenige IT-Systeme beschränkt werden (siehe SYS.2.1.M28 Einrichtung lokaler Paketfilter). Beispielsweise könnten die Filterregeln so festgelegt werden, dass nur mit Servern kommuniziert werden darf.
  Auf Grundlage der IP-Adresse des Servers und der Portnummer des erlaubten Dienstes kann ein unerwünschter Kommunikationsaufbau erschwert werden. Durch den Einsatz von lokalen Paketfiltern kann sowohl die Verwendung von lokalen als auch öffentlichen Client-to-Client-Netzen unterbunden werden.
- Zentrale Filterung am Sicherheitsgateway (Firewall)
  Generell sollte das Sicherheitsgateway nur die notwendige Kommunikation in oder aus dem lokalen Netz zulassen, alle anderen Verbindungen sollten abgewiesen werden (siehe NET.3.2 Firewall). Verhindert das Sicherheitsgateway die Kommunikation der Clients aus dem LAN mit IT-Systemen im Internet, kann die Nutzung von öffentlichen Client-to-Client-Netzen verhindert werden.
- Richtlinie
  Neben technischen Empfehlungen sollte den Mitarbeitern der Institution auch die Verwendung von Client-to-Client-Diensten untersagt werden. Diese Anweisung kann in der Sicherheitsrichtlinie für Benutzer formuliert werden.

Wenn in der Institution Client-to-Client-Dienste genutzt werden sollen, muss dies durch die Leitungsebene der Institution beschlossen werden. Der Informationssicherheitsbeauftragte muss hierbei einbezogen werden, außerdem ist die Entscheidung inklusive der Restrisiken zu dokumentieren.

SYS.2.1.M24 Umgang mit Wechseldatenträgern im laufenden System

Handelsübliche PCs sind heute in der Regel mit einem CD-/DVD-/Blu-ray-Laufwerk bzw. CD-/DVD-/Blu-ray-Brenner ausgestattet, daher sollten die Empfehlungen des Bausteins OPS.1.2.3 Datenträgeraustausch und SYS.3.4 Mobile Datenträger berücksichtigt werden. Zusätzlich besteht die Möglichkeit, über Schnittstellen externe Speichermedien anzuschließen, die von vielen Betriebssystemen automatisch erkannt und eingebunden werden. Beispiele sind USB-Speicher, die an die USB-Schnittstelle angeschlossen werden, und Firewire-Festplatten. Außerdem sind in vielen IT-Systemen Kartenleser für Speicherkarten eingebaut. Durch solche Laufwerke für Wechselmedien und externe Datenspeicher ergeben sich folgende potentielle Sicherheitsprobleme:

- Das IT-System könnte von solchen Laufwerken unkontrolliert gebootet werden.
- Es könnte unkontrolliert Software von solchen Laufwerken eingespielt werden.
- Daten könnten unberechtigt auf Wechselmedien kopiert werden.

Wird von Wechselmedien gebootet oder wird hiervon Fremdsoftware installiert, können nicht nur Sicherheitseinstellungen außer Kraft gesetzt werden, sondern das IT-System kann auch mit Computer-Viren und anderen Schadprogrammen infiziert werden.

Diesen Gefahren muss durch geeignete organisatorische oder technische Sicherheitsmaßnahmen entgegengewirkt werden. Hierfür bieten sich verschiedene Vorgehensweisen an, deren spezifische Vor- und Nachteile im Folgenden kurz dargestellt werden:

- Ausbau von Laufwerken
  Der Ausbau der Laufwerke für Wechselmedien (bzw. der Verzicht bei der Beschaffung) bietet zwar den sichersten Schutz vor den oben genannten Gefährdungen, ist aber meist mit erheblichem Aufwand verbunden. Oft ist ein Ausbau überhaupt nicht möglich, z. B. bei Speicherkartenlesern bei Notebooks. Weiterhin ist zu berücksichtigen, dass der Ausbau unter Umständen die Administration und Wartung des IT-Systems behindert. Diese Lösung sollte in Betracht gezogen werden, wenn besondere Sicherheitsanforderungen bestehen. Wenn abzusehen ist, dass die Laufwerke für Wechselmedien nicht benötigt werden, sollten schon bei der Beschaffung Geräte ohne verbaute Laufwerke bevorzugt werden.
- Verschluss von Laufwerken
  Für einige Laufwerksarten gibt es abschließbare Einschubvorrichtungen, mit denen die unkontrollierte Nutzung verhindert werden kann. Bei der Beschaffung sollte sichergestellt werden, dass die Laufwerksschlösser für die vorhandenen Laufwerke geeignet sind und diese nicht beschädigen können. Es muss beachtet werden, dass nicht für alle Laufwerksarten, wie für eingebaute Speicherkartenleser, Schlösser angeboten werden. Außerdem sollte darauf geachtet werden, dass die Schlösser herstellerseitig mit hinreichend vielen unterschiedlichen Schlüsseln angeboten werden. Nachteilig sind die Beschaffungskosten für die Laufwerksschlösser und der Aufwand für die erforderliche Schlüsselverwaltung. Daher ist diese Lösung nur bei höherem Schutzbedarf oder besonderen Sicherheitsanforderungen sinnvoll.
- Deaktivierung im BIOS bzw. Betriebssystem
  Im BIOS bieten die meisten PCs Einstellmöglichkeiten dafür, von welchen Laufwerken gebootet werden kann. In Verbindung mit einem Passwort-Schutz der BIOS-Einstellungen kann dadurch das unkontrollierte Booten von Wechselmedien und mobilen Datenträgern unterbunden werden. Weiterhin können die vorhandenen Laufwerke und Schnittstellen bei modernen Betriebssystemen einzeln deaktiviert werden.
  Der Client kann auf diese Weise nun nur schwer unberechtigt genutzt werden, da z.B. von den Wechselmedien keine Fremdsoftware installiert oder Informationen hierauf kopiert werden können. Werden die Laufwerke im BIOS bzw. Betriebssystem deaktiviert, hat dies den Vorteil, dass die Hardware nicht verändert werden braucht. Die entsprechenden Einstellungen im Betriebssystem können gegebenenfalls sogar zentral vorgenommen werden. Damit diese Vorgehensweise wirksam ist, muss sichergestellt sein, dass die Benutzer nicht über die Berechtigungen im Betriebssystem verfügen, um die Deaktivierung der Laufwerke rückgängig zu machen.
- Verschlüsselung
  Es gibt Produkte, die dafür sorgen, dass ausschließlich Zugriffe auf dafür zugelassene mobile Datenträger möglich sind. Eine Lösung ist beispielsweise, dass nur noch mobile Datenträger gelesen und beschrieben werden können, die mit bestimmten kryptographischen Schlüsseln verschlüsselt worden sind. Dies schützt nicht nur vor unbefugtem Zugriff über manipulierte mobile Datenträger, sondern schützt auch die Daten auf den mobilen Datenträgern bei Verlust oder Diebstahl.
- Richtlinien für die Nutzung
  In vielen Fällen dürfen die Benutzer die eingebauten Laufwerke für Wechselmedien oder Speichermedien an externen Schnittstellen durchaus verwenden, die Nutzung ist jedoch durch entsprechende Richtlinien reglementiert. Auf technischer Ebene sollte dann das Booten von Wechselmedien im BIOS deaktiviert werden. Somit ist es nicht notwendig, die Laufwerke auszubauen, zu verschließen und im Betriebssystem zu deaktivieren.
  In diesem Fall sollten die Richtlinien für die Nutzung der Laufwerke und Speichermedien so explizit wie möglich definiert werden. Beispielsweise kann alles generell verboten werden, nicht öffentliche Text-Dokumente dürften kopiert werden. Die Richtlinien müssen allen Benutzern bekannt gemacht und die Einhaltung kontrolliert werden. Es sollte untersagt werden, Programme, die von Wechselmedien eingespielt wurden, zu installieren und zu starten, dies sollte soweit wie möglich auch technisch unterbunden werden.
  Diese rein organisatorische Lösung sollte nur dann gewählt werden, wenn die Benutzer mindestens hin und wieder auf die Laufwerke zugreifen müssen. Anderenfalls sollte der Zugriff, wie oben beschrieben, durch technische Maßnahmen unterbunden werden.

Bei der Auswahl einer geeigneten Vorgehensweise müssen immer alle Laufwerke für Wechselmedien berücksichtigt werden, aber ebenso auch alle Möglichkeiten, über Vernetzung Daten auszutauschen, also insbesondere auch E-Mail und Internet-Anbindungen. Wenn das IT-System über eine Verbindung zum Internet verfügt, ist es nicht allein ausreichend, alle Laufwerke für Wechselmedien zu deaktivieren oder auszubauen. Besonderes Augenmerk ist auf den Schutz vor Schadprogrammen, z. B. Computer-Viren oder Trojanische Pferde, zu richten (siehe auch SYS.2.1.M6 Einsatz von Virenschutzprogrammen).

Unabhängig von der Auswahl einer geeigneten Vorgehensweise sollte verhindert werden, dass Inhalte von Wechseldatenträgern automatisch ausgeführt werden, wenn die Datenträger angeschlossen werden. Hierzu sind die entsprechenden Autorun- und Autoplay-Funktionen des Betriebssystems zu deaktivieren.

Damit die Sicherheitsmaßnahmen akzeptiert und beachtet werden, müssen die Benutzer über die Gefährdung durch Laufwerke für Wechselmedien informiert und sensibilisiert werden.

Umgang mit USB-Geräten

Über die USB-Schnittstelle lassen sich eine Vielzahl von Zusatzgeräten an PCs anschließen. Beispiele sind Festplatten, CD/DVD-Brenner und USB-Sticks. Trotz großer Speicherkapazität sind USB-Sticks so handlich, dass sie beispielsweise in Form von Schlüsselanhängern hergestellt werden und in jede Hosentasche passen. In modernen Betriebssystemen sind die Treiber für USB-Massenspeichergeräte bereits integriert, so dass zum Betrieb keine Softwareinstallation mehr notwendig ist. Im Allgemeinen bezieht sich diese Empfehlungen nicht ausschließlich auf USB-Speichermedien, sondern generell auf alle USB-Geräte, die Daten speichern können. Unter anderem können auch USB-Drucker und USB-Kameras zum Speichern der Daten "missbraucht" werden. Dies gilt insbesondere für "intelligente" Geräte mit USB-Anschluss, die jede beliebige USB-Identität annehmen können, wenn sie mit spezieller Software ausgestattet sind. Dies können programmierbare USB-Entwicklerboards sein, aber auch bei vielen Smartphones ist ein solcher Einsatz möglich.

Über USB-Speichermedien können unkontrolliert Informationen und Programme ein- oder ausgelesen werden. Daher ist mit USB-Speichermedien generell genauso wie mit herkömmlichen Speichermedien umzugehen. Der Betrieb von USB-Speichermedien lässt sich nur sehr schwer verhindern, wenn die USB-Schnittstelle für andere Geräte genutzt wird. So werden beispielsweise Notebooks ausgeliefert, die zum Anschluss einer Maus nur die USB-Schnittstelle zur Verfügung stellen. Deswegen ist es meist nicht sinnvoll, ein "USB-Schloss" zu verwenden oder die Schnittstelle durch andere mechanische Maßnahmen zu deaktivieren. Die Nutzung von Schnittstellen sollte daher durch entsprechende Rechtevergabe auf Ebene des Betriebssystems oder mit Hilfe von Zusatzprogrammen geregelt werden. Alternativ kann überwacht werden, ob Geräte hinzugefügt werden. Um Datenspeicher an externen Schnittstellen anzuschließen, werden oftmals vom Betriebssystem Treiber bzw. Kernelmodule geladen oder Einträge in Konfigurationsdateien (wie der Windows-Registry) erzeugt, die detektiert werden können. Nachdem die Veränderungen festgestellt wurden, kann dann beispielsweise eine Protokolldatei erstellt oder der IT-Betrieb benachrichtigt werden. Dies alles kann jedoch nur mit Hilfe von Zusatzsoftware realisiert werden. Hierfür ist entweder eine Eigenentwicklung oder ein Drittprodukt notwendig.

SYS.2.1.M25 Richtlinie zur sicheren IT-Nutzung [Benutzer]

Um einen sicheren und ordnungsgemäßen Einsatz von Informationstechnik in größeren Unternehmen bzw. Behörden zu fördern, sollte eine Richtlinie erstellt werden, in der verbindlich vorgeschrieben wird, welche Randbedingungen eingehalten werden müssen und welche Sicherheitsmaßnahmen zu ergreifen sind. Die Richtlinie ist allen Benutzern zur Kenntnis zu geben, beispielsweise in elektronischer Form auf einem Intranet-Server. Jeder neue Benutzer muss die Kenntnisnahme der Richtlinie bestätigen, bevor er die Informationstechnik nutzen darf. Nach größeren Änderungen an der Richtlinie oder nach spätestens zwei Jahren ist eine erneute Bestätigung erforderlich.

Im Folgenden soll grob umrissen werden, welche Inhalte für eine solche Richtlinie sinnvoll sind:

Zielsetzung und Begriffsdefinitionen

Der erste Teil der Richtlinie dient dazu, die Anwender für Informationssicherheit zu sensibilisieren und zu motivieren. Gleichzeitig werden die für das gemeinsame Verständnis notwendigen Begriffe definiert, wie z. B. PC, Server, Netz, Anwender, Benutzer, schutzbedürftige Objekte.

Geltungsbereich

In diesem Teil muss verbindlich festgelegt werden, für welche Teile des Unternehmens bzw. der Behörde die Richtlinie gilt.

Rechtsvorschriften und interne Regelungen

Hier wird im Überblick dargestellt, welche wesentlichen Rechtsvorschriften, z. B. das Bundesdatenschutzgesetz und das Urheberrechtsgesetz, einzuhalten sind. Anhand von Beispielen sollte deutlich gemacht werden, welche Auswirkungen dies auf die Nutzung der Informationstechnik im jeweiligen Umfeld hat. Darüber hinaus kann diese Stelle genutzt werden, um alle relevanten betriebsinternen Regelungen aufzuführen.

Verantwortungsverteilung

In diesem Teil wird definiert, welcher Funktionsträger im Zusammenhang mit dem IT-Einsatz welche Verantwortung tragen muss. Dabei sind insbesondere die Rollen Benutzer, Vorgesetzte, IT-Betrieb, Revisor, Datenschutzbeauftragter und Sicherheitsmanagement-Team zu unterscheiden.

Ansprechpartner

Die Richtlinie sollte Ansprechpartner und Kontaktinformationen (Telefon, E-Mail etc.) für die Benutzer zu Fragen der Informationssicherheit enthalten oder aufzeigen, wo diese Informationen gefunden werden können. Dabei sollte beachtet werden, dass es häufig zu Verwirrung führt, wenn den Benutzern zu viele unterschiedliche Ansprechpartner genannt werden. Besser ist es meist, nur wenige unterschiedliche Ansprechpartner zu benennen, die dann bei Bedarf die Benutzer an die richtige Stelle verweisen (Help-Desk-Konzept).

Umzusetzende und einzuhaltende Sicherheitsmaßnahmen

Im letzten Teil der Richtlinie für die IT-Nutzung ist festzulegen, welche Sicherheitsmaßnahmen vom Benutzer einzuhalten bzw. umzusetzen sind. Dies kann je nach Schutzbedarf auch über die IT-Grundschutz-Maßnahmen hinausgehen. Typische Beispiele für Sicherheitsmaßnahmen am Arbeitsplatz sind das sichere An- und Abmelden am PC, der ordnungsgemäße Umgang mit Passwörtern und Verhaltensregeln bei der Nutzung des Internets.

Sind Telearbeiter im Unternehmen bzw. in der Behörde beschäftigt, sollte die Richtlinie um die Telearbeitsplatz-spezifischen Regelungen ergänzt werden.

SYS.2.1.M26 Schutz von Anwendungen

Um die Ausnutzung von Schwachstellen in Anwendungen zu erschweren, sollte ASLR und DEP/NX im Kernel aktiviert und von den Anwendungen genutzt werden. Sicherheitsfunktionen des Kernels und der Standardbibliotheken wie z. B. Heap- und Stackschutz sollten nicht deaktiviert werden.

Empfehlungen und Anmerkungen, die über diese Maßnahme hinausgehen, können gerne an die E-Mail-Adresse grundschutz@bsi.bund.de gesendet werden.

SYS.2.1.M27 Geregelte Außerbetriebnahme eines Clients

Bei der Außerbetriebnahme eines Clients muss vor allem sichergestellt werden, dass

- keine wichtigen Daten, die eventuell auf dem Client gespeichert sind, verloren gehen, und dass
- keine sensitiven Daten auf den Datenträgern des Clients zurück bleiben.

Dazu ist es insbesondere wichtig, einen Überblick darüber zu haben, welche Daten wo auf den IT-Systemen gespeichert sind.

- Datensicherung
  Vor der Außerbetriebnahme des Clients müssen lokal gespeicherte Daten, die noch benötigt werden, entweder extern gesichert bzw. archiviert (beispielsweise auf externen Festplatten, CDs oder DVDs) oder auf ein Ersatzsystem oder einen Fileserver übertragen werden. Nach der Sicherung sollte überprüft werden, dass wirklich alle Daten korrekt gesichert wurden.
  In diesem Zusammenhang kann es sinnvoll sein, den Benutzern für die Sicherung eventuell gespeicherter lokaler Daten ein geeignetes Laufwerk, beispielsweise einen externen CD- oder DVD-Brenner, zur Verfügung zu stellen.
  Weitere Informationen zu diesem Themenkomplex finden sich in SYS.2.1.M4 Regelmäßige Datensicherung sowie den Bausteinen OPS.1.1.5 Datensicherung und OPS.1.1.2 Archivierung.
- Austragen des IT-Systems aus Verzeichnisdiensten und Datenbanken
  Etwaige Berechtigungen im Netz, die an den Client selbst (und nicht an einen Benutzer) gekoppelt sind, müssen gelöscht werden. Beispiele hierfür sind Einträge auf Proxyservern am Sicherheitsgateway oder Zugriffsrechte auf Netzdienste, die anhand der IP-Adresse gewährt werden. Ist der Client in netzweiten Verzeichnisdiensten oder Datenbanken eingetragen (etwa in einer Windows Domäne, Active Directory, NIS oder ähnlichen), so müssen die zugehörigen Einträge gelöscht oder zumindest die entsprechenden Kennungen deaktiviert werden.
- Löschen der Daten auf dem IT-System
  Es muss sichergestellt werden, dass keine schützenswerten Informationen mehr auf den Festplatten vorhanden sind. Dazu genügt es nicht, die Platten einfach neu zu formatieren, sondern sie müssen mindestens einmal vollständig überschrieben werden. Es ist zu beachten, dass weder das logische Löschen mit den Löschfunktionen des Betriebssystems noch das Neuformatieren der Platten die Daten tatsächlich von den Festplatten entfernt. Mit geeigneter Software können Daten in solchen Fällen, oft sogar ohne großen Aufwand, wieder rekonstruiert werden.
  SSDs können wegen Wear Leveling und Reservekapazitäten nicht effektiv überschrieben werden, außerdem reduziert sich hierbei die erwartete Restlebensdauer der SSD. Bei SSDs empfiehlt sich stattdessen, die von der SSD bereitgestellte SECURE ERASE Funktionalität zu nutzen und anschließend das Ergebnis zu prüfen.
- Löschen von Datensicherungsmedien
  Nach der Außerbetriebnahme der IT-Systeme müssen gegebenenfalls auch die entsprechenden Datensicherungsmedien gelöscht werden, wenn die darauf gespeicherten Daten nicht mehr benötigt werden.
- Entfernen sonstiger Informationen
  Sind auf einem Client noch an anderen Stellen als auf der Festplatte (etwa in einem nichtflüchtigen Speicher) potentiell sensitive Daten gespeichert (beispielsweise bestimmte Konfigurationsdaten), so müssen auch diese vor der Weitergabe des Geräts entfernt werden.

Es wird empfohlen, anhand der oben gegebenen Empfehlungen eine Checkliste zu erstellen, die abgearbeitet werden kann, wenn das IT-Systeme außer Betrieb genommen wird. Auf diese Weise kann vermieden werden, dass einzelne Schritte vergessen werden. Vertiefende Informationen sind auch in OPS.1.2.7 Verkauf/Aussonderung von IT zu finden.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

SYS.2.1.M28 Verschlüsselung der Clients (C)

Vertrauliche Informationen auf Datenträgern können auf verschiedene Weise verschlüsselt und damit vor unbefugter Kenntnisnahme geschützt werden. So können beispielsweise der komplette Datenträger, eine einzelne Partition oder nur einzelne Dateien verschlüsselt werden. Aus Sicherheitssicht ist es besser, den kompletten Datenträger zu verschlüsseln, da dann weniger Benutzereingriffe erforderlich sind und alle Daten vor unbefugtem Zugriff geschützt sind. Die Verschlüsselung eines gesamten Datenträgers oder einer kompletten Partition ist für die Benutzer nahezu transparent. Lediglich beim Booten oder dem ersten Zugriff auf die Partition müssen sich die Benutzer authentisieren. Werden nur einzelne Dateien oder Dateicontainer verschlüsselt, besteht die Gefahr, dass versehentlich schützenswerte Daten in unverschlüsselten Bereichen der Festplatte abgelegt werden. Zudem muss hierfür ein Verschlüsselungsprogramm explizit von den Benutzern gestartet werden.

Auch wenn einzelne Partitionen komplett verschlüsselt werden, kann dies dazu führen, dass aus verschiedenen Gründen vertrauliche Informationen auf unverschlüsselten Partitionen landen. Daher ist eine vollständige Verschlüsselung von Datenträgern die beste und effizienteste Methode, um vertrauliche Daten zuverlässig vor unbefugtem Zugriff zu schützen.

Datenträgerverschlüsselung lässt sich mit Software, aber auch mit Hardware-Unterstützung umsetzen. Software-Lösungen sind BitLocker von Microsoft oder entsprechende Open-Source-Programme, wie dm-crypt oder Veracrypt.

Mobile Datenträger, wie USB-Sticks und Laptops, sollten möglichst immer vollständig verschlüsselt werden, auch wenn sie nur gelegentlich für vertrauliche Informationen eingesetzt werden. Bei stationären IT-Systemen sollten die Datenträger bei hohem Schutzbedarf bezüglich Vertraulichkeit komplett verschlüsselt werden.

Neben dem Verschlüsselungsprogramm (siehe Abschnitt "Einsatz eines Verschlüsselungsproduktes") selbst sind für die Datenträgerverschlüsselung noch die kryptographischen Schlüssel nötig. Die kryptographischen Schlüssel sollten geeignet erzeugt und getrennt vom verschlüsselten Datenträger aufbewahrt werden. Hierfür können beispielsweise Chipkarten oder USB-Token eingesetzt werden. Eine solche Trennung ist bei der Verschlüsselung von USB-Sticks in der Regel nicht möglich, was bei der Sicherheitsanalyse berücksichtigt werden sollte. Weitere Informationen sind in CON.1 Kryptokonzept zu finden.

Natürlich müssen auch die auf den verschlüsselten Datenträgern gespeicherten Daten regelmäßig gesichert werden.

Einige Programme zur Datenträger- oder Partitionsverschlüsselung oder für den Einsatz von verschlüsselten Dateicontainern bieten die Möglichkeit, die verschlüsselten Bereiche zu "verstecken". Da solche Funktionen schwierig anzuwenden sind und Fehlbedienung zu vollständigem Datenverlust führen kann, sollten sie nur in besonderen Fällen angewendet werden.

Vertiefende Informationen zur Verschlüsselung von Festplatten sind unter [NIST800111] zu finden.

Einsatz eines Verschlüsselungsproduktes

Um zu verhindern, dass aus einem trotz aller Vorsichtsmaßnahmen gestohlenen tragbaren IT-System schutzbedürftige Daten ausgelesen werden können, sollte ein Verschlüsselungsprogramm oder eine vorhandene Betriebssystemfunktion eingesetzt werden. Mit Hilfe der marktgängigen Produkte ist es möglich, einzelne Dateien, bestimmte Bereiche oder die ganze Festplatte so zu verschlüsseln, dass nur derjenige, der über den geheimen Schlüssel verfügt, in der Lage ist, die Daten zu lesen und zu gebrauchen.

Die Sicherheit der Verschlüsselung hängt dabei von drei verschiedenen Punkten zentral ab:

- Der verwendete Verschlüsselungsalgorithmus muss so konstruiert sein, dass es ohne Kenntnis des verwendeten Schlüssels nicht möglich ist, den Klartext aus dem verschlüsselten Text zu rekonstruieren. Nicht möglich bedeutet dabei, dass der erforderliche Aufwand um den Algorithmus zu brechen oder den Klartest zu entschlüsseln in keinem Verhältnis zum dadurch erzielbaren Informationsgewinn seht.
- Der Schlüssel ist geeignet zu wählen. Nach Möglichkeit sollte ein Schlüssel zufällig erzeugt werden.
- Der Verschlüsselungsalgorithmus, die verschlüsselten Dateien und die Schlüssel dürfen nicht zusammen auf einem Datenträger gespeichert werden. Es bietet sich an, den Schlüssel einzeln aufzubewahren. Die kryptographischen Schlüssel sollten auf einem auswechselbaren Datenträger, wie z. B. auf Chipkarte oder USB-Stick, gespeichert werden und getrennt vom tragbaren IT-System aufbewahrt werden (z. B. in der Brieftasche).

Eine Verschlüsselung kann online oder offline vorgenommen werden. Online bedeutet, dass sämtliche Daten der Festplatte (bzw. einer Partition) verschlüsselt werden, ohne dass der Benutzer dies aktiv veranlassen muss. Eine Offline-Verschlüsselung wird explizit vom Benutzer initiiert. Er muss dann auch entscheiden, welche Dateien verschlüsselt werden sollen.

Selbstverschlüsselnde Festplatten

Um zu verhindern, dass Unbefugte an vertrauliche Daten auf Festplatten gelangen können, sollten diese nach Möglichkeit komplett verschlüsselt werden. Es gibt Hard- und Software-basierte Verfahren zur Verschlüsselung, an dieser Stelle wird die hardware-basierte Verschlüsselung in Form von selbstverschlüsselnden Festplatten (englisch: "Self-Encrypting Device", SED) behandelt. SEDs greifen für die Verschlüsselung auf einen speziellen Hardware-Kryptocontroller zu und sind dadurch sehr performant. Die eingesetzten Verschlüsselungslösungen sehen oft nur vor, dass diese nur durch einen Benutzer genutzt werden, Mehr-Benutzer-Lösungen sind im Allgemeinen nicht vorgesehen.

Werden selbstverschlüsselnde Festplatten genutzt, kann das IT-System unter Umständen nicht mehr in den Arbeitsspeicher suspendiert werden, da alle Daten verschlüsselt werden, wenn die Festplatte abgeschaltet wird, und ein im RAM gespeicherter Schlüssel ein Sicherheitsrisiko wäre. Dies ist vor dem Einsatz zu bedenken.

Selbstverschlüsselnde Festplatten sollten nicht mit einem TPM-Modul kombiniert werden, da es bei einer solchen Kombination in der Regel keine Möglichkeit gibt, die Festplatte in einem anderen IT-System mit einem Master-Key zu entschlüsseln. Wird in so einem Fall das IT-System beschädigt, lassen sich die Daten auf der Festplatte nicht mehr entschlüsseln, da die Festplatte durch das TPM-Modul fest mit dem IT-System verwoben ist.

Bei selbstverschlüsselnden Festplatten wird in der Regel AES eingesetzt. Der Schlüssel, mit dem die Informationen verschlüsselt werden, ist der sogenannte "Data Encryption Key" (DEK). Es sollte darauf geachtet werden, dass sich der DEK nur im Kryptocontroller befindet und dieser vor Manipulationen (z.B. Auslesen) besonders geschützt ist. Der DEK sollte auf Basis zufälliger Hardware-Ereignisse generiert werden. Dieser DEK wird mit einem "Authentication Key" (AK) verschlüsselt. Der AK wird typischerweise vom Benutzer durch die Wahl eines Passwortes erzeugt. Bei einigen selbstverschlüsselnden Festplatten kann auch der AK auf einem Token, beispielsweise einer Chipkarte oder einem Stick, gespeichert und zusätzlich mit einem Passwort verschlüsselt werden. Dies ermöglicht die Umsetzung einer Zwei-Faktor-Authentisierung.

Zusätzlich zum DEK und AK gibt es in der Regel auch noch einen Master-Key, der es erlaubt, die Daten zu entschlüsseln, auch wenn das Passwort oder der Token verloren wurde. Ein solcher Schlüssel muss bei der Installation erzeugt und für den Fall, dass das Passwort bzw. der Token verloren geht, sicher aufbewahrt werden. Es muss geregelt werden, wie organisatorisch vorgegangen wird, wenn ein Benutzer das Passwort zu einer verschlüsselten Festplatte vergisst. In diesem Fall muss mit dem Master-Key das Passwort zurückgesetzt werden und der Benutzer ein neues Passwort setzen.

Wenn sich der Benutzer erfolgreich authentisiert hat, wird der DEK entschlüsselt. Mit dem DEK werden alle auf der Festplatte befindlichen Daten ent- und verschlüsselt, ohne dass der Benutzer im Betrieb etwas davon bemerkt. Fährt der Rechner herunter oder wird die Laufwerkseinbindung des SEDs gelöst, werden alle Daten mit dem DEK und der DEK mit dem AK verschlüsselt.

Generell sollte die verwendete Schlüssellänge des von der Festplatte verwendeten Verschlüsselungsverfahrens hinreichend lang sein. Es sollte darauf geachtet werden, dass der Verschlüsselungsalgorithmus in einem für eine Festplattenverschlüsselung sicheren Modus betrieben wird. Ansonsten können beim Entschlüsseln Probleme auftreten, wenn das Chiffrat zwischen zwei Sektoren verschoben wird.

Bevor selbstverschlüsselnde Festplatten beschafft werden, sollte geprüft werden, ob die Festplatten mit der übrigen Hardware des IT-Systems kompatibel sind. Ferner sollte geprüft werden, ob die Schreib- und Leserate der ausgesuchten Festplatte angemessen ist. Überdies sollte geprüft werden, ob weitere Randbedingungen für den Einsatz beim IT-System erfüllt werden müssen. Zum Beispiel lassen sich nur sehr wenige Modelle von selbstverschlüsselnden Festplatten in einer bestehenden "Single-Sign-On"-Architektur integrieren. Auch sollte überprüft werden, ob und wie IT-Systeme mit normalen Festplatten zu selbstverschlüsselnden Festplatten migriert werden können (mit einem mitgelieferten Programm oder über eine Neuinstallation).

Die Installation einer selbstverschlüsselnden Festplatte sollte in Institutionen durch geschulte Administratoren durchgeführt werden. Dafür müssen diese zunächst einen neuen DEK erzeugen und ein Passwort vergeben sowie einen Master-Key erstellen, der sicher aufbewahrt werden muss. Das DEK-Startpasswort muss der Benutzer des Clients als Erstes in ein sicheres Passwort ändern.

Wird eine selbstverschlüsselnde Festplatte repariert oder soll sie verkauft bzw. entsorgt werden, so muss sichergestellt sein, dass sich von ihr keine schützenswerten Informationen entnehmen lassen. Dazu sollte vor Reparatur, Verkauf oder Entsorgung der DEK neu generiert oder ein Löschbefehl "ATA Secure Erase" ausgeführt werden.

SYS.2.1.M29 Systemüberwachung (A)

Um auf kritische Systemereignisse reagieren zu können, sollte für Clients ein geeignetes Systemüberwachungs- bzw. Monitoringkonzept erstellt werden. Dazu gehört, dass Systemzustand und Funktionsfähigkeit der Clients laufend überwacht werden. Wenn Fehler auftreten oder definierte Grenzwerte über- oder unterschritten werden, sollte dies automatisch an das Betriebspersonal gemeldet werden.

Hierfür werden in der Regel Statusinformationen von einem zentralen IT-System abgerufen, auf dem die Ereignisse ausgewertet werden. Über die Schnittstelle, die benötigt wird, um die Systemereignisse vom IT-System abzurufen, können aber oft Systemeinstellungen des Betriebssystems verändert werden, z. B. über SNMP (Simple Network Management Protocol). Ist eine solche Modifikation nicht gewünscht, dann sollten diese Merkmale deaktiviert werden.

SYS.2.1.M30 Einrichten einer Referenzinstallation für Clients (CIA)

Es wird empfohlen, für Clients eine Referenzinstallation zu erstellen, in der die Grundkonfiguration und alle Konfigurationsänderungen, Updates und Patches vor dem Einspielen auf den Clients bei den Anwendern vorab getestet werden können. Dies betrifft die Grundeinstellungen des IT-Systems, Sicherheitspatches und -updates und auch normale Updates, die vom Hersteller herausgegeben werden.

Darüber hinaus kann eine solche Referenzinstallation gegebenenfalls auch dazu genutzt werden, die Installation oder das Wiederaufsetzen von Clients zu vereinfachen, indem eine entsprechend vorkonfigurierte Installation auf geeignete Art und Weise auf den zu installierenden Client überspielt wird ("klonen"). Im Idealfall brauchen anschließend nur noch wenige Einstellungen angepasst zu werden. Eine Referenzinstallation, die zum Klonen von Clients verwendet wird, muss mit besonderer Sorgfalt konfiguriert und getestet werden.

Die Referenzinstallation muss so beschaffen sein, dass die wesentlichen Parameter der Hard- und Softwareplattform für alle IT-Systeme, die von dieser Referenzinstallation abgeleitet werden, dieselben sind. Dies bedeutet nicht notwendigerweise, dass deswegen auf sämtlichen Clients eine identische Hard- und Softwarekonfiguration bestehen muss. Die Konfiguration verschiedener Clients muss aber hinreichend ähnlich sein, damit der Referenzcharakter der Installation erhalten bleibt.

Bei Tests von Anwendungsprogrammen und Einstellungen, die die Anwender auf den Clients betreffen, ist es darüber hinaus besonders wichtig, dass der IT-Betrieb diese nicht mit Administratorrechten durchführen, sondern unter einer Benutzerkennung, der dieselben Berechtigungen besitzt und für den dieselben Einstellungen für die Benutzerumgebung gewählt wurden, wie die Anwender, die mit dem IT-System arbeiten sollen.

Gegebenenfalls kann es vorteilhaft sein, für verschiedene Arten von Tests unterschiedliche Testsysteme zu nutzen, etwa ein oder mehrere IT-Systeme für Tests von Gerätetreibern oder systemnaher Programme und von Betriebssystempatches, und ein anderes für Tests im Zusammenhang mit Anwendungsprogrammen. In einem solchen Fall ist es jedoch wichtig, sich bewusst zu sein, dass auf diese Weise gewisse Arten von Wechselwirkungen zwischen Betriebssystemumgebung und Anwendungsprogrammen nicht abgedeckt werden können. Bei besonderen Anforderungen an die Sicherheit der Clients kann es deswegen erforderlich werden, tatsächlich für bestimmte Einsatzszenarien nur identisch ausgestattete und konfigurierte IT-Systeme einzusetzen.

Für verschiedene typische und häufiger wiederkehrende Testfälle sollten Checklisten erstellt werden, die beim Testen abgearbeitet werden können und die neben der reinen Dokumentation des Tests oft auch zu einer Erhöhung der Effizienz und zur Vermeidung von Fehlern beitragen können.

Alle Tests sollten so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können. Dies ist insbesondere bei Tests von Sicherheitsupdates und von neuen Gerätetreibern notwendig, bei denen eine fehlerhafte Konfiguration oder ein Fehlschlagen der Installation dazu führen kann, dass die betroffenen Clients keinen Zugang mehr zum Netz erhalten oder gar überhaupt nicht mehr starten. Gerade in solchen Fällen kann eine aussagekräftige Dokumentation die notwendige Zeit für die Fehlersuche und -beseitigung wesentlich verkürzen.

SYS.2.1.M31 Einrichtung lokaler Paketfilter (CIA)

Das gesamte Netz einer Institution sollte durch ein entsprechendes Sicherheitsgateway geschützt sein. Zusätzlich ist es empfehlenswert, auch auf jedem Client entsprechende Zugriffsbeschränkungen auf Anwendungs- oder Netzebene einzurichten.

Ein lokaler Paketfilter kann einen Client gegen Angriffe schützen, die aus demselben Subnetz heraus gestartet werden. Außerdem kann ein solcher Paketfilter dazu benutzt werden, eine feiner abgestufte Zugriffskontrolle für einzelne Dienste zu realisieren, als dies beispielsweise mit Paketfiltern nur an Netzübergängen möglich ist.

Darüber hinaus kann ein lokaler Paketfilter auch dazu benutzt werden, ausgehende Netzverbindungen zu beschränken und so die Folgen einer Kompromittierung der IT-Systeme zu begrenzen. Ein solcher Schutz kann zwar eventuell von einem Angreifer nach einer erfolgreichen Kompromittierung des Clients deaktiviert werden, andererseits wird ein Angreifer auf diese Weise zumindest behindert. Auf diese Weise kann entscheidende Zeit bei der Entdeckung und für mögliche Reaktionen gewonnen werden.

Zuletzt kann die Protokollfunktion eines lokalen Paketfilters es ermöglichen, bestimmte Angriffe überhaupt zu entdecken.

Praktisch alle aktuellen Betriebssysteme bieten die Möglichkeit, Filter zu definieren, die alle empfangenen oder zu sendenden Pakete nach bestimmten Regeln untersuchen und behandeln. Die Filtermöglichkeiten unterscheiden sich dabei zwischen den einzelnen Betriebssystemen teilweise erheblich. Praktisch immer können jedoch Regeln basierend auf der Quell- und Zieladresse des Pakets sowie auf dem verwendeten Protokolltyp (TCP/IP, UDP/IP, ICMP etc.) sowie gegebenenfalls dem Quell- oder Zielport definiert werden. Mit Hilfe von Paketfilterregeln können so beispielsweise Pakete, die von bestimmten IT-Systemen oder aus bestimmten Subnetzen stammen, gezielt verworfen werden.

Manche Anwendungen besitzen eigene Mechanismen, um den Zugriff auf den Dienst für einzelne IP-Adressen oder Adressbereiche zu erlauben oder zu verbieten. Gegenüber diesen Mechanismen hat ein lokaler Paketfilter auf Betriebssystemebene den Vorteil, dass er den Dienst selbst gegen mögliche Angriffe schützt, die zu einer Kompromittierung führen, bevor die eingebaute Zugriffsbeschränkung überhaupt wirksam werden kann.

Es gibt zwei allgemeine Strategien, mit der Paketfilter-Regeln implementiert werden können: Die Blacklist-Strategie erlaubt alle Arten von Verbindungen, die nicht bestimmte Ausschlusskriterien erfüllen (Freizügige Strategie: "Alles ist erlaubt, was nicht explizit verboten ist"). Der Vorteil liegt dabei in einem eventuell geringeren Aufwand bei der Administration und der Fehlersuche. Ein schwerwiegender Nachteil ist jedoch, dass vergessene Regeln, die den Zugriff auf nicht geschützte Netzdienste ermöglichen, als Grundlage für einen Angriff dienen können.

Demgegenüber werden bei der Whitelist-Strategie alle Arten von Verbindungen blockiert, die nicht zu einer Liste erlaubter Dienste gehören (Restriktive Strategie: "Alles ist verboten, was nicht explizit erlaubt ist").

Die Whitelist-Strategie bietet die größere Sicherheit und sollte daher grundsätzlich verwendet werden, wenn nicht wichtige Gründe dagegen sprechen. Der Nachteil liegt in einem tendenziell höheren Administrationsaufwand, da bei jeder Änderung der Anforderungen neue Regeln definiert werden müssen. In Ausnahmefällen, beispielsweise wenn ein Protokoll nicht auf fest definierten Ports arbeitet, kann auf die Blacklist-Strategie zurückgegriffen werden.

Es ist empfehlenswert, auf Clients, die besondere Anforderungen an die Sicherheit stellen, im Rahmen der Grundkonfiguration einen lokalen Paketfilter mit einem Basis-Regelwerk einzurichten, bei dem grundsätzlich alle Verbindungsanfragen von außen abgewiesen werden. Dieses Regelwerk sollte aktiv sein, wenn der Client ans Netz angeschlossen wird. Je nachdem, welche Dienste von dem Client genutzt werden sollen, können nach deren Konfiguration die dafür benötigten Protokolle und Ports freigeschaltet werden.

Paketfilter erlauben meist ein detailliertes Protokollieren des Netzverkehrs. Das Aufsetzen eines lokalen Paketfilters ist daher auch in sicheren Netzen, die mit einem Sicherheitsgateway von einem unsicheren Netz wie dem Internet getrennt sind, sinnvoll, denn gewonnen Informationen können für die Erkennung von Angriffen hilfreich sein. Allerdings muss dabei darauf geachtet werden, dass keine Datenschutzbestimmungen verletzt werden. Gegebenenfalls sollten die entsprechenden Stellen (Datenschutzbeauftragter, Personalvertretung oder andere) beteiligt werden.

Problem ICMP

Das Internet Control Message Protocol ICMP wird dazu verwendet, Nachrichten über Fehler bei der Übertragung von IP-Paketen zu übermitteln. Beispielsweise existieren Nachrichten, die dem Sender eines Pakets mitteilen, dass das Zielnetz nicht erreichbar ist oder dass das Paket zu groß war, um an das Zielsystem weitergeleitet zu werden. Die Funktion der Tools ping und traceroute beruhen ebenfalls auf ICMP.

Neben vielen nützlichen Eigenschaften gibt es jedoch einige ICMP-Nachrichtentypen, mit denen Angreifer sich wichtige Informationen über ein Netz verschaffen und diese direkt für Angriffe benutzen können. Leider ist der radikale Ansatz, ICMP grundsätzlich am Sicherheitsgateway zu blockieren, ebenfalls keine befriedigende Lösung, da bestimmte Funktionen dann nicht mehr verfügbar sind. Auf ping und traceroute kann zwar in der Regel auf normalen Arbeitsplatzrechnern und Servern verzichtet werden, eine globale Blockierung von ICMP kann aber zu Beeinträchtigungen führen, die schwer zu diagnostizieren sind. Daher sollte überlegt werden sowohl am Sicherheitsgateway, als auch beim lokalen Paketfilter eine selektive ICMP-Filterung vorzunehmen, sofern dieser die entsprechenden Möglichkeiten zur Verfügung stellt. Dies sollte stets unter der Berücksichtigung des Einsatzzweckes des Clients, dessen Schutzbedarfs und die am Sicherheitsgateway getroffenen Maßnahmen geschehen. Beispielsweise kann für das interne Netz eine größere Zahl von Nachrichtentypen zugelassen werden, als für das externe Netz.

Umsetzung und Überprüfung

Welche Möglichkeiten der Filterung und Protokollierung zur Verfügung stehen, unterscheidet sich je nach Betriebssystem. Vor dem Aufsetzen eines lokalen Paketfilters sollte die vorhandene Dokumentation zu Rate gezogen werden.

Bei der Einrichtung von Paketfilterregeln sollte mit großer Sorgfalt vorgegangen werden, da ein Fehler in einer Regel unter Umständen dazu führen kann, dass sich ein Administrator, der über das Netz auf dem Client arbeitet, auf diese Weise "aussperrt" und die Korrekturen von der Systemkonsole aus vornehmen muss.

Nach dem Aktivieren des lokalen Paketfilters sollte einerseits geprüft werden, ob die benötigten Dienste noch erreichbar sind, andererseits sollte mit einem Portscan überprüft werden, ob die restlichen Ports alle blockiert sind.

SYS.2.1.M32 Einsatz zusätzlicher Maßnahmen zum Schutz vor Exploits (CIA)

Je nachdem, welche Sicherheitsanforderungen an ein IT-System gestellt werden, reichen eventuell die vorhandenen Sicherheitsfunktionalitäten nicht aus, so dass zusätzlich geeignete Sicherheitsprodukte eingesetzt werden sollten. Typische Beispiele dafür sind Zugangskontrolle, Zugriffsrechteverwaltung und -prüfung, Protokollierung oder Verschlüsselung.

Bei IT-Systemen muss beispielsweise sichergestellt werden, dass

- nur autorisierte Personen das IT-System benutzen können. Hierfür sind geeignete Authentisierungsmechanismen auszuwählen.
- die Benutzer auf die Daten nur in der Weise zugreifen können, die sie zur Aufgabenerfüllung benötigen. Hierbei unterstützen geeignete Benutzertrennung und Rechtevergabe.
- Unregelmäßigkeiten und Manipulationsversuche erkennbar werden. Hierbei helfen Protokollierungsfunktionen, Verschlüsselung und digitale Signatur.
- Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle). Hierbei unterstützen beispielsweise Backup-Programme.

Reichen die Protokollierungsmöglichkeiten des IT-Systems nicht aus, um eine ausreichende Beweissicherung zu gewährleisten, so müssen diese nachgerüstet werden. Hierzu gibt es auch verschiedene Gesetze, die dies erfordern. Beispielsweise ist nach BDSG bei der Eingabekontrolle "zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind".

Ist es mit dem IT-System nicht möglich, den Administrator daran zu hindern, auf bestimmte Daten zuzugreifen oder zumindest diesen Zugriff zu protokollieren und zu kontrollieren, dann kann z. B. mit einer Verschlüsselung der Daten verhindert werden, dass der Administrator diese Daten im Klartext liest, wenn er nicht im Besitz des zugehörigen Schlüssels ist.

Empfohlene Mindestfunktionalitäten

IT-Systeme sollten mindestens die folgenden Sicherheitseigenschaften besitzen. Wenn diese nicht im Standardumfang vorhanden sind, sollten diese über zusätzliche Sicherheitsprodukte nachgerüstet werden.

- Identifikation und Authentisierung: Es sollte eine Sperre des IT-Systems nach einer vorgegebenen Anzahl fehlerhafter Authentisierungsversuche stattfinden, die nur der IT-Betrieb zurücksetzen kann. Wird ein Passwort verwendet, sollte das Passwort mindestens acht Stellen umfassen und dürfen nicht unverschlüsselt in den IT-Systemen gespeichert werden.
- Rechteverwaltung und -kontrolle: Es sollte eine Rechteverwaltung und -kontrolle auf Festplatten und Dateien vorhanden sein, wobei zumindest zwischen lesendem und schreibendem Zugriff unterschieden werden soll. Für Benutzer sollte kein Systemzugriff auf Betriebssystemebene möglich sein.
- Rollentrennung zwischen Administrator und Benutzer: Es sollte eine klare Trennung zwischen Administrator und Benutzer möglich sein, wobei nur der Administrator Rechte zuweisen oder entziehen können sollte.
- Protokollierung der Vorgänge Anmelden, Abmelden und Rechteverletzung sollte möglich sein.

Sollte ein oder mehrere dieser Sicherheitsfunktionalitäten nicht vom Betriebssystem unterstützt werden, so müssen ersatzweise geeignete zusätzliche Sicherheitsprodukte eingesetzt werden.

Zusätzliche Forderungen an Sicherheitsprodukte:

- Benutzerfreundliche Oberfläche zur Erhöhung der Akzeptanz.
- Aussagekräftige und nachvollziehbare Dokumentation für IT-Betrieb und Benutzer.

Wünschenswerte Zusatzfunktionalität von Sicherheitsprodukten:

- Rollentrennung zwischen Administrator, Revisor und Benutzer; nur der Administrator kann Rechte zuweisen oder entziehen und nur der Revisor hat Zugriff auf die Protokolldaten,
- Protokollierung von Administrationstätigkeiten,
- Unterstützung der Protokollauswertung durch konfigurierbare Filterfunktionen,
- Verschlüsselung der Datenbestände mit einem geeigneten Verschlüsselungsalgorithmus und in einer Weise, dass ein Datenverlust bei Fehlfunktion (Stromausfall, Abbruch des Vorgangs) systemseitig abgefangen wird.

Die Realisierung dieser Funktionalität kann sowohl in Hardware wie auch in Software erfolgen. Bei der Neubeschaffung eines Produktes sollte der Baustein OPS.1.2.6 Beschaffung, Ausschreibung und Einkauf berücksichtigt werden.

Übergangslösung

Sollte es nicht möglich sein, kurzfristig ein geeignetes Sicherheitsprodukt zu beschaffen, sind andere geeignete Sicherheitsmaßnahmen zu ergreifen. Diese sind dann typischerweise organisatorischer Natur und müssen von den Benutzern konsequent eingehalten werden. Wenn ein IT-System beispielsweise keine Bildschirmsperre hat, muss dieses in den kurzen Phasen, wo es nicht benutzt wird, ein- oder weggeschlossen werden.

SYS.2.1.M33 Application Whitelisting (CIA)

Grundsätzlich müssen Clients nur Anwendungen ausführen können, die dafür notwendig sind, dass die angebotenen Dienste funktionieren. Entsprechende Whitelist-Lösungen können sicherstellen, dass nur erlaubte Programme ausgeführt werden können. Es gibt hier betriebssystemeigene Mechanismen und Lösungen von Drittanbietern, die zur Umsetzung von Whitelisting infrage kommen.

Ein einfacher Ansatz ist pfadbasiertes Application Whitelisting für vollständige Pfade, bei dem z. B. Programmverzeichnisse oder Verzeichnisse mit Betriebssystemdateien erlaubt werden. So kann verhindert werden, dass etwa ein Schadprogramm aus dem Browser-Cache oder einem temporären Ordner heraus ausgeführt wird.

Alternativ kann explizit einzelnen Anwendungen die Ausführung gestattet werden. Dieser Ansatz erhöht die Sicherheit zusätzlich, da nur vorab festgelegte Anwendungen gestartet werden können. Gleichzeitig erhöht sich aber auch der Aufwand, da z. B. sichergestellt werden muss, dass alle nötigen Betriebssystemkomponenten ausgeführt werden können. Auch bei Updates ist zusätzlicher Aufwand nötig, um geänderte Programme in der Whitelist nachzupflegen.

Bei Whitelisting ist zu beachten, dass z.B. auch Skripte nicht ausgeführt werden dürfen.

SYS.2.1.M34 Einsatz von Anwendungsisolation (CIA)

Die verschiedenen Betriebssysteme bieten unterschiedliche Möglichkeiten, um Anwendungen zu isolieren. Hierzu zählen Container-Lösungen wie AppContainer (Windows), Linux Containers (LXC) oder Docker wie auch mit den Betriebssystemen mitgelieferte Virtualisierungslösungen wie Hyper-V (Windows), KVM/Xen (Linux), VMware Workstation oder Virtualbox. Darüber hinaus können spezialisierte Lösungen von Drittherstellern genutzt werden. Dies hat den Vorteil, dass Anwendungen, mit denen Internetinhalte oder Daten von externen Stellen geöffnet werden, einen deutlichen Sicherheitsgewinn durch eine Isolation erhalten können. Dies umfasst z. B. Webbrowser, Office-Anwendungen, E-Mail-Programme und PDF-Betrachter.

SYS.2.1.M35 Aktive Verwaltung der Wurzelzertifikate (CI)

Weitere Informationen zur Verwaltung von Wurzelzertifikaten befinden sich in den folgenden Dokumenten:

- Windows: Configure Trusted Roots and Disallowed Certificates [MSROOT
- Mozilla: CA:Root Change Process [MOZRCP]
- Java: keytool - Key and Certificate Management Tool [KEYTOOL]
- OpenSSL: Certificate Installation with OpenSSL [OPENSSL]
- GnuPG: Agent Configuration - Using the GNU Privacy [GNUPG]

SYS.2.1.M36 Selbstverwalteter Einsatz von SecureBoot und TPM (CI)

Auf UEFI-kompatiblen Systemen sollten Bootloader, Kernel sowie alle benötigten Firmware-Komponenten durch selbstkontrolliertes Schlüsselmaterial signiert und nicht benötigtes Schlüsselmaterial entfernt werden. Sofern das TPM nicht benötigt wird, sollte es deaktiviert werden.

SYS.2.1.M37 Schutz vor unbefugten Anmeldungen (CIA)

Um einen Zugang zum System durch kompromittierte Anmeldeinformationen zu verhindern, sollte eine Mehrfaktorauthentisierung verwendet werden.

SYS.2.1.M38 Einbindung in die Notfallplanung (A)

Im Rahmen der Notfallvorsorge ist ein Konzept zu entwerfen, wie die Folgen eines Ausfalls minimiert werden können und welche Aktivitäten im Falle eines Ausfalls durchzuführen sind.

Folgende Aspekte müssen dabei berücksichtigt werden:

- Die Notfallplanung für die Clients sollte in den existierenden Notfallplan integriert werden (siehe auch Baustein DER.4 Notfallmanagement).
- Durch einen Systemausfall können Daten verloren gehen. Daher ist im Rahmen des allgemeinen Datensicherungskonzepts (siehe auch OPS.1.1.5 Datensicherung) ein Datensicherungskonzept für die Clients zu erstellen.
- Im Rahmen von Wartungs- und Serviceverträgen oder durch eigene Lagerhaltung muss die Versorgung mit Ersatzteilen innerhalb einer Frist sichergestellt werden.
- Die Systemkonfiguration muss dokumentiert werden. Wichtige Aufgaben müssen so beschrieben sein, dass das Gesamtsystem im Notfall auch ohne vorherige Kenntnis dieser Systemkonfiguration wiederhergestellt werden kann.

Erstellen eines Notfall-Bootmediums

Wird ein Client eingerichtet, sollte direkt ein Bootmedium erstellt werden. Auf diese Weise kann das IT-System gestartet werden, wenn eine Festplatte ausfällt, außerdem kann es genutzt werden, um einen kontrollierten Systemzustand wieder herzustellen, nachdem z.B. ein Schadprogramm aufgetreten ist. Solche Medien können beispielsweise DVDs sein, die vom jeweiligen Betriebssystem erstellt werden, es können aber auch eigens eingerichtete DVDs oder portable Laufwerke (beispielsweise USB-Sticks oder externe Festplatten) erstellt werden. Art und Umfang des Notfall-Bootmediums richten sich nach dem Einsatzzweck des Clients und den vorhandenen Schnittstellen.

Das Notfall-Bootmedium kann unter anderem bei folgenden Problemen eingesetzt werden:

- Datenverlust durch Fehlbedienung,
- Bedienungs- und Administrationsfehler, die die Benutzung und einen Neustart verhindern,
- Infektion des IT-Systems mit Schadprogrammen (beispielsweise Computer-Viren),
- Kompromittierung des IT-Systems durch einen Angreifer, oder auch
- Hardware-Probleme.

Idealerweise sollte das Notfall-Bootmedium alle Programme und Daten enthalten, die benötigt werden, um das IT-System untersuchen und um Probleme beseitigen zu können. Gegebenenfalls können unterschiedliche Medien für verschiedene Problemszenarien erstellt werden.

Als "Grundausstattung" für ein Notfall-Bootmedium werden folgende Programme empfohlen:

- Viren-Schutzprogramme mit aktuellen Signaturen,
- Programme zur Bearbeitung von Konfigurationsdateien oder Datenbanken des IT-Systems (Editoren für Dateien, Registry oder ähnliches),
- Programme zur Wiederherstellung von Datenstrukturen der Systemfestplatte wie Bootsektor und MBR (Master Boot Record) oder GPT (GUID Partition Table),
- Backup- / Recovery-Programme,
- Diagnoseprogramme zur Analyse von Hardware-Defekten.

Darüber hinaus können Programme zur weitergehenden Analyse hinzugefügt werden, etwa um kompromittierte IT-System forensisch zu untersuchen.

Dabei ist es wichtig, dass alle Programme und Bibliotheken ausschließlich vom Bootmedium geladen werden. Es dürfen keine Komponenten des installierten IT-Systems verwendet werden. Wird ein Bootmedium erstellt, istaußerdem darauf zu achten, dass neben den notwendigen Programmen auch alle Treiber vorhanden sind, die für den Zugriff auf die eingebauten Platten des Clients benötigt werden. Dazu zählen beispielsweise Treiber für Festplattencontroller (insbesondere RAID-Controller) und Treiber für eine Festplattenverschlüsselung oder Festplattenkomprimierung.

Falls das Bootmedium genügend Speicherplatz bietet, können weitere Programme oder Dokumentation auf dem Medium gespeichert werden. Beispielsweise kann es die Effizienz der Fehlersuche erhöhen, wenn auf dem Bootmedium stets eine aktuelle Dokumentation der Systemkonfiguration enthalten ist.

Das Notfall-Bootmedium muss selbst frei von Viren und anderen Schadprogrammen sein. Es dürfen deshalb nur Programme eingesetzt werden, die aus vertrauenswürdigen Quellen (etwa direkt von der CD/DVD des Herstellers) stammen oder deren digitale Signatur überprüft wurde. Nachdem das Bootmedium erstellt und nachdem es geändert wurde, sollte es außerdem mit einem Viren-Schutzprogramm überprüft werden.

Es ist nicht unbedingt notwendig, für jedes IT-System ein eigenes Bootmedium zu erstellen. Ein entsprechend flexibel angelegtes Bootmedium kann für eine große Anzahl verschiedener IT-Systeme ausreichend sein. Auf dem Bootmedium braucht nicht einmal notwendigerweise dasselbe Betriebssystem eingesetzt zu werden, wie auf dem Zielsystem selbst. Aus Gründen der Kompatibilität ist dies jedoch oft vorteilhaft. Es muss allerdings unbedingt durch entsprechende Tests sichergestellt werden, dass das Medium auch wirklich bei allen Clients funktioniert, für die es eingesetzt werden soll. Je nach Betriebssystem müssen außerdem noch systemspezifische Aspekte beachtet werden, die in den jeweiligen IT-Grundschutz-Bausteinen beschrieben werden.

Wurde das Zielsystem verändert, etwa nach einem Update des Betriebssystems oder Konfigurationsänderungen, muss gegebenenfalls das Notfall-Bootmedium und die darauf gespeicherte Dokumentation aktualisiert werden. Wird das Bootmedium geändert, muss dies dokumentiert werden.

Das Notfall-Bootmedium muss für die Systembetreuer schnell greifbar sein, damit im Falle einer Störung nicht wertvolle Zeit verloren geht. Andererseits muss es auch so sicher aufbewahrt werden, dass Unbefugte keinen Zugriff darauf haben.

Die Funktion des Notfall-Bootmediums sollte regelmäßig getestet und die Bedienung der darauf gespeicherten Programme geübt werden, damit sichergestellt ist, dass das Medium im Fall von Problemen funktioniert und der IT-Betrieb mit der Bedienung vertraut sind. Es sollte überlegt werden, mit dem Medium eine kurze gedruckte Anleitung aufzubewahren, die für typische Einsatzszenarien die wichtigsten Schritte zusammenfasst.

SYS.2.1.M39 Unterbrechungsfreie und stabile Stromversorgung [Haustechnik] (A)

Wenn es bei Clients erhöhte Anforderungen an die Verfügbarkeit gibt, sollten diese an eine unterbrechungsfreie Stromversorgung (USV) angeschlossen werden, damit Stromausfälle solange überbrückt werden können, bis entweder die (Ersatz-) Energieversorgung wieder sichergestellt ist oder die Clients geordnet heruntergefahren sind. Vertiefende Informationen zu einer unterbrechungsfreien und stabilen Stromversorgung sind in dem Baustein und den Umsetzungshinweisen zum SYS.1.1 Allgemeiner Server zu finden.

SYS.2.1.M40 Betriebsdokumentation (A)

Um einen reibungslosen Betriebsablauf zu gewährleisten, müssen Administratoren einen Überblick über die IT-Systeme haben bzw. sich verschaffen können. Dieses muss auch für deren Vertreter möglich sein, falls ein Administrator unvorhergesehen ausfällt. Der Überblick wird oft vorausgesetzt, um die IT-Systeme (z. B. auf problematische Einstellungen, Konsistenz bei Änderungen) prüfen zu können.

Daher sollten die Veränderungen, die Administratoren an den IT-Systemen vornehmen, dokumentiert werden, nach Möglichkeit automatisiert. Dieses gilt insbesondere für Änderungen an Systemverzeichnissen und -dateien.

Bei Installation neuer Betriebssysteme oder bei Updates sind die vorgenommenen Änderungen besonders sorgfältig zu dokumentieren. Indem neue Systemparameter aktiviert oder bestehende geändert werden, kann das Verhalten eines IT-Systems (insbesondere auch Sicherheitsfunktionen) maßgeblich verändert werden.

SYS.2.1.M41 Verhinderung der Überlastung der lokalen Festplatte (A)

Es sollte überlegt werden, Quotas einzurichten. Alternativ sollten Mechanismen des verwendeten Datei- oder Betriebssystemsystems genutzt werden, die die Benutzer bei einem bestimmten Füllstand der Festplatte warnen oder nur noch dem Systemadministrator Schreibrechte einräumen.

3 Weiterführende Informationen

3.1 Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Allgemeiner Client" finden sich unter anderem in folgenden Veröffentlichungen:

[BSITLS] Migration auf TLS 1.2 Handlungsleitfaden

Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 1.2, Juni 2016, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Migrationsleitfaden_Mindeststandard_BSI_TLS_1_2_Version_1_2.pdf, zuletzt abgerufen am 06.09.2018

[GNUPG] Using the GNU Privacy Guard

Agent Configuration, https://www.gnupg.org/documentation/manuals/gnupg/Agent-Configuration.html , zuletzt abgerufen am 06.09.2018

[ISiClient] Whitepaper Absicherung eines PC-Clients (ISi-Client)

Bundesamt für Sicherheit in der Informationstechnik (BSI), 2011, https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-Client/client_node.html , zuletzt abgerufen am 05.09.2018

[KEYTOOL] keytool - Key and Certificate Management Tool

Oracle, https://docs.oracle.com/javase/6/docs/technotes/tools/windows/keytool.html , zuletzt abgerufen am 06.09.2018

[MOZRCP] Mozilla CA: Certificate Change Process: Mozilla Wiki

https://wiki.mozilla.org/CA:Root_Change_Process, zuletzt abgerufen am 28.08.2018

[MSROOT] Configure Trusted Roots and Disallowed Certificates

Microsoft, https://technet.microsoft.com/en-us/library/dn265983(v=ws.11).aspx , zuletzt abgerufen am 06.09.2018

[NIST800111] Guide to Storage Encryption Technologies for End User Devices

NIST Special Publication 800-111, November 2007, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf , zuletzt abgerufen am 06.09.2018

[NISTSP800123] Guide to General Server Security

NIST Special Publication 800-123, Juli 2008, https://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf , zuletzt abgerufen am 05.09.2018

[OPENSSL] Certificate Installation with OpenSSL - Other People´s Certificates

http://gagravarr.org/writing/openssl-certs/others.shtml , zuletzt abgerufen am 06.09.2018

[RFC5246] The Transport Layer Security (TLS) Protocol

RFC 5246, Internet Engineering Task Force (IETF), June 1969, https://tools.ietf.org/html/rfc5246 , zuletzt abgerufen am 06.09.2018

[RFC5746] Transport Layer Security (TLS) Renegotiation Indication Extension

RFC 5746, Internet Engineering Task Force (IETF), Februar 2010, https://tools.ietf.org/html/rfc5746 , zuletzt abgerufen am 06.09.2018

[TR02102] Kryptographische Verfahren

Empfehlungen und Schlüssellängen: BSI TR-02102, Bundesamt für Sicherheit in der Informationstechnik (BSI), Januar 2018, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html , zuletzt abgerufen am 13.09.2018

Umsetzungshinweise zum Baustein SYS.2.4 Clients unter macOS

1 Beschreibung

1.1 Einleitung

macOS ist ein Client-Betriebssystem der Firma Apple. macOS basiert auf Darwin, dem frei verfügbaren Unix-Betriebssystem von Apple, das wiederum auf FreeBSD aufbaut. macOS setzt sich im Wesentlichen aus Darwin sowie der proprietären grafischen Oberfläche Aqua und weiteren Anwendungen und Diensten zusammen. Gemäß den Lizenzbedingungen von Apple darf macOS nur auf IT-Systemen ("Macs") von Apple installiert werden, weshalb Eigenheiten dieser Systeme ebenfalls Bestandteil des Bausteins sind

Die Sicherheit eines Betriebssystems spielt eine wichtige Rolle für die Sicherheit in einem Informationsverbund. Schwachstellen auf der Betriebssystemebene können die Sicherheit aller Anwendungen und aller IT-Systeme des gesamten Netzes beeinträchtigen.

1.2 Lebenszyklus

Planung und Konzeption

Die geregelte und sichere Einführung von macOS setzt eine umfangreiche Planung voraus. Details dazu finden sich in SYS.2.4.M1 *Planung des sicheren Einsatzes von macOS*.

Beschaffung

macOS darf nur auf IT-Systemen von Apple verwendet werden. Ein wichtiger Aspekt ist hierbei die Unterstützung des Geräts mit Sicherheitsupdates durch den Hersteller, siehe hierzu SYS.2.4.M6 *Verwendung aktueller Hardware*.

Umsetzung

Die sichere Konfiguration von macOS berührt zahlreiche Punkte, von der Nutzung von integrierten Sicherheitsmechanismen (siehe SYS.2.4.M2 *Nutzung der integrierten Sicherheitsfunktionen von macOS*, SYS.2.4.M4 *Verwendung der Festplattenverschlüsselung* oder SYS.2.4.M10 *Aktivierung der Personal Firewall*) bis zur zielgerichteten Benutzerverwaltung (siehe SYS.2.4.M3 *Verwaltung der Benutzerkonten*).

Betrieb

Beim Betrieb eines Macs sind weitere Aspekte zu beachten, die auch den Benutzer betreffen. So sollten die verwendeten Apple IDs geeignet abgesichert werden, siehe SYS.2.4.M7 *Zwei-Faktor-Authentisierung für Apple-ID*. Außerdem sollte darauf geachtet werden, ob auf dem Mac verarbeitete Daten das Gerät unbeabsichtigt verlassen, vergleiche SYS.2.4.M8 *Keine Nutzung von iCloud für sensible Daten*.

Aussonderung

Bei der Aussonderung eines Macs sind neben den üblichen Schritten wie Datenlöschung auch Aspekte zu beachten, die spezifisch für Apple-Geräte sind, siehe hierzu SYS.2.4.M11 *Geräteaussonderung*.

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Clients unter macOS" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

SYS.2.4.M1 Planung des sicheren Einsatzes von macOS

Die geregelte und sichere Einführung von macOS setzt eine umfangreiche Planung voraus. In dieser Maßnahme wird auf softwaretechnische Aspekte eingegangen, um eine reibungslose Projektumsetzung zu ermöglichen. Die verwendeten Hardwarekomponenten in einem macOS-System sind von Apple vorgegeben.

Einführung sowie Plattformwechsel

Bei einem Plattformwechsel von einem anderen Betriebssystem zu macOS muss im Vorfeld geprüft werden, ob gleiche oder gleichwertige Anwendungen für macOS zur Verfügung stehen und ob diese zu bestehenden Systemen kompatibel sind. Dies betrifft nicht nur die Anwendungen, die direkt auf dem Client betrieben werden, sondern auch serverbasierte Anwendungen mit bestimmten Voraussetzungen. Zum Beispiel benötigen bestimmte webbasierte Anwendungen Technologien (z. B. ActiveX, Java), die unter macOS möglicherweise nicht oder nur eingeschränkt Verfügung stehen. Vorhandene Software, die nicht kompatibel zu macOS ist, kann beispielsweise mithilfe einer Software-Virtualisierungslösung betrieben werden. Jedoch ist dies nur als Notlösung anzusehen, da erhöhte Ansprüche an die Hardware gestellt werden und es um ein Vielfaches komplexer ist, eine Anwendung in einer virtualisierten Umgebung zu betreiben.

Generell muss geprüft werden, ob bestehende Software-Lizenzverträge auch macOS-Systeme abdecken. Falls nicht, muss in zukünftigen Lizenzverträgen darauf geachtet werden, dass Software gewählt wird, die auf verschiedenen Plattformen betrieben werden kann bzw. deren Lizenzverträge den Einsatz auf anderen Plattformen gestatten.

Bei der Einführung von macOS-Systemen muss ebenfalls geprüft werden, ob bestehende externe Hardware, wie zum Beispiel Drucker, Kartenlesegeräte oder sonstige benötigte Geräte kompatibel zu macOS sind und entsprechende Gerätetreiber zur Verfügung stehen. Ebenfalls muss geprüft werden, ob die eingesetzten Netzprotokolle von macOS unterstützt werden, um eine Verbindung zwischen unterschiedlichen Systemen herstellen zu können. Wird zum Beispiel das "Andrew File System"-Protokoll (AFS) als verteiltes Netz-Dateisystem verwendet, muss im Vorfeld ein geeigneter Client für macOS gewählt werden.

Benutzerkonzept

Im Vorfeld der Einführung von macOS ist ein Benutzerkonzept zu erstellen, falls es noch nicht vorhanden ist. Es legt fest, mit welchen Rechten die Benutzer bestimmte Arbeiten verrichten können. Bei der Planung des Benutzerkonzepts ist zwischen lokalen und domänenweiten Benutzerkonten zu unterscheiden. Sowohl bei lokalen als auch bei domänenweiten Benutzerkonten ist darauf zu achten, dass die Benutzerrechte möglichst restriktiv gewählt werden. So wird das mögliche Schadensmaß bei einer absichtlichen oder versehentlichen missbräuchlichen Nutzung des Benutzerkontos begrenzt. Unter macOS ist für jeden Benutzer ein Konto mit Standardbenutzer-Rechten einzurichten, das zum täglichen Arbeiten verwendet werden muss.

Wenn die Clients unter macOS in einen Verzeichnisdienst integriert werden, muss der Baustein APP.2.1 *Allgemeiner Verzeichnisdienst* beachtet werden. Falls es sich um ein heterogenes Netz mit einem Windows-Server als Basis des Verzeichnisdienstes handelt, ist auch der Baustein APP.2.2 *Active Directory* zu beachten.

Administrationskonzept

Im Vorfeld der Einführung von macOS ist ein Administrationskonzept zu erstellen, falls es noch nicht vorhanden ist. Es sind grundsätzlich zwei verschiedene Konten für die Administration vorgesehen.

macOS unterscheidet zwischen Benutzer- und Administratorenkonten. Ein Benutzer, der unter einem Benutzerkonto angemeldet ist, kann keine Systemeinstellungen verändern, Applikationen in allgemein zugängliche Verzeichnisse installieren oder andere Benutzerkonten verwalten. Administratoren haben hingegen diese genannten Möglichkeiten. Soweit möglich, müssen die Administratoren für ihre Arbeit ein Konto mit den Privilegien eines Standardbenutzers verwenden. Nur wenn diese Privilegien nicht mehr ausreichend sind, kann ein Konto mit administrativen Privilegien genutzt werden. Bei macOS sind Aufgaben, die die erweiterten Rechte eines Administrators erfordern, durch das Symbol eines kleinen Vorhängeschlosses gekennzeichnet. Bei Klick auf das Schloss werden die Zugangsdaten des Administrators abgefragt, danach sind Änderungen mit administrativen Privilegien möglich. Nach der Erfüllung der Aufgaben muss sich der Administrator durch einen weiteren Klick auf das Symbol wieder vom Konto mit administrativen Privilegien abmelden und mit dem Standardbenutzerkonto weiterarbeiten.

Als Besonderheit existiert bei macOS zudem ein root-Konto, das in der Standardeinstellung deaktiviert ist. Außerdem ist für das root-Konto standardmäßig kein Passwort gesetzt. Administratoren- und root-Konto unterscheiden sich dahingehend, dass ein Administratorkonto keine Berechtigung besitzt, um Informationen aus wichtigen Systemordnern zu löschen. Somit kann ein Administrator zwar viele Änderungen am System vornehmen, aber nicht das gesamte Betriebssystem komplett unbrauchbar machen. Es ist jedoch möglich, mit einem Administratorenkonto das root-Konto zu aktivieren und zu nutzen. Die Deaktivierung des root-Kontos stellt also nur einen unvollständigen Schutz gegen das unbeabsichtigte Löschen von Systemdateien dar. In der Standard-Konfiguration verhindert macOS durch die sogenannte System Integrity Protection (SIP) jedoch einen tiefgehenden Zugriff durch das root-Konto. Aufgrund von Sicherheitsproblemen in der Vergangenheit (vgl. CVE-2017-13872) ist es zusätzlich empfehlenswert, für das root-Konto ein sicheres Passwort festzulegen, auch wenn es nicht verwendet werden bzw. deaktiviert bleiben soll.

Protokollierungskonzept

Um Angriffe oder Unregelmäßigkeiten erkennen zu können, müssen die Protokollierungsmöglichkeiten des einzelnen Systems aktiviert und benutzt werden. Um sinnvoll zu protokollieren, muss im Vorfeld überlegt werden, welche Programme auf dem Client unter macOS eine bedeutende Rolle einnehmen. Allen geschäftskritischen Anwendungen muss ein möglichst hohes Log-Level zugeordnet werden, dadurch können insbesondere alle (Warn-) Meldungen protokolliert werden. In einem Störfall stehen dann genug Informationen zur Fehlerbeseitigung zur Verfügung. Wird ein Client zum Beispiel hauptsächlich zum Versenden von E-Mail-Nachrichten verwendet, sollten jegliche Hinweise bezüglich des E-Mail-Programms an eine zentrale Stelle weitergeleitet und ausgewertet werden. Grundsätzlich sollte der Baustein OPS.1.1.5 *Protokollierung* berücksichtigt werden.

Datenablage, Datensicherung und Verschlüsselung

Es ist festzulegen, wo die Benutzerdaten gespeichert werden. Werden alle relevanten Daten auf Servern gespeichert, so kann auf eine lokale Datensicherung verzichtet werden. Im Gegensatz dazu müssen Datensicherungen zentral durchgeführt werden. Dieses Vorgehen ist jedoch stark von den lokalen Gegebenheiten abhängig. Wird zum Beispiel auf einem Client spezielle Software eingesetzt, die nach einem Defekt nur mit hohem Arbeitsaufwand wieder in Betrieb genommen werden kann, muss eine Datensicherung des Clients in regelmäßigen Zyklen erfolgen. Weitere Informationen zum Thema Datensicherung finden sich im Baustein CON.3 *Datensicherungskonzept*.

Werden mobile Macs eingesetzt, müssen (temporär) die Informationen oft lokal abgelegt werden. Somit muss die clientseitige Datenablage und ihr (kryptographischer) Schutz geplant werden.

Grundsätzlich sollte die gesamte Festplatte eines Macs verschlüsselt werden.

Sicherheitsrichtlinie

Eine der wichtigsten organisatorischen Aufgaben bei der Einführung von macOS ist es, eine entsprechende Sicherheitsrichtlinie für macOS zu planen und zu definieren. Diese Richtlinie legt die später umzusetzenden Sicherheitsbestimmungen für macOS Clients fest. Die Sicherheitsrichtlinie muss allen Anwendern und anderen Personen, die an der Beschaffung und dem Betrieb der Clients beteiligt sind, bekannt und Grundlage für deren Arbeit sein. Wie bei allen Richtlinien sind ihre Inhalte und ihre Umsetzung im Rahmen einer übergeordneten Revision regelmäßig zu prüfen.

Die in der macOS-Sicherheitsrichtlinie definierten Anforderungen werden durch die entsprechenden Sicherheitseinstellungen auf Betriebssystemebene umgesetzt. In Fällen, in denen technische Maßnahmen nicht ausreichen, müssen sie durch zusätzliche organisatorische Maßnahmen begleitet und unterstützt werden. Nach Möglichkeit kann eine technische Lösung gegenüber einer organisatorischen vorgezogen werden

Die zu erstellende Sicherheitsrichtlinie hat sich an den bisher geltenden Sicherheitsrichtlinien der jeweiligen Institution zu orientieren und darf diesen nicht widersprechen. In der Regel werden die existierenden Regelungen für macOS angepasst oder sinngemäß erweitert. Dabei sind insbesondere spezifische Funktionen von macOS wie beispielsweise FileVault und Time Machine zu berücksichtigen. Generell gilt, dass sich die Planung der macOS-Infrastruktur an der jeweiligen übergreifenden Sicherheitsrichtlinie orientiert. Die Infrastruktur beeinflusst jedoch über einen Feedback-Prozess diese übergreifende Sicherheitsrichtlinie. Nicht zuletzt ist beim Erstellen der Sicherheitsrichtlinie darauf zu achten, dass geltende rechtliche Bestimmungen berücksichtigt werden. Die Sicherheitsrichtlinie für macOS ist zu dokumentieren und den Benutzern des Client-Server-Netzes im erforderlichen Umfang mitzuteilen. Alle Administratoren müssen die Sicherheitsrichtlinie kennen und umsetzen.

Datensicherung und Wiederherstellung von macOS Clients

Damit Daten im Bedarfsfall wiederhergestellt werden können, müssen regelmäßige Backups angelegt werden. Darüber hinaus muss jedes angelegte Backup verschlüsselt werden. Hierzu kann die in macOS integrierte Funktion "Time Machine" oder eine Drittanbieterlösung verwendet werden.

"Time Machine" steht bereits bei einer Standardinstallation von macOS zur Verfügung. Time Machine lässt sich auch von den Benutzern leicht konfigurieren, mit dem Programm können vollständige Festplatten gesichert werden.

Im ersten Schritt erzeugt Time Machine eine vollständige Kopie der zu sichernden Informationen, anschließend werden nur noch Informationen gesichert, die seit der letzten Datensicherung verändert wurden oder neu hinzugekommen sind (inkrementelle Datensicherung).

Werden die Informationen mit Time Machine gesichert, sollten folgende Punkte beachtet werden:

- Die Daten auf den Sicherungsmedien sind standardmäßig unverschlüsselt. Das Backup muss daher verschlüsselt oder vor unbefugtem Zugriff geschützt aufbewahrt werden.
- Die gesicherten Informationen werden nicht komprimiert und können mehr als den eingeplanten Speicherplatz belegen.
- Eine vollständige Wiederherstellung der gespeicherten Daten kann zeitintensiv sein.
- Die Datensicherung erfolgt automatisch alle 30 Minuten nach dem Start des IT-Systems. Allerdings können Benutzer ein Backup manuell zu jedem Zeitpunkt auslösen.
- Es können bei einer Sicherung über ein Datennetz ohne zusätzliche Systemeingriffe nur spezielle Network-Attached-Storage-Systeme (NAS) genutzt werden.

Aufgrund dieser und weiterer limitierender Faktoren ist der Einsatz von Time Machine prinzipiell nur beschränkt zu empfehlen und stark abhängig von den lokalen Gegebenheiten. Bei der Wahl einer Datensicherungssoftware in heterogenen Umgebungen wird empfohlen, ein Programm zur Datensicherung einzusetzen, das mehrere Plattformen wie macOS, Windows und Linux unterstützt.

Mit Time Machine können Datensicherungen auf externen Datenträgern, anderen macOS Systemen oder auf einem internen Datenträger, von dem das System nicht gestartet wurde, abgelegt werden. Sollen lokal angeschlossene Datenträger zur Datensicherung genutzt werden, müssen diese mit dem Dateisystem "Mac OS Extended (Journaled)" formatiert sein. Alternativ kann eine Datensicherung in einem freigegebenen Verzeichnis auf einem entfernten System im Netz abgelegt werden. Voraussetzung hierfür ist die Nutzung des Apple Filing Protocols (AFP). Das SMB / CIFS -Protokoll kann mit folgendem Befehl auf der Konsole aktiviert werden:

defaults write com.apple.systempreferences TMShowUnsupportedNetworkVolumes 1

Die Variable "TMShowUnsupportedNetworkVolumes" ist ein inoffizieller Weg, um weitere Netzwerkprotokolle freizuschalten. Damit kann aber kein fehlerfreier Einsatz garantiert werden und Apple gewährt auch keine Unterstützung für dieses Vorgehen.

Time Machine kann in den Systemeinstellungen unter "Time Machine" aktiviert werden. Anschließend muss ein kompatibles Laufwerk zur Ablage der Datensicherung gewählt werden. Time Machine erstellt eine Kopie aller auf der Festplatte befindlichen Daten. Sollen Daten von der Datensicherung nicht erfasst werden, lassen sich Ausnahmen in den Optionen definieren. Reicht der verfügbare Speicherplatz nicht mehr aus, um eine Datensicherung durchzuführen, wird der Anwender darauf aufmerksam gemacht, dass er entweder ältere Datensicherungen löschen muss, oder dass das Programm automatisch ältere Sicherungen löscht, bis genug Speicherplatz zur Verfügung steht.

Bei der Durchführung einer Datensicherung sind die folgenden Punkte zu beachten:

- Time Machine kann alle Systemdateien, die zum Start des lokalen Rechners notwendig sind, sichern. Eine Datensicherung sollte automatisch in regelmäßigen Abständen und manuell nach größeren Änderungen der Konfiguration durchgeführt werden.
- Nach Abschluss der Datensicherung ist die zugehörige Protokolldatei /var/log/system.log daraufhin zu überprüfen, ob während der Sicherung Fehler aufgetreten sind. Die Protokolldatei kann über das macOS-Dienstprogramm "Konsole" eingesehen werden. Die Datensicherung wird vom Prozess "backupd" erstellt, sodass nach allen Meldungen mit diesem Prozessnamen gesucht werden kann. Da in der Protokolldatei /var/log/system.log unter anderem vertrauliche Informationen aufgelistet sind, kann sie nur ein Benutzer mit Administrator-Privilegien einsehen.

Systemwiederherstellung

Um ein komplettes System wiederherzustellen, muss der Client entweder von einem Installationsmedium (DVD oder USB-Stick) oder im Recovery-Modus gestartet werden. Dazu muss während des Startvorganges die Alt-Taste (für USB-Sticks), die Taste C (für optische Medien) oder die Tastenkombination Cmd +R (für Recovery-Modus) gedrückt gehalten werden. Nach Auswahl der Menüsprache findet sich in den Dienstprogrammen die Möglichkeit, eine Datenwiederherstellung durchzuführen. Anschließend müssen der Datenträger, auf der sich die Datensicherung befindet, und die Festplatte, die wiederhergestellt werden soll, ausgewählt werden.

Time Machine kann auch nur ausgewählte Dateien wiederherstellen. Dazu müssen in den verschiedenen, hintereinander dargestellten, zeitlich geordneten Fenstern die Objekte in der gewünschten Version ausgewählt und über die Schaltfläche "Wiederherstellen" zum Zielort kopiert werden.

Anforderung an Sicherungssoftware für macOS

Soll für umfangreichere Installationen bzw. bei hohen Verfügbarkeitsanforderungen zusätzliche Software zur Durchführung von Datensicherungen eingesetzt werden, ist bei der Auswahl der Sicherungssoftware darauf zu achten, dass sie so viele der folgenden Anforderungen wie möglich erfüllt:

- Die bei macOS eingesetzten Dateisysteme APFS und HFS+ müssen bei der Sicherung und Wiederherstellung unterstützt werden. Weitere unterstützte Dateisysteme wie FAT und NTFS sind von Vorteil.
- Es muss möglich sein, Sicherungen automatisch zu frei definierbaren Zeiten oder in einstellbaren Intervallen durchführen zu lassen, ohne dass Eingriffe außer dem eventuell notwendigen Bereitstellen von Sicherungsdatenträgern erforderlich wären.
- Die Sicherungssoftware muss den Schutz des Backup-Mediums vor unbefugtem Zugriff durch ein Passwort oder besser durch Verschlüsselung unterstützen. Weiterhin sollte sie in der Lage sein, die gesicherten Daten in komprimierter Form abzuspeichern.
- Von Vorteil ist es, wenn ein oder mehrere ausgewählte Benutzer automatisch über das Sicherungsergebnis und eventuelle Fehlermeldungen per E-Mail oder ähnliche Mechanismen informiert werden können.
- Das Erstellen von Include- und Exclude-Listen muss möglich sein. Durch Vorgabe geeigneter Include- und Exclude-Listen bei der Datei- und Verzeichnisauswahl sollte genau spezifiziert werden können, welche Daten zu sichern sind und welche übersprungen werden können. Es sollte möglich sein, diese Listen zu Sicherungsprofilen zusammenzufassen, abzuspeichern und für spätere Sicherungsläufe zu benutzen.
- Die Sicherung sollte auf verschiedenen Datenträgern wie optischen Datenträgern, auf Festplatten, Bandlaufwerken, USB-Laufwerken sowie Netzlaufwerken erfolgen können.
- Es sollte möglich sein, die zu sichernden Daten in Abhängigkeit vom Datum ihrer Erstellung bzw. ihrer letzten Modifikation auszuwählen.
- Die Sicherungssoftware sollte die Erzeugung einer Volldatensicherung sowie inkrementeller Kopien (Änderungssicherungen) unterstützen.
- Die Sicherungssoftware sollte in der Lage sein, nach der Sicherung einen automatischen Vergleich der gesicherten Daten mit dem Original durchzuführen und nach der Wiederherstellung von Daten einen entsprechenden Vergleich zwischen den rekonstruierten Daten und dem Inhalt des Sicherungsdatenträgers durchzuführen.
- Bei der Wiederherstellung von Dateien sollte ausgewählt werden können, ob die Dateien am ursprünglichen oder an einem anderen Ort wiederhergestellt werden. Ebenso sollte es möglich sein, das Verhalten der Software für den Fall zu steuern, dass am Zielort schon eine Datei gleichen Namens vorhanden ist. Dabei sollte einstellbar sein, ob diese Datei immer, nie oder nur in dem Fall überschrieben wird, dass sie älter ist als die zu rekonstruierende Datei, oder dass in diesem Fall eine explizite Anfrage an den Benutzer erfolgt.

Wiederherstellung von Systemparametern beim Einsatz von macOS

Falls ein macOS-System nicht mehr startet oder Probleme mit der Lesbarkeit von Dateien auftreten, gibt es verschiedene Handlungsmöglichkeiten. Benutzer und Administratoren sind über die Maßnahmen zur Wiederherstellung von Systemparametern beim Einsatz von macOS zu informieren. Um Fehler bei der Nutzung eines Clients unter macOS zu finden, die einen normalen Betriebssystem-Start verhindern, kann zwischen verschiedenen Startmodi gewählt werden.

Single-User-Mode

Wird ein Client unter macOS gestartet, muss die Tastenkombination Cmd+S gedrückt gehalten werden, um in den Single-User-Modus zu gelangen. Der Single-User-Modus bootet nur ein rudimentäres Betriebssystem ohne grafische Benutzeroberfläche. Dieser Modus ist sehr robust und meistens auch dann noch verfügbar, wenn das System durch eine fehlgeschlagene Installation oder einen Dateisystemfehler nicht mehr startet. Zur Arbeit im Single-User-Modus wird zwar das root-Konto verwendet, jedoch kann zu Beginn nur mit Leserechten auf das Startlaufwerk zugegriffen werden.

Um das Dateisystem zu überprüfen, kann der Befehl "/sbin/fsck -fy" eingegeben werden. Es ist zu beachten, dass im Single-User-Modus die amerikanische Tastaturbelegung verwendet wird.

Wurde das Dateisystem überprüft und gegebenenfalls repariert, so kann durch den Befehl "/sbin/mount -uw /" der Schreibzugriff auf das Startlaufwerk aktiviert werden. Nun stehen weitere Möglichkeiten zur Verfügung, um den Fehler zu beseitigen. So können beispielsweise fehlerhafte Programme entfernt werden, die automatisch mit dem System starten.

Verbose-Mode

Der "Verbose-Mode" bietet eine weitere Möglichkeit, um tiefere Einblicke in das System zu erhalten. Um in diesen Modus zu kommen, muss während des Systemstarts die Tastenkombination Cmd+V gedrückt gehalten werden. Dadurch wird das System normal gestartet, die Bildschirmausgabe jedoch nicht mehr durch das Apple-Logo verdeckt. Statt dessen zeigt das System Informationen an, die zum Beispiel Auskunft darüber geben, welcher Dienst gerade gestartet wird. So können mögliche Fehlerquellen weiter eingegrenzt werden.

Safe-Boot-Mode

Wird während des Startvorgangs die Taste "Shift" gedrückt gehalten, werden keine Kernel-Extensions und Startobjekte von Fremdherstellern geladen. Somit wird bereits während des Starts eine hohe Zahl an Fehlerquellen ausgeschlossen. Wurde festgestellt, dass eines der Startobjekte den regulären Betriebssystemstart verhindert, kann das entsprechende Startobjekt in den "Systemeinstellungen" unter "Benutzerkonten" deaktiviert werden. Die nicht über die grafische Oberfläche erreichbaren Startobjekte befinden sich im Verzeichnis „/Library/StartupItems/“.

Startobjekte anpassen

Wird durch den Safe-Boot-Mode festgestellt, dass ein Startobjekt Probleme verursacht und die grafische Benutzeroberfläche nicht eingesetzt werden kann, um das Objekt zu entfernen, muss manuell auf die Startobjekte zugegriffen werden. Die Startobjekte des "LaunchDaemons", die mit root-Privilegien ausgeführt werden, befinden sich entweder in den Verzeichnissen "/System/Library/LaunchDaemons" oder "/Library/LaunchDaemons". Startobjekte, die mit Benutzer-Privilegien ausgeführt werden, sind in den Verzeichnissen "/System/Library/LaunchAgents" oder "/Library/LaunchAgents" zu finden. Um ein Startobjekt zu entfernen, reicht es aus, die Dateiendung zu verändern.

Parameterspeicher löschen

Im Permanent Random Access Memory (PRAM) werden Systeminformationen wie die Wiederholfrequenz, Auflösung und Farbtiefe, aber auch Informationen über das Startlaufwerk gespeichert. Um den Parameterspeicher zu löschen, muss beim Starten des Computers die Tastenkombination Command+Alt +P+R gleichzeitig gedrückt gehalten werden, bis der Startton mehrmals zu hören ist.

Power Management Unit zurücksetzen

Startet das System nach einem PRAM-Reset noch immer nicht, sollte die Power Management Unit zurückgesetzt werden. Da sich die Vorgehensweise stark von Produkt zu Produkt unterscheidet, sollte der Anwender die Apple-Wissensdatenbank im Internet zu Rate ziehen.

SYS.2.4.M2 Nutzung der integrierten Sicherheitsfunktionen von macOS

macOS enthält "Xprotect", einen integrierten Schutz gegen bekannte, Mac-spezifische Schadprogramme, der durch Apple in unregelmäßigen Abständen aktualisiert wird und standardmäßig aktiviert ist. Zusätzlich enthält macOS mit dem sogenannten "Gatekeeper" eine Funktion, welche die Ausführung von Anwendungen kontrolliert. Standardmäßig erlaubt Gatekeeper nur die Ausführung von Programmen, die entweder über den App Store bezogen oder von Apple signiert wurden (das Programm stammt von einem Entwickler, der von Apple verifiziert wurde). Die Funktion Gatekeeper muss in dieser Standardkonfiguration betrieben werden, solange unsignierte Programme nicht absolut nötig sind.

Manuelle Überprüfung der Signaturen von macOS Anwendungen

In macOS sind Betriebssystemkomponente sowie Programme aus dem App Store von Apple digital signiert. Darüber hinaus sind Dritthersteller, die ihre Programme nicht im App Store anbieten, aufgerufen, ihre Programme zu signieren. Wird ein signiertes Programm in irgendeiner Form verändert, zum Beispiel durch Schadsoftware, so wird die Signatur ungültig. Wird ein neues Programm eingesetzt, muss daher dessen Signatur manuell überprüft werden. Liegen keine Signaturinformationen vor, sollte das Programm zumindest mit einem Viren-Schutzprogramm überprüft werden. Um die Gültigkeit einer Signatur zu überprüfen, wird von Apple eine Public-Key-Infrastruktur verwendet, ähnlich wie bei HTTPS -Webseiten. Die Administratoren sollten im Umgang mit dem Befehl "codesign" geschult werden, um jedes neue Programm einer einmaligen Signaturprüfung unterziehen zu können. Ob ein Programm eine gültige Signatur hat, kann mit folgendem Kommandozeilen-Befehl überprüft werden:

codesign --verify --verbose /Pfad/Dateiname.app

Handelt es sich um eine gültige Signatur, so entspricht die Datei dem vom Hersteller vertriebenen Original und wurde nicht verändert. Somit kann mit einer Signaturprüfung eine mögliche Manipulation auf dem Übertragungsweg ausgeschlossen werden.

Signaturen werden ebenfalls genutzt, um Programme eindeutig wiederzuerkennen. So ist sichergestellt, dass für diese Programme die entsprechenden Einstellungen in der "Kindersicherung", der Firewall und dem Schlüsselbund gelten.

Einschränkung der Programmzugriffe unter macOS

Um unter macOS den Zugriff auf bestimmte Funktionen des Computers einzuschränken, kann die "Kindersicherung" eingesetzt werden. Obwohl diese Funktion Kindersicherung bezeichnet wird, kann deren Nutzung auch in Behörden oder Unternehmen sinnvoll sein. Durch diese Kindersicherung, zu finden in den Systemeinstellungen, können Benutzerkonten weiter eingeschränkt werden. Auch die Programmzugriffe lassen sich mit der Kindersicherung weiter einschränken, nachdem alle nicht benötigten Programme entfernt wurden. Unter Umständen können Einschränkungen hierdurch präziser eingestellt werden.

So kann zum Beispiel für die Benutzer der Zugriff auf bestimmte Anwendungsprogramme, Webseiten oder Computerkomponenten beschränkt werden. Dieses Vorgehen ist auch geeignet, um das Verzeichnis "Dienstprogramme" zu sperren, da hier Programme zur Administration des Computers liegen, die tiefere Einblicke in das System ermöglichen. Soll nur der Zugriff auf bestimmte Webseiten bzw. Domänen erlaubt sein, kann unter dem Menüpunkt "Inhalt" beziehungsweise "Content" der Zugriff auf eine Domäne wie "*.bund.de" erlaubt werden. Weiterhin ist es möglich, die E-Mail-Kommunikation nur zwischen vorher festgelegten Partnern zu erlauben.

Unter dem Menüpunkt "Mail" kann eine Liste von freigegebenen E-Mail-Kommunikationspartnern erstellt werden. Durch diese Einstellung kann vermieden werden, dass Informationen über das E-Mail-Programm abfließen. Es muss jedoch beachtet werden, dass weiterhin HTTP-Webmailer benutzt werden können, um E-Mails an nicht autorisierte Personen zu versenden. Jedoch ist es zurzeit nicht möglich, die Liste der erlaubten Kommunikationspartner mittels regulären Ausdrücken anzupassen. Die Anmeldezeiten für Benutzerkonten lassen sich unter dem Menüpunkt "Time" anpassen. Wird zum Beispiel davon ausgegangen, dass die Hauptarbeitszeit zwischen 7 und 17 Uhr liegt, sollten die erlaubten Benutzeranmeldezeiten diesen Zeiten ungefähr entsprechen.

Weitere verfügbare Einstellungsmöglichkeiten, wie zum Beispiel der Zugriff auf optische Laufwerke, sollten möglichst restriktiv gehalten werden. Jedoch muss beachtet werden, dass eine zu starke Einschränkung hinderlich und demotivierend sein kann. Daher sollte im Vorfeld durch den Leiter der IT und den ISB geklärt werden, welche Restriktionen an welchen Clients umgesetzt werden sollen. Dies sollte dokumentiert werden.

Die Clients können ebenfalls zentral gesteuert werden. Wird in den "Systemeinstellungen" unter "Kindersicherung" die Option "Kindersicherung von einem anderen Computer aus verwalten" aktiviert, können Benutzerkonten auf entfernten Computern mittels Kindersicherung eingeschränkt werden. Hierfür wird der Benutzername und das Passwort eines Administrators auf dem zu steuernden IT-System benötigt. Mit diesen Zugangsdaten können die Benutzerrechte auf dem zu steuernden IT-System vom administrierenden IT-System aus, so wie oben beschrieben, eingeschränkt werden.

SYS.2.4.M3 Verwaltung der Benutzerkonten [Benutzer]

Das bei der Erstkonfiguration von macOS angelegte Benutzerkonto ist ein Administrator-Konto mit umfassenden Berechtigungen zur Systemkonfiguration. Es muss daher für die tägliche Verwendung des Macs auf jeden Fall zusätzlich ein Standard-Benutzerkonto angelegt werden. Sollte der Mac von mehreren Anwendern genutzt werden, muss für jeden Anwender ein eigenes Benutzerkonto angelegt werden. Es sollten nur solche Anwender administrative Aufgaben auf dem System wahrnehmen dürfen, die diese Funktionalität auch benötigen und beherrschen.

Gast-Benutzer-Account deaktivieren

Der Gast-Benutzer-Account unter macOS ist standardmäßig aktiviert und muss zusammen mit dem Zugriff für Gäste auf freigegebene Ordner deaktiviert werden. Unter "Systemeinstellungen | Benutzer | Andere Accounts | Gast-Account" muss die Option "Gästen den Zugriff auf freigegebene Ordner erlauben" deaktiviert werden.

Zugriffsschutz der Benutzerkonten unter macOS

Unter macOS müssen die Einstellungen der Benutzerkonten angepasst werden, um die System-Sicherheit weiter zu erhöhen. Zum Beispiel könnte die Merkhilfe für Passwörter von Unbefugten genutzt werden, um Hinweise auf das Passwort zu erhalten. Diese Anpassungen lassen sich in den Systemeinstellungen unter "Benutzer" vornehmen.

Die Sicherheit eines Benutzerkontos vor unbefugtem Zugriff ist im hohen Maße von dem verwendeten Passwort abhängig, daher muss ein starkes Passwort verwendet werden. Eine weitere wichtige Bedingung für ein sicheres Benutzerkonto ist das Deaktivieren von Merkhilfen des Passwortes, durch die ein Angreifer wichtige Hinweise auf das Passwort erhalten kann. Da die Informationen in der Merkhilfe im schlimmsten Fall dem eigentlichen Passwort entsprechen, sollte diese Funktion deaktiviert werden. Wird eine Passwort-Merkhilfe dennoch eingesetzt, müssen unbedingt alle Benutzer für diese mögliche Gefahr sensibilisiert werden. Ebenfalls sollte das Anmeldefenster nicht in Form einer Liste aller Benutzer angezeigt werden, da ein Angreifer damit alle Informationen über auf dem System existierende Benutzer erhält. Er benötigt dann nur noch die entsprechenden Passwörter, um unerlaubten Zugriff auf das System zu erhalten. Ohnehin sollte die Anmeldung am System grundsätzlich nicht automatisch erfolgen, sondern nur mit Benutzername und Passwort möglich sein.

Festlegung von Passwortrichtlinien unter macOS

Für alle Clients unter macOS müssen Richtlinien für Passwörter definiert werden, um sie mit einem angemessenen starken Passwort zu versehen. Dazu kann das Kommandozeilen-Programm "pwpolicy" benutzt werden. Mit diesem Programm lassen sich beispielsweise eine minimal erforderliche Anzahl von Buchstaben und Zahlen, eine Mindestzeichenlänge oder eine maximale Anzahl fehlgeschlagener Login-Versuche definieren.

Der folgende Befehl legt eine Richtlinie für Passwörter fest, die eine Minimallänge des Passwortes von 8 Zeichen fordert und 8 fehlgeschlagene Anmeldeversuche zulässt, bevor das Konto deaktiviert wird.

```
pwpolicy -n /Local/Default -setglobalpolicy "minChars=8 maxFailedLoginAttempts=8"
```

Automatische Anmeldung deaktivieren

Das automatische Anmelden am System sollte deaktiviert werden. Ist es möglich, sich an einem macOS-System ohne Passwortabfrage anzumelden, werden viele Sicherheitsfunktionen übergangen. Die Option "Automatisches Anmelden deaktivieren" ist in den Systemeinstellungen unter Sicherheit im Menüpunkt "Allgemein" zu finden und sollte aktiviert werden.

Aktivierung der Bildschirmsperre

Wird der Bildschirmschoner oder der Ruhezustand beendet, sollte das Kennwor erneut für den aktuell angemeldeten Benutzer abgefragt werden. Die Option "Kennwort erforderlich" ist in den Systemeinstellungen unter Sicherheit in dem Menüreiter "Allgemein" zu finden und sollte aktiviert werden. Dieser Wert sollte möglichst niedrig gewählt werden. Es empfiehlt sich eine Einstellung von höchstens 15 Minuten.

Abmelden nach x Minuten Inaktivität

Befindet sich das IT-System längere Zeit im Leerlauf, kann eine automatische Abmeldung des Benutzers sinnvoll sein. Die Option "Abmelden nach x Minuten Inaktivität" ist in den Systemeinstellungen unter Sicherheit in dem Menüreiter "Allgemein" zu finden und kann aktiviert werden. Dieser Wert sollte möglichst niedrig gewählt werden. Wenn das System den Benutzer nach einer bestimmten Zeit automatisch abmelden soll, empfiehlt sich eine Einstellung von 15 Minuten.

Sicherheit des Schlüsselbundes erhöhen

Das Passwort des Schlüsselbundes sollte geändert werden, sodass es nicht mehr mit dem Passwort des aktuell angemeldeten Benutzers übereinstimmt. Damit wird verhindert, dass eine Person, die unberechtigten Zugang zum Client erlangt, auch Zugang zu allen Informationen im Schlüsselbund erhält. Um das Passwort zu ändern, muss unter den Dienstprogrammen die Applikation "Schlüsselbund" aufgerufen und unter dem Menüpunkt "Bearbeiten" die Option "Kennwort für Schlüsselbund 'Anmeldung' ändern" gewählt werden. Dadurch wird die Synchronisation zwischen Benutzeraccount-Passwort und Schlüsselbund-Passwort aufgehoben. Zusätzlich sollte die Option "Einstellungen für den Schlüsselbund 'Anmeldung' ändern" aufgerufen werden, um die Optionen "Nach X Minuten Inaktivität schützen" und "Bei Wechsel in Ruhezustand schützen" zu aktivieren. Bei der ersten Option empfiehlt es sich, 15 Minuten einzustellen.

Verwenden der Passwortabfrage für jede Systemeinstellung

Es sollte die "Kennwortabfrage für die Freigabe jeder geschützten Systemeinstellung" aktiviert werden, damit nur Administratoren die Systemeinstellungen ändern können. Weiterhin sorgt diese Einstellung dafür, dass bei einem unbefugten Zugriff nur freigeschaltete Systemeinstellungen verändert werden können. Die Option "Kennwortabfrage für die Freigabe jeder geschützten Systemeinstellung" ist in den Systemeinstellungen unter Sicherheit in dem Menüreiter "Allgemein" zu finden.

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich SYS.2.4 *Clients unter macOS*.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Clients unter macOS".

SYS.2.4.M4 Verwendung der Festplattenverschlüsselung

Mit aktivierter Festplattenverschlüsselung sind die Festplatten-Daten eines Macs im ausgeschalteten Zustand verschlüsselt. Die Festplattenverschlüsselung muss daher insbesondere bei mobilen Macs (z.B. MacBooks) verwendet werden. Hierzu kann beispielsweise die in macOS integrierte Funktion "FileVault" verwendet werden.

Mit FileVault können Partitionen mit dem Algorithmus AES-XTS-128 verschlüsselt werden. Da es sehr einfach zu benutzen ist, wird empfohlen, alle Partitionen des Macs generell zu verschlüsseln. Das gilt besonders für sensible Informationen auf mobilen Rechnern, die einem erhöhten Diebstahlsrisiko ausgesetzt sind.

FileVault schützt die Informationen nur, wenn der Client ordnungsgemäß heruntergefahren wurde oder der Benutzer noch nicht angemeldet ist. Nachdem sich der Benutzer erfolgreich angemeldet hat, wird die von FileVault verschlüsselte Partition in das System eingebunden und ist verfügbar. Meldet sich der Benutzer ab, wird die von FileVault verschlüsselte Partition wieder aus dem Dateisystem ausgehängt und die Dateien sind geschützt.

Können sich die Benutzer ohne Authentisierung am Client anmelden ("Automatische Anmeldung"), werden die mit FileVault geschützten Informationen ohne Passwortabfrage entschlüsselt. Für wirksamen Schutz der Informationen durch FileVault muss die automatische Anmeldung deaktiviert und ein ausreichend sicheres Passwort gewählt werden.

Vorbereitung des Einsatzes von FileVault

Mit FileVault können nur Partitionen geschützt werden, die mit den Dateisystemen HFS+ ("Mac OS Extended") oder APFS formatiert sind und bei denen der Zusatz "Case sensitive" bzw. "Groß- und Kleinschreibung" nicht aktiviert wurde.

FileVault aktivieren

Um das Startvolume eines Macs zu verschlüsseln, kann FileVault in den Systemeinstellungen aktiviert werden. Wenn FileVault auf einem Mac mit mehr als einem Benutzer aktiviert wird, erscheint die Aufforderung, die jeweiligen Benutzer anzugeben, die das Startvolume entsperren können.

Datenwiederherstellung

Beim Aktivieren von FileVault erhält man einen Wiederherstellungsschlüssel, der dazu verwendet werden kann, die Daten auf dem verschlüsselten Startvolume wiederherzustellen, falls der Benutzer das Passwort vergessen sollte. Der Wiederherstellungsschlüssel darf nicht online bei Apple gespeichert werden. Der von FileVault erzeugte Wiederherstellungsschlüssel muss an einem sicheren Ort aufbewahrt werden.

Besteht der Verdacht, dass der Wiederherstellungsschlüssel publik wurde, weil er zum Beispiel an einem ungesicherten Ort aufbewahrt worden ist, muss er sofort geändert werden, da sonst der Zugriff auf alle auf dem Computer befindlichen verschlüsselten Daten möglich ist.

Der Wiederherstellungsschlüssel sollte an einer geeigneten Stelle aufbewahrt werden, damit die Daten in einem Störfall schnell und personalunabhängig durch einen Administrator wiederhergestellt werden können.

Sichere Datenhaltung und sicherer Transport unter macOS

Unter macOS können Disk-Images erstellt werden. Disk-Images stellen sich wie Dateien dar, enthalten jedoch intern ein eigenes Dateisystem, das per Doppelklick als virtuelles Laufwerk in das System eingebunden werden kann. Disk-Images können komprimiert und verschlüsselt werden. Jedes macOS-System kann die so erzeugten Disk-Images problemlos lesen. Auf anderen Plattformen ist dafür zusätzliche Software notwendig. Grundsätzlich sollte darauf geachtet werden, dass vertrauliche Informationen unter macOS nur in einem verschlüsselten Disk-Image oder mittels einer anderen geeigneten Verschlüsselungsmethode transportiert und gelagert werden. Die Benutzer müssen im Umgang mit Disk-Images geschult sein.

Wird ein Disk-Image von einem vorhandenen Verzeichnis erstellt, so werden zwei Einstellungsmöglichkeiten angeboten. Zum einen kann das Image-Format ausgewählt werden, zum Beispiel "Komprimiert", "Nur lesen" oder "Lesen/Schreiben". Für genaue Abbilder von CDs/ DVDs ist das Image-Format "DVD/ CD-Master" geeignet. Zum anderen wird eine Verschlüsselung angeboten. Befinden sich vertrauliche Informationen im Disk-Image, sollte es verschlüsselt werden. Hierfür sollte eine 256-Bit- AES -Verschlüsselung sowie ein komplexes Passwort gewählt und triviale Passwörter vermieden werden.

Soll ein neues, leeres Disk-Image erstellt werden, stehen im Gegensatz zu einem Image aus einem vorhandenen Ordner weitere Einstellungsmöglichkeiten zur Verfügung. Als wichtigste Optionen kann die maximale Größe des Disk-Images eingestellt sowie das Image-Format ausgewählt werden. Wird ein "Mitwachsendes Bundle-Image" gewählt, so wird Festplattenspeicher nur dann belegt, wenn er benötigt wird. Das Image wächst mit den hinzugefügten Daten. Das "Mitwachsende Bundle-Image" schrumpft jedoch nicht, wenn Daten wieder daraus entfernt werden. Belegter Speicher lässt sich jedoch im Nachhinein wieder freigeben. Eine weitere Einstellung bei einem neu erstellen Disk-Image ist die Wahl zwischen den gängigen Dateisystemen von Apple und Microsoft.

Das Kennwort für das Disk-Image kann ebenfalls wie andere vertrauliche Informationen im Schlüsselbund abgelegt werden. Arbeiten mehrere Personen mit einem Disk-Image, muss ein zentraler, sicherer Ablageort gewählt werden, damit das aktuelle Passwort jedem autorisierten Mitarbeiter zur Verfügung steht.

Einsatz von Apple-Software-Restore unter macOS

Unter macOS können Dateisysteme mit der Funktion Apple-Software-Restore (ASR) dupliziert und geklont werden. ASR bietet nicht nur die Möglichkeit, Partitionen zu klonen, sondern auch ein Disk-Image im Netz bereitzustellen und dieses über das Netz auf Clients zu verteilen.

Wurde ein Client unter macOS nach den Vorgaben des Unternehmens oder der Behörde installiert und entspricht den Sicherheitsrichtlinien, so kann dieses System geklont und für eine Netz-Installation für weitere Clients genutzt werden. Damit wird es ermöglicht, dass alle Clients unter macOS eine gleiche Grundkonfiguration erhalten, die den Sicherheitsvorgaben der Institution entspricht.

SYS.2.4.M5 Erhöhung des Schutzes von Daten

macOS bietet verschiedene Funktionen, um dem Benutzer einen hohen Bedienkomfort zu ermöglichen. Dazu gehören beispielsweise die Ortungsdienste, das Speichern zuletzt verwendeter Objekte, das automatische Öffnen von heruntergeladenen Daten und das automatische Starten von CDs und DVDs. Da diese Funktionen allerdings einen negativen Einfluss auf den Datenschutz des Benutzers haben, sollten diese Funktionen deaktiviert bzw. konfiguriert werden.

Ortungsdienste deaktivieren

Unter Verwendung der Daten aus WLAN-Netzen ist es möglich, den ungefähren Aufenthaltsort eines macOS Clients zu ermitteln. Diese Standortinformationen können dazu verwendet werden, Systemdienste wie die Zeitzone für das aktuelle Datum und die Uhrzeit automatisch einzustellen. Jedoch können auch Webseiten mit Lokalisierungsfunktion diese Informationen nutzen, um den Standort des Webseiten-Besuchers zu bestimmen. Dies kann nützlich, aber auch aus Datenschutz- und Sicherheitssicht problematisch sein. Beispielsweise kann mithilfe der Ortungsdienste der Standort des nächsten Bankautomaten oder Postamtes angezeigt werden. Möchte eine Webseite den Standort lokalisieren, erscheint normalerweise ein Dialogfenster, um die Erlaubnis des Benutzers dazu einzuholen. Dennoch sollten die Ortungsdienste in den Systemeinstellungen generell deaktiviert werden.

Automatisches Öffnen "sicherer Dateien" in Safari deaktivieren

Der mitgelieferte Browser Safari bietet die Möglichkeit, Dateien direkt nach einem Download mit dem damit verknüpften Programm zu öffnen. Diese Einstellung ermöglicht es auch, Dateien automatisch und ohne Nachfrage auszuführen, die Schadcode enthalten könnten. Wird zum Beispiel aus einer unsicheren Quelle, wie einer manipulierten Webseite im Internet, eine präparierte PDF-Datei heruntergeladen und automatisch geöffnet, könnte eingebetteter Schadcode ausgeführt werden, was zu Datenverlusten oder anderen Problemen führen kann. Das automatische Öffnen sollte daher in den Safari-Einstellungen deaktiviert werden.

Autostart-Funktion deaktivieren

Die Funktion Autostart ermöglicht es, Programme von externen Datenträgern sofort auszuführen, wenn diese, wie zum Beispiel CDs, DVDs oder externe Festplatten, mit dem Computer verbunden werden. Da die hierdurch automatisch ausgeführten Programme auch Schadsoftware enthalten könnten, sollte diese Funktion für jeden Benutzer in den Systemeinstellungen deaktiviert werden.

Daneben gibt es weitere Konfigurationsmöglichkeiten, die aus dem Blickwinkel der Datensparsamkeit sinnvoll sind:

Liste der zuletzt verwendeten Objekte reduzieren

macOS speichert eine Liste der zuletzt verwendeten Anwendungen, Dokumente und Serververbindungen. In erster Linie erleichtern diese Informationen das Arbeiten, jedoch sind damit auch Rückschlüsse auf vertrauliche Informationen möglich, wie zum Beispiel mit welchen Dokumenten kürzlich gearbeitet wurde oder die Adressen der zuletzt benutzten Server. Um diese Informationen auf ein Minimum zu beschränken, sollte in den Systemeinstellungen die Anzahl der zuletzt verwendeten Objekte reduziert bzw. auf 0 gesetzt werden.

Sicheres Entleeren des Papierkorbes aktivieren

Um zu verhindern, dass gelöscht geglaubte Dateien aus dem Papierkorb unter macOS wiederhergestellt werden können, sollte der Papierkorb regelmäßig entleert werden. macOS bietet zudem die Einstellung "Sicheres Entleeren" an, bei der das Betriebssystem die Dateien nach dem Entleeren des Papierkorbs mit einem Bitmuster überschreibt. Um diese Einstellung zu aktivieren, muss im Finder die Einstellung "Papierkorb sicher entleeren" aktiviert werden.

SYS.2.4.M6 Verwendung aktueller Hardware

Bei der Anschaffung von neuen Macs sollte auf aktuelle Modelle zurückgegriffen werden. Beim Einsatz von vorhandenen Macs sollte überprüft werden, ob diese weiterhin von Apple mit Software-Updates versorgt werden. Leider stellt Apple keine offiziellen Informationen über einen Software-Product-Lifecycle (SPL) von macOS zur Verfügung. Die Vergangenheit hat gezeigt, dass Apple mindestens zwei Jahre Sicherheitsupdates für macOS bereitstellt. Da derzeit jährlich eine neue Hauptversion von macOS erscheint, werden somit in der Regel die beiden vorhergehenden Hauptversionen zumindest mit Sicherheitsupdates versorgt. Deshalb ist es sinnvoll, andere Informationsquellen sowie Erfahrungswerte zu nutzen. Beispielsweise ist es empfehlenswert, verschiedene Webseiten und Blogs zu prüfen, die sich mit dem Thema macOS auseinandersetzen. Nach Möglichkeit sollte stets die neuste Version von macOS genutzt werden.

SYS.2.4.M7 Zwei-Faktor-Authentisierung für Apple-ID [Benutzer]

Die Zwei-Faktor-Authentisierung für die Verwendung des Apple-ID-Kontos sollte aktiviert werden. Bei diesem Authentisierungsverfahren wird bei bestimmten Aktionen neben dem Kennwort eine zusätzliche PIN abgefragt. Diese PIN erhält der Nutzer über ein registriertes vertrauenswürdige iOS-Gerät oder über eine SMS an die hinterlegte Mobilfunknummer (falls kein iOS-Gerät vorhanden ist). Die Zwei-Faktor-Authentisierung ist momentan nur für Macs geeignet, da nur hier die Authentisierung mittels zweier unabhängiger Komponenten (Mac und iOS-Gerät) stattfindet. Die Zwei-Faktor-Authentisierung für eine bestimmte Apple-ID kann auf der Webseite "appleid.apple.com" eingerichtet werden.

SYS.2.4.M8 Keine Nutzung von iCloud für sensible Daten [Benutzer]

Eine Synchronisation der Daten zwischen mehreren Geräten über den iCloud-Dienst "Handoff" sollte verhindert werden, da damit sensible Daten die eigene Kontrolle verlassen. Die Geräte sollten daher immer über selbst betriebene Dienste synchronisiert werden. Sensible Daten sollten nicht in iCloud gespeichert werden. Das automatische Speichern von Entwürfen (E-Mails, Dokumente etc.) in iCloud sollte deaktiviert werden. iCloud selbst kann in den Systemeinstellungen von macOS deaktiviert werden, falls bei der Einrichtung des macOS-System iCloud aktiviert worden ist. Des Weiteren sollte sichergestellt werden, dass die Funktion "Handoff" unter "Allgemein" in den Systemeinstellungen deaktiviert ist.

SYS.2.4.M9 Verwendung von zusätzlichen Schutzprogrammen

Apple bietet mit Xprotect in macOS einen integrierten Schutz vor Schadprogrammen. Darüber hinaus existieren Virenschutz-Lösungen von Drittanbietern, die bei Bedarf eingesetzt werden sollten. Beispielsweise könnte in heterogenen Umgebungen ein zusätzliches Virenschutz-Programm eingesetzt werden, um IT-Systeme mit anderen Betriebssystemen (z. B. Windows) bei der Weitergabe von Daten zu schützen. Bei dem Einsatz eines Virenschutz-Programmes muss darauf geachtet werden, dass dessen Signaturen regelmäßig aktualisiert werden. Das Viren-Schutzprogramm sollte im Hintergrund laufen und mindestens beim Zugriff auf eine Datei eine Virenüberprüfung durchführen. Weitere Informationen sind im Baustein OPS.1.1.4 *Schutz vor Schadprogrammen* zu finden. Dabei sollte beachtet werden, dass das Viren-Schutzprogramm auch Schadsoftware für Windows-Systeme erkennt, damit gefahrlos mit Windows-Systemen kommuniziert werden kann.

SYS.2.4.M10 Aktivierung der Personal Firewall

macOS enthält eine integrierte Personal Firewall, die jedoch im Auslieferungszustand deaktiviert ist. Um den Mac vor unerwünschten Netzwerk-Zugriffen zu schützen, sollte die Personal Firewall aktiviert und konfiguriert werden.

Konfiguration der Personal Firewall

Bevor die Personal Firewall unter macOS eingesetzt wird, müssen zwei Fakten überprüft werden. Mit der Personal Firewall können ein- oder ausgehende Verbindungen gefiltert werden oder der Zugriff von Programmen und Diensten auf das Internet eingeschränkt werden. Bevor für einzelne Anwendungen die Netzkommunikation abgeschaltet wird, sollte geprüft werden, ob es möglich ist, die Netzkommunikation programmintern abzuschalten. Außerdem sollte geprüft werden, ob bei dem jeweiligen Programm oder Dienst nach dem Sperren der Netzkommunikation keine unerwünschten Nebeneffekte auftreten. Wird direkt versucht, mit einer Personal Firewall die Netzkommunikation eines Programms zu unterbinden, können Probleme auftreten, da ein Programm auf die Netzkommunikation angewiesen sein kann und auf eine Antwort aus dem Netz wartet, bevor es weiter ausgeführt wird.

Der Einsatz einer Personal Firewall, die direkt auf dem zu schützenden Client betrieben wird, ersetzt in keinem Fall ein eigenständiges Sicherheitsgateway (Firewall), dass das gesamte interne Netz der Institution schützt. Um aber beispielsweise macOS-Geräte vor Angriffen aus dem lokalen Netz zu schützen, kann der Einsatz einer Personal Firewall sinnvoll sein. Beim mobilen Einsatz von macOS-Geräten ist die Nutzung einer Personal Firewall immer empfehlenswert, um den Rechner vor Angriffen aus dem Internet zu schützen.

Vor dem Einsatz einer Personal Firewall muss festgelegt werden, welche Programme Netzzugriff erhalten sollen und welche nicht. Generell ist zunächst jegliche Netzkommunikation zu blockieren, im zweiten Schritt werden nur die gewünschten Ports oder Anwendungen freigeschaltet.

Integrierte Anwendungsfirewall

Die Anwendungsfirewall ermöglicht das Sperren und das Freigeben der Kommunikation von bestimmten Anwendungsprogrammen. Dazu muss der Anwender nicht wissen, welche Ports verwendet werden. Die Anwendungsfirewall überprüft auch die Signatur eines Programms. Es ist nicht möglich, ein für die Netzkommunikation freigegebenes Programm zu manipulieren, ohne dass eine erneute Firewall-Regeldefinition abgefragt wird. Unter macOS ist die Anwendungsfirewall im Auslieferungszustand deaktiviert. Diese muss in den Systemeinstellungen aktiviert werden. Über den Menüpunkt "Optionen" ist es möglich, die Einstellungen anzupassen.

Mit der Option "Alle eingehenden Verbindungen blocken" werden zunächst nur unbedingt notwendige macOS-Datenverbindungs- bzw. Kommunikationsdienste erlaubt, wie DHCP und Bonjour. Werden Freigaben wie beispielsweise "Dateifreigabe" oder "Entferne Anmeldung" aktiviert, öffnet macOS selbstständig die notwendigen Ports in der Firewall, über den die Dienste kommunizieren können.

Wird die Option "Alle eingehenden Verbindungen blocken" nicht verwendet, wird über die Liste der Anwendungsfirewall definiert, welche Dienste und Programme zum Öffnen von Ports in der Firewall berechtigt sind. Mit einem Mausklick auf das "+"-Symbol können Programme dieser Liste hinzugefügt werden. Nachdem ein Programm zu dieser Liste hinzugefügt wurde, muss definiert werden, ob eingehende Verbindungen für dieses Programm erlaubt oder blockiert werden sollen. Auch Befehlszeilenprogramme können zu dieser Liste hinzufügt werden. Beim Hinzufügen einer Anwendungssoftware zu dieser Liste ergänzt macOS das Programm um eine digitale Signatur, falls dies nicht zuvor schon einmal geschehen ist. Wird ein Programm nachträglich verändert, dass sich in der Liste befindet, wird der Anwender erneut aufgefordert, für das Programm eingehende Netzverbindungen zu erlauben oder zu blockieren. Auch für Programme ohne digitale Signatur, die sich nicht in dieser Liste befinden, wird dem Anwender ein Dialogfeld mit Optionen zum Erlauben oder Blockieren von Verbindungen angezeigt. Sobald der Anwender die Verbindungen erlaubt oder blockiert, versieht macOS das Programm mit einer digitalen Signatur und fügt es automatisch, einschließlich der vergebenen Berechtigungen, zur Liste der Anwendungsfirewall hinzu.

Wird die Option "Signierter Software automatisch erlauben, eingehende Verbindungen zu empfangen" aktiviert, können alle Programme, die mit einer digitalen Signatur versehen sind, eingehende Verbindungen empfangen, auch wenn die Programme nicht in der Liste angezeigt werden. Diese digitale Signatur muss von einer Zertifizierungsstelle (CA) ausgestellt worden sein, der Apple vertraut. Jede ausführbare Betriebssystemkomponente von macOS wurde durch Apple mit einer digitalen Signatur versehen und kann eingehende Verbindungen empfangen. Auch digital signierte Programme, die automatisch von anderen Programmen geöffnet werden, können zu dieser Gruppe gehören. Soll der Netzzugriff eines Programms mit einer digitalen Signatur über die Firewall blockiert werden, muss das Programm zuerst zur Anwendungsfirewall-Liste hinzufügt und dann ausdrücklich die Verbindungen blockiert werden. Wird der Zugriff eines Programms über die Firewall blockiert, kann das zu Störungen des Programms oder anderer, darauf basierender Programme führen oder die Leistung anderer verwendeter Programme und Dienste beeinflussen. Da diese Option nicht transparent ist, sollte von der Verwendung abgesehen werden.

Die Option "Tarn-Modus aktivieren" sollte nicht verwendet werden, da diese Option dem Internetstandard RFC 1122 widerspricht. Durch einen aktivierten Tarn-Modus werden keine Antworten auf Anfragen gesendet, die von einer blockierten Anwendung ausgehen. Ping ist beispielsweise eine der ICMP-Nachrichten, die durch den Tarnmodus nicht mehr funktionieren. Der Tarn-Modus bietet darüber hinaus aber keinen Schutz. Wäre der Rechner tatsächlich nicht vorhanden, würde die letzte Station vor dem Rechner an den Sender melden, dass das Ziel nicht erreichbar ist. Im Tarnmodus kommt jedoch keine Nachricht zurück. Daraus kann der Sender schließen, dass der Rechner da ist, aber nicht antwortet.

Deaktivieren nicht benötigter Netzdienste

Nicht benötigte Netzdienste sollten deaktiviert werden, da diese Systemressourcen belegen und ein Angriffsziel darstellen können. Dazu sind Administratorrechte notwendig. Wurden Veränderungen an den Systemdiensten vorgenommen, sind diese zu dokumentieren. Weiterhin sollte regelmäßig überprüft werden, ob nur nach dem Sicherheitskonzept zulässige Dienste aktiviert und über das Netz erreichbar sind.

Die verfügbaren Dienste werden in den Systemeinstellungen unter dem Menüpunkt "Freigaben" aufgelistet. Im Regelfall sollte ein Client-Betriebssystem keine oder nur wenige Dienste in einem Netz anbieten. Je nach Einsatzgebiet muss eine individuelle Entscheidung getroffen werden, ob und welcher Dienst aktiviert bleiben sollte.

Zur Verwaltung verwendete Dienste, wie zum Beispiel der "Apple Remote Desktop" (TCP-Port 5900), "Entfernte Anmeldung" (SSH-Zugriff, TCP-Port 22) oder Netzdienste des Viren-Schutzprogramms müssen aktiviert bleiben.

Wird in einem Netz der Dienst "Bonjour" nicht verwendet, sollte dieser ebenfalls deaktiviert werden, da er Systemressourcen belegt und einen weiteren Angriffspunkt darstellt.

sudo launchctl unload -w /System/Library/LaunchDaemons/com.apple.mDNSResponder.plist

sudo launchctl unload -w/System/Library/LaunchDaemons/com.apple.mDNSResponderHelper.plist

Wird das Betriebssystem aktualisiert, könnten Dienste unbeabsichtigt wieder aktiviert werden. Daher sollte nach jeder Aktualisierung geprüft werden, ob die Dienste weiterhin deaktiviert sind.

SYS.2.4.M11 Geräteaussonderung

Daten müssen von nicht mehr verwendeten Geräten gelöscht werden. Unverschlüsselte und verschlüsselte Festplatten müssen vor einer Geräteaussonderung vollständig überschrieben werden. Darüber hinaus sollte der nichtflüchtige Datenspeicher des Macs (NVRAM, Non-Volatile Random-Access Memory) zurückgesetzt werden. Der NVRAM dient dazu, verschiedene Einstellungen (z.B. Daten für die WLAN-Authentisierung) des Macs zu speichern.

Aussonderung eines macOS Systems

Auf ausgesonderten Arbeitsplatz-PCs müssen alle sensiblen Informationen auf geeignete Weise gelöscht werden. Dies gilt auch für Informationen auf defekten Datenträgern. Wurden auf einem Datenträger sensible Informationen abgelegt und kann durch einen Hardware-Fehler nicht mehr auf den Datenträger zugegriffen werden, so muss der Datenträger in geeigneter Weise zerstört werden.

Um unter macOS Informationen zu löschen, kann das "Festplatten-Dienstprogramm" verwendet werden. Handelt es sich um den Datenträger mit der Systempartition, muss der Computer von der macOS-Installations-DVD gestartet und das "Festplatten-Dienstprogramm" von der Installations-DVD aufgerufen werden. Mit diesem Programm lässt sich ein Datenträger auf unterschiedliche Arten löschen. In den Sicherheitsoptionen sollte "Daten mit Nullen überschreiben" eingestellt werden. Die Administratoren müssen im Umgang mit dem "Festplatten-Dienstprogramm" geschult und über die Vorgehensweise des sicheren Löschens von Datenträgern unter macOS informiert werden.

Bevor IT-Systeme oder Datenträger ausgesondert werden, müssen sie gesichtet werden, ob sich darauf noch benötigte Daten befinden. Diese müssen dann auf anderen Datenträgern gesichert bzw. archiviert werden. Es sollte überprüft werden, dass wirklich alle Daten korrekt gesichert wurden.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

SYS.2.4.M12 Aktivieren des Firmware-Kennworts [Benutzer] (CI)

Um ein unberechtigtes Booten des Macs zu verhindern, sollte das Firmware-Kennwort aktiviert werden. Sofern dieses aktiviert ist, können ohne Authentisierung außerdem keine Änderungen an den Einstellungen, wie den Bootoptionen, durchgeführt werden.

Das Firmware-Passwort kann in zwei verschiedenen Modi gesetzt werden:

Command-Modus: Die Firmware fragt beim Bootvorgang nach einem Passwort, wenn der Benutzer versucht, von einem anderen Startlaufwerk zu booten. Wenn der Rechner ganz normal gestartet wird, erfolgt keine Passwortabfrage.

Full-Modus: Wenn dieser Modus gesetzt ist, wird bei jedem Start des Rechners nach dem Passwort gefragt, also auch beim ganz normalen OS-Bootvorgang.

Firmware-Passwörter können unter macOS nur über "/usr/sbin/firmwarepasswd" gesetzt werden. Dafür sind Administrationsrechte Voraussetzung. Auf der Recovery-Partition gibt es eine GUI-Applikation namens "Firmware-Passwortdienstprogramm", die ebenfalls das Firmware-Passwort setzt, jedoch nur im Command-Modus.

Nicht zu verwechseln ist das Firmware-Passwort mit der vierstelligen “iCloud-PIN“, die nach dem Sperren eines Macs durch die Funktion "Find My Mac" angezeigt wird. Der grundsätzliche Wirkmechanismus ist jedoch gleich, der Mac setzt seine Arbeit erst fort, wenn die korrekte PIN eingegeben wurde.

3 Weiterführende Informationen

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Clients unter macOS" finden sich unter anderem in folgenden Veröffentlichungen:

[NIST800179] NIST Special Publication 800-179

Guide to Securing Apple OS X 10.10 Systems for IT Professional

SYS.3: Mobile Devices

Umsetzungshinweise zum Baustein SYS.3.1 Laptops

1 Beschreibung

1.1 Einleitung

Ein Laptop ist ein mobiler PC. Er hat eine kompakte Bauform, integriert Peripheriegeräte wie Tastatur und Bildschirm und kann über Akkus zeitweise unabhängig von externer Stromversorgung betrieben werden. Er verfügt über eine Festplatte und meist auch über weitere Speichergeräte, wie DVD- oder Blu-ray-Laufwerke, sowie über Schnittstellen zur Kommunikation über verschiedene Medien, beispielsweise LAN, USB, Firewire, WLAN. Laptops können mit allen üblichen Betriebssystemen wie Windows, Apple macOS oder Linux betrieben werden.

Da Laptops häufig mobil genutzt werden, sind sie oft nicht direkt am LAN der Institution angeschlossen, sondern wählen sich per Virtual Private Network (VPN) über das Internet oder andere Datennetze ein, um so auf die Ressourcen des LANs zuzugreifen. Auch die Infrastruktur einer klassischen Büroumgebung, wie kontrollierbare Umwelteinflüsse, eine stabile Stromversorgung oder zutrittsgeschütze Bereiche, kann für den mobilen Einsatz von Laptops nicht vorausgesetzt werden.

Für den Laptop wird vorausgesetzt, dass er innerhalb eines bestimmten Zeitraums nur von einem Benutzer gebraucht wird. Ein anschließender Benutzerwechsel wird berücksichtigt.

1.2 Lebenszyklus

Planung und Konzeption

Um Laptops sicher und effektiv in Institutionen einsetzen zu können, sollte ein Konzept erstellt werden, das auf den Sicherheitsanforderungen für die bereits vorhandenen IT-Systeme sowie den Anforderungen aus den geplanten Einsatzszenarien beruht (siehe SYS.3.1.M1 *Regelungen zur Nutzung von Laptops*). Darauf aufbauend ist die Laptop-Nutzung zu regeln und es sind Sicherheitsrichtlinien dafür zu erarbeiten (siehe SYS.3.1.M6 *Sicherheitsrichtlinien für Laptops*).

Beschaffung

Für die Beschaffung von Laptops müssen die aus dem Konzept resultierenden Anforderungen an die jeweiligen Produkte formuliert und darauf basierend geeignete Produkte ausgewählt werden (siehe SYS.3.1.M15 *Geeignete Auswahl von Laptops*).

Umsetzung

Es ist notwendig, die Betriebssystem- und Software-Komponenten sorgfältig auszuwählen und zu installieren. Die hier durchzuführenden Schutzmaßnahmen sind abhängig vom eingesetzten Betriebssystem und werden daher in den spezifischen Bausteinen beschrieben, beispielsweise *SYS.2.2.3 Client unter Windows 10* oder SYS 2.3 *Clients unter Unix*. Je nach Sicherheitsanforderungen müssen die beteiligten Software-Komponenten unterschiedlich konfiguriert werden. Die hier zu treffenden Maßnahmen sind ebenfalls abhängig vom eingesetzten Betriebssystem.

Betrieb

Eine der wichtigsten Sicherheitsmaßnahmen beim Betrieb heutiger Laptops ist es, ein Antivirenprogramm zu installieren und es permanent zu aktualisieren (siehe SYS.3.1.M4 *Einsatz von Antivirenprogrammen*). Da bei Laptops ein relativ hohes Diebstahlsrisiko besteht, sollten die Daten auf dem Laptop verschlüsselt (siehe SYS.3.1.M13 *Verschlüsselung von Laptops*) und Diebstahlsicherungen genutzt werden (siehe SYS.3.1.M18 *Einsatz von Diebstahl-Sicherungen*).

Sofern Laptops bei mobiler Nutzung direkt an das Internet angeschlossen werden, ist es unabdingbar, sie durch eine restriktiv konfigurierte Personal Firewall gegen Angriffe aus dem Netz zu schützen (siehe SYS.3.1.M3 *Einsatz von Personal Firewalls für Clients*). Auch muss die Kommunikation in andere Netze oder zu anderen Geräten (siehe SYS.3.1.M9 *Sicherer Fernzugriff von unterwegs)* sowie ins interne Netz (siehe SYS.3.1.M8 *Sicherer Anschluss von Laptops über Datennetze*) abgesichert werden.

Häufig ist es notwendig, die Datenbestände zwischen Server und Laptop miteinander zu synchronisieren. Dabei muss gewährleistet werden, dass jederzeit erkennbar ist, ob sich die aktuellste Version der bearbeiteten Daten auf dem Laptop oder dem Server befindet (siehe SYS.3.1.M10 *Abgleich der Datenbestände von Laptops*).

Um einen Überblick über die aktuell in das lokale Netz eingebundenen Laptops zu behalten und die Konfiguration aller Laptops jederzeit nachvollziehen zu können, sollten diese Geräte zentral verwaltet werden (siehe SYS.3.1.M16 *Zentrale Administration von Laptops*). Je nach der in einem Gebäude oder Büroraum gegebenen baulichen Sicherheit kann es auch sinnvoll oder sogar notwendig sein, Diebstahl-Sicherungen zu verwenden (siehe SYS.3.1.M18 *Einsatz von Diebstahl-Sicherungen*). Auch sind Laptops unterwegs geeignet aufzubewahren (siehe SYS.3.1.M14 *Geeignete Aufbewahrung von Laptops*).

Notfallvorsorge

Die Vorgehensweise und der erforderliche Umfang der Datensicherung richten sich nach dem Einsatzszenario des Laptops (siehe SYS.3.1.M5 *Datensicherung*).

Aussonderung

Wird ein Laptop ausgesondert, ist darauf zu achten, dass keine schützenswerten Informationen mehr auf der Festplatte vorhanden sind (siehe SYS.3.1.M7 *Geregelte Übergabe und Rücknahme eines Laptops*).

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Laptops" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

SYS.3.1.M1 Regelungen zur mobilen Nutzung von Laptops

Laptops, die ausschließlich innerhalb einer hauseigenen Liegenschaft eingesetzt werden, sind oft bereits durch infrastrukturelle Sicherheitsmaßnahmen ausreichend vor Missbrauch und Diebstahl geschützt. Häufig sollen aber Laptops auch außerhalb der Institution eingesetzt werden, z. B. bei Dienstreisen oder Telearbeit. Um die Geräte auch in diesen Fällen ausreichend schützen zu können, muss die Mitnahme von Datenträgern und IT-Komponenten klar geregelt werden.

Dabei muss festgelegt werden,

- welche IT-Komponenten bzw. Datenträger außer Haus mitgenommen werden dürfen,
- wer IT-Komponenten bzw. Datenträger mitnehmen darf,
- welche grundlegenden Sicherheitsmaßnahmen dabei beachtet werden müssen (z. B. Virenschutz, Verschlüsselung schützenswerter Daten, Aufbewahrung).

Die Art und der Umfang der anzuwendenden Sicherheitsmaßnahmen für Laptops hängen einerseits vom Schutzbedarf der darauf gespeicherten IT-Anwendungen und Daten und andererseits von der Sicherheit der Einsatz- bzw. Aufbewahrungsorte ab.

Grundsätzlich sollte für alle Laptops, die extern eingesetzt werden sollen, eine entsprechende Genehmigung eingeholt werden.

Außerhalb der institutionseigenen Liegenschaften sind die Benutzer für den Schutz der ihnen anvertrauten Laptops verantwortlich. Darauf und auf die zu ergreifenden Vorsichtsmaßnahmen sind sie hinzuweisen.

SYS.3.1.M2 Zugriffsschutz am Laptop [Benutzer]

Jeder Laptop sollte mit einem Zugriffsschutz versehen werden, der verhindert, dass er unberechtigt benutzt werden kann. So ist es in nahezu allen Betriebssystemen möglich, Anmeldepasswörter einzurichten und diese mit geeigneten Restriktionen zu versehen (z. B. Mindestlänge, Lebensdauer). Da diese Bordmittel nur begrenzt sicher sind, empfiehlt es sich bei Laptops mit schützenswerten Daten, zusätzliche Sicherheitshard- oder -software einzusetzen. Dazu gehören beispielsweise Chipkarten oder Token, die die Authentisierung absichern.

Sind die Daten auf dem Laptop nicht verschlüsselt, sollte verboten werden, dass Mitarbeiter schutzbedürftige Informationen auf der Festplatte speichern (siehe SYS3.1.M13 *Verschlüsselung von Laptops*). Stattdessen sollten sie auf verschlüsselten mobilen Datenträgern gespeichert werden, z. B. USB-Sticks. Diese sind dann getrennt vom Laptop aufzubewahren.

Bei kurzen Arbeitsunterbrechungen muss unbedingt ein Zugriffsschutz aktiviert werden, z. B. ein kennwortgeschützter Bildschirmschoner. Ist es absehbar, dass die Unterbrechung länger dauert, ist der Laptop auszuschalten.

SYS.3.1.M3 Einsatz von Personal Firewalls

Personal Firewalls kontrollieren und unterbinden Zugriffe auf Clients über angebundene IT-Netze bzw. von Clients auf diese Netze. Je nach Art des Netzdienstes und der Richtung des Verbindungsaufbaus kann von der Personal Firewall des Clients ein Kommunikationsaufbau gestattet oder abgewiesen werden. Eine Personal Firewall könnte beispielsweise so konfiguriert sein, dass alle Verbindungen, die von dem Client aufgebaut werden, erlaubt und alle von außen ankommenden Anfragen blockiert werden.

Personal Firewalls können nach unterschiedlichen Prinzipien arbeiten:

- Zustandslose (stateless) Personal Firewalls entscheiden anhand von Eigenschaften der übertragenen Datenpakete (z. B. Quell- und Ziel-Adressen oder Ports) darüber, ob die Verbindung erlaubt oder abgewiesen werden soll. Im Wesentlichen wird hierzu die Absender- bzw. Zieladresse und Port-Nummer des Dienstes herangezogen. Zustandslose Personal Firewalls können oft mit präparierten Paketen umgangen werden.
- Kontextsensitive (stateful) Personal Firewalls berücksichtigen bei der Entscheidung auch vorangegangene Pakete. So kann eine kontextsensitive Personal Firewall ein zu prüfendes Paket in den Kontext einer Verbindung bringen und nur dann erlauben, wenn die Verbindung selbst zulässig ist. Nicht in den Verbindungskontext passende Pakete werden verworfen.
- Anwendungsfirewalls (Application firewall) können Netzverkehr auf Basis der Anwendung, die eine Verbindung aufbauen will, prüfen. Dazu verfügt die Applikations-Firewall über eine Whitelist, in der die kommunikationsberechtigten Anwendungen eingetragen sind. Anwendungen, die nicht auf der Whitelist stehen, können keine Verbindungen über das Netz aufbauen oder entgegennehmen.

Viele Betriebssysteme beinhalten bereits eine Personal Firewall. Diese braucht oft nur aktiviert zu werden. Je nach Betriebssystem sind unterschiedlich umfangreiche Funktionen verfügbar. Zusätzlich werden von diversen Drittherstellern Sicherheitslösungen ("Security Suite") angeboten, die unter anderem eine Personal Firewall beinhalten. Oft sind die im Betriebssystem integrierten Personal Firewalls im Gegensatz zu den Sicherheitslösungen weniger umfangreich und weniger komfortabel. Dafür können diese bordeigenen Lösungen sofort aktiviert werden und es entstehen keine zusätzlichen Kosten für die Beschaffung. Es ist zu entscheiden, ob die bordeigene Personal Firewall oder eine Lösung von einem Drittheresteller eingesetzt werden soll, auf einen Mischbetrieb sollte verzichtet werden.

Einsatzumgebungen

Als alleinige Maßnahme um ein Behörden- oder Unternehmensnetz vor Angriffen aus dem Internet zu schützen genügen Personal Firewalls nicht. Der alleinige Einsatz von Personal Firewalls bringt folgende Nachteile mit sich:

- Alle direkt ans Internet angeschlossenen Clients müssen besonders gehärtet werden, d. h. die potenziellen Schwachstellen des Betriebssystems müssen behoben werden, da der Client nicht durch andere IT-Systeme, wie Sicherheitsgateways, geschützt wird.
- Wie bei jeder dezentral eingesetzten Software ist es aufwändig, die einzelnen Personal Firewalls zu managen und die jeweiligen Protokolle auszuwerten.

Es sollte geprüft werden, auf welchen Laptops und mit welchen Rahmenbedingungen eine Personal Firewall eingesetzt werden soll. Eventuell kann auf sie verzichtet werden, wenn die Laptops nur in einem LAN mit einem schützenden Sicherheitsgateway betrieben werden. Bei einem höheren Schutzbedarf sollte auch in diesem Fall der Einsatz von Personal Firewalls jedoch geprüft werden.

Wenn Laptops direkt an das Internet angeschlossen werden, sollten sie unbedingt durch eine restriktiv konfigurierte Personal Firewall gegen Angriffe aus dem Netz geschützt werden.

Aufgrund des vielfältigen Funktionsumfangs der verschiedenen Varianten von Personal Firewalls und deren Komplexität muss sichergestellt sein, dass sie nur durch geeignetes Personal administriert werden. Die Benutzer sollten sie weder selber konfigurieren müssen noch die Einstellungen ändern dürfen.

Personal Firewalls als Bestandteil einer Sicherheitslösung (Security Suite)

Personal Firewalls werden inzwischen von vielen Herstellern angeboten. Institutionen müssen dafür meistens eine Lizenz kaufen. Personal Firewalls werden häufig in Fachzeitschriften getestet. Die Ergebnisse dieser Tests können dabei helfen, ein geeignetes Produkt zu finden.

Prinzipiell ist es z. B. bei umfangreichen Sicherheitslösungen von Drittherstellern, die eine Personal Firewall beinhalten, möglich, mit ihnen die Clients auf Schadsoftware zu überprüfen, die über E-Mail, Java, ActiveX oder ähnliche Mechanismen übertragen werden kann. Hierfür können Mechanismen wie Sandboxing eingesetzt werden, mit denen der Zugriff von Applikationen, die vom Internet auf das lokale System übertragen werden (Java, ActiveX etc.), eingeschränkt werden kann. Mit diesen oft umfangreichen Sicherheitslösungen wird die Prüfung auf Schadsoftware dezentralisiert und damit das zentrale Firewall-System entlastet. Ein weiterer Vorteil liegt darin, dass die Problematik der Filterung von verschlüsselten Daten auf der zentralen Firewall umgangen werden kann.

Konfiguration

Bei Konfiguration und Betrieb einer Personal Firewall auf Laptops sollten folgende Aspekte berücksichtigt werden:

- Die Filterregeln sollten so restriktiv wie möglich eingestellt werden. Dabei gilt der Grundsatz: Alles was nicht ausdrücklich erlaubt ist, ist verboten. Es wird empfohlen, dass abgehende Verbindungen nur von dafür zugelassenen Anwendungen oder Diensten aufgebaut werden dürfen. Basierend auf der IP-Adresse des Zielsystems, der Port-Nummer des benötigten Dienstes und der zugreifenden Anwendung bzw. des zugreifenden Dienstes könnten folgende vom Client aufgebaute Zugriffe beschränkt bzw. erlaubt werden:Ankommende Verbindungen sollten auf die für Fernwartung, Software-Verteilung, Systemaktualisierung und Überwachung der erforderlichen Dienste und die hierfür verwendeten Server-Systeme beschränkt werden.
    - zu Datei-Servern, zum Internet für den Browser über das Sicherheitsgateway,
    - zum Internet für den Browser über das Sicherheitsgateway,
    - zum E-Mail- und Kalender-Server für die E-Mail- und Kalenderanwendung,
    - zu Update-Servern im lokalen Netz, um das Betriebssystem, Anwendungen und insbesondere das Virenschutzprogramm zu aktualisieren,
    - Kommunikation zum eventuell vorhandenen zentralen Protokollierungsdienst für alle Dienste und Anwendungen, die Meldungen protokollieren.
- Ankommende Verbindungen sollten auf die für Fernwartung, Software-Verteilung, Systemaktualisierung und Überwachung der erforderlichen Dienste und die hierfür verwendeten Server-Systeme beschränkt werden.

- Die Filterregeln der Personal Firewall sollten nach der erstmaligen Konfiguration daraufhin getestet werden, ob die erlaubten Ereignisse zugelassen und unerlaubte Ereignisse unterbunden werden.
- Die korrekte Konfiguration der Filterregeln sollte in sporadischen Abständen überprüft werden, wenn die Installation des Clients nicht ohnehin regelmäßig gelöscht und anhand eines Festplatten-Abbildes (Images) erneut aufgespielt wird.
- Falls das verwendete Produkt diese Möglichkeit bietet, sollten die Regeln der Personal Firewall auch speziellen Programmen zugeordnet werden. Dadurch kann erkannt und verhindert werden, dass ein anderes als die vorgesehenen Client-Programme sich mit Rechnern im Internet verbindet.

- Da viele der Prüfmechanismen einer Personal Firewall auf aktuellen Erkenntnissen beruhen, müssen vom Hersteller veröffentlichte Patches bzw. Updates regelmäßig eingespielt werden. Dabei ist sicherzustellen, dass die dafür erforderlichen Dateien von einer vertrauenswürdigen Quelle bezogen werden, beispielsweise direkt vom Hersteller.
- Die Personal Firewall muss so konfiguriert werden, dass die Benutzer nicht durch viele Warnmeldungen belästigt werden, die sie nicht interpretieren können.
- Falls das verwendete Produkt diese Möglichkeit bietet, sollten sicherheitsrelevante Ereignisse protokolliert werden. Die Protokolldaten sollten regelmäßig durch fachkundiges Personal ausgewertet werden.

Einige Produkte verfügen über die Möglichkeit, mit einer sehr restriktiven Grundkonfiguration zu starten und danach die Einstellungen im laufenden Betrieb zu verfeinern. Dabei wird jedes Mal, wenn ein sicherheitsrelevantes Ereignis auftritt, für das bisher noch keine eindeutige Regel existiert, der Benutzer gefragt, ob dieses Ereignis zulässig ist. Ein Beispiel für ein solches sicherheitsrelevantes Ereignis ist der Zugriff eines bestimmten installierten Programms auf das Internet. Auf der Grundlage der Antworten des Benutzers ermittelt die Personal Firewall Schritt für Schritt die gewünschte Konfiguration, z. B. die Filterregeln.

Der Vorteil dieser inkrementellen Konfiguration ist, dass dadurch die Administration nicht mehr so komplex ist. Nachteilig ist jedoch, dass Benutzer oft nicht beurteilen können, ob ein bestimmtes Ereignis zulässig ist oder nicht. Die inkrementelle Konfiguration der Personal Firewall kann daher nur dann empfohlen werden, wenn den Benutzern entweder präzise Vorgaben gemacht werden, wie sie auf Rückfragen des Programms antworten sollen oder wenn dies unter Anleitung eines Administrators erfolgt, z. B. durch telefonische Rückfragen.

SYS.3.1.M4 Einsatz von Antivirenprogrammen [Benutzer]

Um sich vor Schadprogrammen zu schützen, können unterschiedliche Wirkprinzipien genutzt werden (siehe OPS.1.1.4 *Schutz vor Schadprogrammen*). Antivirenprogramme, die IT-Systeme nach sämtlichen bekannten Schadprogrammen durchsuchen, sind ein wirksames Mittel in der Schadprogramm-Prävention. Daher müssen sie abhängig vom installierten Betriebssystem und anderer vorhandener Schutzmechanismen installiert und aktiviert sein.

Regelmäßige Untersuchung des gesamten Datenbestands

Auch wenn das Antivirenprogramm bei jedem Dateizugriff auf Schadprogramme prüft, müssen regelmäßig alle Dateien auf dem Laptop durchsucht werden. So können auch Schadprogramme gefunden werden, für die es noch keine Erkennungssignatur gab, als sie gespeichert wurden. In derartigen Fällen muss beispielsweise untersucht werden, ob das Schadprogramm bereits vertrauliche Daten gesammelt, Schutzfunktionen deaktiviert oder Code aus dem Internet nachgeladen hat.

Aus Performance-Gründen sollte der Datenbestand nur vollständig überprüft werden, wenn die IT-Ressourcen nicht stark beansprucht sind. Ideal ist es, wenn die Software überwacht, ob der Laptop ausgelastet ist und dessen "Arbeitspausen" automatisch nutzt, um ihn zu überprüfen. Das Antivirenprogramm könnte z. B. auch mit dem Start des Bildschirmschoners gekoppelt werden.

Datenaustausch und Datenübertragung

Daten, die versendet werden sollen, müssen unmittelbar vor dem Versand auf Schadprogramme geprüft werden. Analog müssen empfangene Daten unmittelbar nach dem Empfang auf Schadprogramme geprüft werden. Diese Überprüfungen sind sowohl erforderlich, wenn auf Datenträger zugegriffen wird als auch bei der Datenübertragung über Kommunikationsverbindungen. Sie sollten so weit wie möglich automatisiert werden.

Wechselwirkungen mit Verschlüsselungstechniken

Wenn Verschlüsselungstechniken eingesetzt werden, ist zu bedenken, wie sich das auf den Schutz vor Schadprogrammen auswirkt. Werden Daten verschlüsselt, so können Systemkomponenten bzw. Anwendungen auf diese Daten nicht zugreifen, solange sie nicht über die entsprechenden Schlüssel verfügen. Das impliziert, dass ein Antivirenprogramm entweder im Kontext des Benutzers laufen oder mit den entsprechenden kryptografischen Schlüsseln ausgestattet werden muss, um eine verschlüsselte Datei auf Schadprogramme überprüfen zu können. Wird jedoch die Benutzer-Kennung, unter der das Antivirenprogramm ausgeführt wird, mit den entsprechenden kryptografischen Schlüsseln ausgestattet, entstehen neue Sicherheitsrisiken, die es zu vermeiden gilt. Daher wird der Einsatz eines residenten Antivirenprogramms empfohlen, das die Prüfung auf Schadprogramme im Benutzer-Kontext bei jedem Zugriff auf eine Datei durchführt.

Schutz vor unerlaubter Deaktivierung oder Änderung

Die Antivirenprogramme auf den Laptops müssen so konfiguriert sein, dass die Benutzer keine sicherheitsrelevanten Einstellungen verändern können. Insbesondere muss sichergestellt sein, dass die Benutzer sie nicht deaktivieren können.

SYS.3.1.M5 Datensicherung [Benutzer]

Laptops sind in aller Regel nicht permanent in ein Netz eingebunden. Der Datenaustausch mit anderen IT-Systemen erfolgt üblicherweise über temporäre Netzanbindungen. Letztere können beispielsweise durch ein Virtual Private Network (VPN) oder direkten Anschluss an ein LAN nach Rückkehr zum Arbeitsplatz realisiert sein. Anders als bei stationären Clients ist es daher bei Laptops meist unvermeidbar, dass Daten zumindest zeitweise lokal anstatt auf einem zentralen Server gespeichert werden. Deshalb ist mithilfe geeigneter Datensicherungsmaßnahmen vorzubeugen, dass Daten verloren gehen.

Generell bieten sich folgende Verfahren zur Datensicherung an:

- **Datensicherung auf externen Datenträgern**
  Der Vorteil dieses Verfahrens ist, dass die Datensicherung an nahezu jedem Ort und zu jeder Zeit erfolgen kann. Nachteilig ist, dass zusätzliche Datenträger, z. B. externe Festplatten, mitgeführt werden müssen und dass für den Benutzer mehr Aufwand für die ordnungsgemäße Handhabung der Datenträger entsteht. Die Datenträger sollten eine ausreichende Speicherkapazität besitzen, sodass der Benutzer nicht mehrere Datenträger pro Sicherungsvorgang verwenden muss. Bei unverschlüsselter Datenhaltung ergibt sich außerdem die Gefahr, dass Datenträger abhandenkommen und dadurch schützenswerte Daten kompromittiert werden können. Die Datenträger und der Laptop sollten möglichst getrennt voneinander aufbewahrt werden, damit bei Verlust oder Diebstahl des Laptops nicht beide abhandenkommen.
  Die Speicherung auf externen Datenträgern zur Datensicherung bietet sich insbesondere an, wenn auch der Datenaustausch mit anderen IT-Systemen über externe Datenträger erfolgt. Diese beiden Prozesse können auch kombiniert werden. Nach Rückkehr zum Arbeitsplatz müssen die Datensicherungen auf den Datenträgern in das Backup-System oder in das Produktivsystem bzw. die zentrale Datenhaltung der Institution eingepflegt werden.
- **Datensicherung über temporäre Netzverbindungen**
  Wenn es möglich ist, den Laptop regelmäßig an ein Netz anzuschließen, beispielsweise über VPNs, können die lokalen Daten auch über die Netzanbindung gesichert werden. Vorteilhaft ist hier, dass der Benutzer keine Datenträger verwalten und mitführen muss. Weiterhin lässt sich das Verfahren weitgehend automatisieren, beispielsweise kann die Datensicherung beim Einsatz von VPNs nach jedem Einwahlvorgang automatisch gestartet werden.
  Entscheidend bei der Datensicherung über eine temporäre Netzverbindung ist, dass deren Bandbreite für das Volumen der zu sichernden Daten ausreichen muss. Die Datenübertragung darf nicht zu lange dauern und nicht zu übermäßigen Verzögerungen führen, wenn der Benutzer gleichzeitig auf entfernte Ressourcen zugreifen muss. Einige Datensicherungsprogramme bieten daher die Möglichkeit an, lediglich Informationen über die Änderungen des Datenbestands seit der letzten Datensicherung über die Netzverbindung zu übertragen. In vielen Fällen kann hierdurch das zu transportierende Datenvolumen stark reduziert werden.
  Die Datensicherungssoftware muss unerwartete Verbindungsabbrüche erkennen und ordnungsgemäß behandeln. Die Konsistenz der gesicherten Daten darf durch Verbindungsabbrüche nicht beeinträchtigt werden.

Bei beiden Verfahren zur Datensicherung ist es wünschenswert, das Volumen der zu sichernden Daten zu minimieren. Neben verlustfreien Kompressionsverfahren, die in vielen Datensicherungsprogrammen integriert sind, können auch inkrementelle oder differenzielle Sicherungsverfahren eingesetzt werden. Hierdurch erhöht sich jedoch eventuell der Aufwand für die Wiederherstellung einer Datensicherung.

Die Datensicherung sollte möglichst weitgehend automatisiert werden, sodass die Benutzer nur wenige Aktionen selbst durchführen müssen. Wenn die Mitarbeit der Benutzer erforderlich ist, sollten sie dazu verpflichtet werden, Datensicherungen regelmäßig durchzuführen. Schließlich sollte sporadisch geprüft werden, ob angelegte Datensicherungen wiederhergestellt werden können.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Laptops".

SYS.3.1.M6 Sicherheitsrichtlinien für Laptops [Leiter IT]

Laptops, die außerhalb der eigenen Institution eingesetzt werden, sind mehr Risiken ausgesetzt, als solche, die sich innerhalb geschützter Räumlichkeiten befinden. Es gibt aber Möglichkeiten, sie auch unterwegs zu schützen. Es sollte eine Sicherheitsrichtlinie erstellt werden, in der alle umzusetzenden Sicherheitsmechanismen beschrieben sind. Zusätzlich sollte für die Benutzer ein kurzes und übersichtliches Merkblatt erstellt werden, das beschreibt, wie Laptops sicher genutzt werden.

Sensibilisierung der Benutzer

Je kleiner und leichter IT-Systeme werden, desto leichtfertiger wird erfahrungsgemäß damit umgegangen. Daher sollten Mitarbeiter für den Wert mobiler IT-Systeme und den Wert der darauf gespeicherten Informationen sensibilisiert werden. Sie sollten auch über die spezifischen Gefährdungen von Laptops aufgeklärt werden und die erforderlichen Maßnahmen kennen.

Die Mitarbeiter sollten auch darüber aufgeklärt werden, dass sie vertrauliche Informationen unterwegs nicht mit jedem austauschen und dies unterwegs auch nicht in Hör- und Sichtweite von Externen machen sollten. Insbesondere sollte die Identität des Kommunikationspartners hinterfragt werden, bevor detaillierte Auskünfte gegeben werden.

Regelungen zur Nutzung von Laptops

Für die sichere Benutzung von Laptops sind diverse Punkte zu regeln:

- Die Benutzer müssen darüber informiert sein, welche Informationen mit Laptops unterwegs verarbeitet werden dürfen. Die Daten sollten klassifiziert sein, um Einschränkungen für die Benutzer transparent zu machen. Dienstgeheimnisse dürfen nur dann auf Laptops verarbeitet werden, wenn hierfür geeignete und freigegebene Sicherheitsmechanismen eingesetzt werden.
- Daten, die ein hohes Maß an Sicherheit verlangen (z. B. Angebote, Konstruktionsdaten, Wirtschaftsdaten eines Unternehmens) sollten stets verschlüsselt auf dem Laptop abgelegt werden.
- Es ist zu klären, ob mobile Mitarbeiter von unterwegs Zugriff auf interne Daten ihrer Institution erhalten. Falls das vorgesehen ist, muss dieser Zugriff angemessen geschützt werden (siehe hierzu auch SYS.3.1.A9 Sichere Fernzugriff von unterwegs und SYS.3.1.A8 Sicherer Anschluss von Laptops an lokale Netze).
- Es muss geklärt werden, ob Laptops für private Zwecke benutzt werden dürfen.
- Die Benutzer sollten darauf hingewiesen werden, wie sie sorgfältig mit Laptops umgehen sollten, um einem Verlust oder Diebstahl vorzubeugen bzw. um eine lange Lebensdauer zu gewährleisten (z. B. Akkupflege, sichere Aufbewahrung außerhalb von Büro- oder Wohnräumen, Empfindlichkeit gegenüber zu hohen oder zu niedrigen Temperaturen).
- Es sollte geregelt sein, wie Laptops verwaltet, gewartet und weitergegeben werden.
- Bei jedem Benutzerwechsel müssen alle benötigten Passwörter gesichert weitergegeben werden.
- Laptops und deren Anwendungen können oft durch PINs oder Passwörter abgesichert werden. Diese Mechanismen sollten auch genutzt werden.
- Es sollte festgelegt werden, wie in öffentlichen Umgebungen gearbeitet werden darf (siehe INF.9 Mobiler Arbeitsplatz).
- Es sollte überlegt werden, zu protokollieren, wann und von wem welcher Laptop außer Haus eingesetzt wurden.

Werden Laptops in fremden Büroräumen benutzt, so sind die Sicherheitsregelungen der besuchten Institution zu beachten. In fremden Räumlichkeiten wie Hotelzimmern sollten sie nicht ungeschützt ausliegen. Alle Passwort-Schutzmechanismen sollten spätestens jetzt aktiviert werden. Wenn die Geräte in einem Schrank eingeschlossen werden, behindert das zumindest Gelegenheitsdiebe.

Entsorgung von Datenträgern

Es ist zu regeln, wie ausgediente Datenträger und Geräte entsorgt werden sollen. Ein unterwegs defekter werdender Laptop muss wieder mit zurück transportiert werden und darf nicht unterwegs entsorgt werden. Das gilt auch, wenn die Datenträger defekt sind, da Experten auch hieraus wieder wertvolle Informationen zurückgewinnen können.

Nutzungsverbot

Es sollte überlegt werden, ob in allen oder bestimmten Bereichen einer Institution eingeschränkt oder verboten werden sollte, Laptops zu benutzen oder mitzubringen. Das kann z. B. für Besprechungsräume sinnvoll sein. Wenn die Sicherheitsrichtlinie der Institution es nicht zulässt, dass Laptops mitgebracht werden dürfen, muss an allen Eingängen deutlich darauf hingewiesen werden. Das sollte dann auch regelmäßig kontrolliert werden.

SYS.3.1.M7 Geregelte Übergabe und Rücknahme eines Laptops [Benutzer]

Laptops werden je nach Einsatzzweck nur von einem einzelnen Mitarbeiter eingesetzt, z. B. als Arbeitsplatzrechner, der auch mobil genutzt wird. Sie können aber auch abwechselnd von verschiedenen Mitarbeitern benutzt werden, z. B. für Präsentationen. Je nach Einsatzart ergeben sich verschiedene Sicherheitsanforderungen. Daher sollte Einsatzzweck und -art sorgfältig geplant werden.

Ist der Laptop ein Arbeitsplatzrechner, wird er typischerweise abwechselnd mobil und stationär benutzt. Dabei kann auf verschiedene Netze zugegriffen werden. Dafür müssen die Laptops so abgesichert sein, dass auf der einen Seite durch den mobilen Einsatz weder wichtige Daten des Laptops kompromittiert, manipuliert oder verloren werden können. Auf der anderen Seite dürfen über die Laptops keine Gefährdungen in die internen Netze eingeschleppt werden.

Wenn Laptops abwechselnd von verschiedenen Personen genutzt werden, ist eine geregelte Übergabe extrem wichtig. Damit dies gut funktioniert, sollte ein Laptop-Pool eingerichtet werden (siehe SYS.3.1.A17 *Sammelaufbewahrung tragbarer IT-Systeme*).

Wird ein Laptop übergeben oder zurückgenommen, sind folgende Punkte zu beachten:

Übergabe:

- Der neue Benutzer wird aufgefordert, direkt bei der Übergabe das alte Passwort des Laptops bzw. das Standardpasswort zu ändern.
- Dem neuen Benutzer sollte ein Merkblatt für den sicheren Umgang mit dem tragbaren IT-System übergeben werden.
- Damit jederzeit nachvollziehbar ist, wo sich die Geräte befinden, sollte jeder Benutzer mit Namen, Organisationseinheit, Telefonnummer, Einsatzzweck in ein Übergabe-/Rücknahmejournal eingetragen werden.

Rücknahme bzw. Weitergabe:

- Der Benutzer gibt sein zuletzt benutztes Passwort bekannt bzw. stellt ein Standardpasswort ein.
- Der Laptop muss mittels eines aktuellen Antivirenprogramms auf Malware überprüft werden.
- Der Benutzer muss sicherstellen, dass vor Übergabe des Gerätes sämtliche Daten, die der Benutzer noch benötigt, auf ihm zugängliche Datenträger übertragen werden. Darüber hinaus hat der Benutzer dafür zu sorgen, dass sämtliche von ihm erzeugten Dateien und Daten gelöscht werden. Hierfür müssen geeignete Tools vorhanden sein.
- Die Rückgabe des Laptops und das Ergebnis der Virensuche werden dokumentiert. Die Vollständigkeit des Gerätes, des Zubehörs und der Dokumentation ist sicherzustellen.
- Um sicherzustellen, dass die definierte sichere Grundkonfiguration vorhanden ist und sich keine schützenswerten Dateien mehr auf dem Laptop befinden, sollte er mithilfe einer Referenzinstallation neu installiert werden.

Die vorgesehenen Einsatzarten der Laptops sind zu dokumentieren.

SYS.3.1.M8 Sicherer Anschluss von Laptops an Datennetze [Benutzer]

Es ist wichtig festzulegen, welche Regelungen beim Anschluss von Laptops an eigene und fremde LANs und an das Internet zu beachten sind. Es sollte vermieden werden, dass dadurch der sichere Betrieb des eigenen LANs und anderer damit gekoppelter IT-Systeme beeinträchtigt wird, z. B. durch eingeschleppte Schadsoftware.

Wenn ein Laptop nach einem externen Einsatz wieder an das Unternehmens- bzw. Behördennetz angeschlossen werden soll, so ist zunächst durch eine gründliche Überprüfung mit aktuellen Virensignaturen sicherzustellen, dass dieser Laptop nicht infiziert ist.

Kopplung mit anderen IT-Systemen

Über Laptops werden auch häufig Daten mit anderen IT-Systemen ausgetauscht, etwa mit denen von Geschäftspartnern. Auch um auf das Internet zugreifen zu können, ist es häufig erforderlich, das eigene Gerät mit anderen IT-Systemen zu koppeln. Das kann auf verschiedene Arten erfolgen, je nachdem, welche Techniken die beteiligten Geräte unterstützen, beispielsweise über Bluetooth- oder WLAN-Schnittstellen. Hier müssen zum einen die Übertragungstechniken sicher eingesetzt werden, zum anderen muss der eigene Laptop sicher konfiguriert sein. Dazu gehören Sicherheitsmaßnahmen wie z. B. Zugriffsschutz, Benutzerauthentisierung, Virenschutz, Personal Firewall, restriktive Datei- und Ressourcenfreigabe auf Betriebssystemebene und eine lokale Verschlüsselung.

Soll ein Laptop an fremde Netze oder an das Internet angeschlossen werden, so sollte er grundsätzlich über eine Personal Firewall abgesichert werden (siehe SYS.3.1.M3 *Einsatz von Personal Firewalls für Clients*).

In allen Institutionen sollte klar geregelt sein, auf welche Daten von unterwegs zugegriffen werden darf und auf welche nicht. Vor allem muss allen Benutzern bekannt sein, unter welchen Randbedingungen sie Daten über externe Netze oder direkt mit fremden IT-Systemen austauschen dürfen.

Zertifikate/MAC-Adressen

Es sollte sichergestellt sein, dass nicht jeder beliebige Laptop sich an ein LAN anmelden kann. Bevor einem Laptop gestattet wird, auf ein LAN zuzugreifen, sollte er sich erfolgreich gegenüber einem Authentikationsserver authentisiert haben.

Um zu überprüfen, welche Geräte grundsätzlich zum Netzzugriff berechtigt sind, können beispielsweise Geräte-Zertifikate oder MAC-Adressen benutzt werden. Zu beachten ist hierbei allerdings, dass MAC-Adressen gefälscht werden können und deshalb nicht als alleiniges Authentisierungskriterium herangezogen werden sollten.

Zugriffsbeschränkungen

Es muss sichergestellt werden, dass ein VPN-Nutzer ausschließlich auf die zur Aufgabenerledigung notwendigen Dienste auf den Servern im LAN zugreifen kann. Das könnte beispielsweise durch eine benutzerbezogene Authentisierung auf Anwendungsebene und die Kontrolle des Verkehrs mithilfe von Paketfiltern (Paketfilter alleine sind aufgrund der Fälschbarkeit der IP-Adressen nicht ausreichend) sichergestellt werden.

DHCP

Über das Dynamic Host Configuration Protocol (DHCP) werden in IP-basierten Netzen den angeschlossenen Clients automatisch temporäre IP-Adressen sowie Routing- und DNS-Server-Informationen zugewiesen, sodass der Laptop zum Internet-Zugriff nicht mehr vom Benutzer konfiguriert werden muss.

Wenn DHCP aktiviert ist, wird einem IT-System automatisch eine gültige IP-Adresse für das lokale Netz zugewiesen, sodass es auf alle freigegebenen Ordner und Laufwerke zugreifen kann. Als Abhilfe sollte zum einen DHCP auf dem Laptop deaktiviert werden, wenn es nicht benötigt wird (dann müssen allerdings die IP-Adressen manuell verteilt werden). Zum anderen sollte bei der IP-Adressvergabe zusätzlich über die MAC-Adresse überprüft werden, ob der Client zum Netz zugelassen werden sollte.

Internet-Zugriffe

Es muss geregelt werden, ob Laptops direkt auf das Internet zugreifen dürfen. Der kritische Punkt hierbei ist, dass dabei die institutionseigenen Sicherheitsgateways und Sicherheitsmechanismen umgangen werden, dies also potenziell Sicherheitsprobleme nach sich ziehen kann.

Sofern Laptops bei mobiler Nutzung voraussehbar direkt an das Internet angeschlossen werden, ist es unabdingbar, sie durch eine restriktiv konfigurierte Personal Firewall gegen Angriffe aus dem Netz zu schützen. Der Virenschutz reicht alleine nicht aus, um alle zu erwartenden Angriffe abzuwehren. Ebenso ist es unbedingt erforderlich, die Software des Laptops auf aktuellem Stand zu halten und notwendige Sicherheitspatches zeitnah einzuspielen. Es ist sinnvoll, vor einem Zugriff auf das Produktivnetz zu überprüfen, ob Personal Firewall, andere Sicherheitsprogramme und Sicherheitspatches auf dem Laptop auf dem aktuellen Stand sind. Empfehlenswert ist es, über entsprechende Tools diese Prüfungen automatisiert durchzuführen, sodass bei Sicherheitsmängeln der Zugriff auf das interne Netz abgewiesen werden kann.

Die auf dem Laptop installierten Internet-Anwendungsprogramme, vor allem Browser und E-Mail-Clients, sollten mit sicheren Einstellungen betrieben werden. Es sollte administrativ unterbunden werden, dass der Benutzer voreingestellte Optionen verändern kann. Zusätzlich könnten Tools eingesetzt werden, die die Funktionalität des Browsers einschränken, sodass dieser in einer sandbox-ähnlichen Umgebung ausgeführt wird.

Für den Zugriff auf Internet-Anwendungen, bei denen schützenswerte Daten wie personenbezogene Daten, interne Informationen oder Kontendaten ausgetauscht werden, muss zumindest TLS zur Verschlüsselung genutzt werden.

Je nach Sicherheitsanforderungen und Einsatzumgebung kommen darüber hinaus verschiedene weitere Lösungsmöglichkeiten in Betracht:

- Verbot direkter Internet-Zugriffe: Diese Lösung hat natürlich den Vorteil, dass sie am einfachsten umzusetzen ist. Sie schränkt allerdings die Bewegungsfreiheit der Benutzer am meisten ein und wird daher nicht einfach durchzusetzen sein.
- Nutzung verschiedener Benutzerkennungen: Auf Betriebssystem-Ebene sollten in diesem Fall zwei verschiedene Benutzerkennungen genutzt werden, einmal für die allgemeine geschäftliche Nutzung und einmal für Internet-Zugriff. Hierbei sollte die Internet-Kennung nur über minimale Rechte verfügen.
- Nutzung verschiedener Partitionen/Betriebssysteminstallationen: Bei dieser Lösung werden verschiedene Partitionen angelegt, die möglichst stark getrennt sind, beispielsweise durch unterschiedliche Betriebs- und Dateisysteme. Je stärker die Trennung ist, desto höher sind die Hürden, mit denen verhindert wird, dass Schadsoftware aus dem Internet oder ähnliches die Produktiv-Umgebung beeinträchtigt.
- Virtuelle Maschinen: Hierbei kann das Internet ausschließlich über ein Betriebssystem benutzt werden, das in einer virtuellen Maschine betrieben wird (z. B. User Mode Linux, UML). Durch die virtuelle Maschine wird der benutzte Browser stärker vom eigentlichen Host-Betriebssystem getrennt, als das ohne virtuelle Maschine der Fall ist. Allerdings besteht bei dieser Variante das Restrisiko, dass Schadprogramme mittels Copy&Paste zwischen dem Host-Betriebssystem und dem virtuellen Betriebssystem hin und her kopiert werden können. Das Host-Betriebssystem könnte sich in diesem Fall bei der nächsten VPN-Einwahl in einem unsicheren Zustand befinden.
- Verwendung von Boot-CDs: Hierbei wird für die Internet-Nutzung von einem schreibgeschützten Medium wie einer CD-ROM eine internetfähige Betriebsumgebung hergestellt, wobei die Nutzbarkeit dadurch eingeschränkt wird, dass notwendige IP-Informationen eventuell von Hand eingetragen werden müssen. Hierzu kann beispielsweise Knoppix verwendet werden, eine komplett von einer CD lauffähige Zusammenstellung von GNU/Linux-Software (siehe [KNOP]).
- Internet-Zugriff nur über VPN (über Intranet über institutionseigenen Sicherheitsgateway ins Internet). Dies hat den Vorteil, dass gefährliche Inhalte aussortiert werden.

Nutzung von IrDA-Schnittstellen

Die Infrared Data Association (IrDA) hat Spezifikationen veröffentlicht, in der zunächst die unteren Schichten eines Protokolls für eine Infrarot-Schnittstelle definiert wurden. Dabei wird infrarotes Licht als Träger für den Datenaustausch über kurze Distanzen verwendet. Mittlerweile stellt IrDA auch höhere Protokolle für unterschiedliche Einsatzbereiche zur Verfügung. IrDA wird heute von allen gängigen Betriebssystemen unterstützt, allerdings verliert diese Schnittstelle im Vergleich zu Bluetooth, WLAN oder USB zunehmend an Bedeutung.

Im IrDA-Standard sind keine Sicherheitsmechanismen spezifiziert, die dagegen helfen, dass Angreifer den Datenverkehr mitschneiden können. Die Daten werden nur auf Protokollebene mittels Prüfsummenverfahren gegen Übertragungsfehler gesichert. Sicherheitsmechanismen wie Authentisierung, kryptografischer Integritätsschutz und Verschlüsselung sind nicht vorhanden. Daher sollte die IrDA-Schnittstelle nur bei konkretem Bedarf aktiviert werden.

Da die Kopplung nur in einem sehr eingeschränkten Bereich möglich ist, kann die Kommunikation meist nicht mitgehört werden. Das bestehende geringe Restrisiko aufgrund der Streustrahlung der IrDA-Komponenten kann durch zusätzliche Sicherheitsmechanismen (z. B. Authentisierung und Verschlüsselung auf Applikationsebene) oder den Ersatz von IrDA durch leitungsgebundene Übertragung weiter minimiert werden.

SYS.3.1.M9 Sicherer Fernzugriff von unterwegs [Benutzer]

Mit Laptops soll auch häufig unterwegs auf Daten aus dem internen Netz einer Institution zugegriffen werden. Dabei werden üblicherweise öffentliche Kommunikationsnetze benutzt. Da weder die Institution noch die mobilen Mitarbeiter großen Einfluss darauf nehmen können, ob die Vertraulichkeit, Integrität und Verfügbarkeit im öffentlichen Kommunikationsnetz gewahrt werden, sind zusätzliche Maßnahmen zum Schutz der Informationen erforderlich.

Generell muss die Datenübertragung zwischen einem Laptop und dem LAN einer Institution folgende Sicherheitsanforderungen erfüllen:

- Sicherstellung der Vertraulichkeit der übertragenen Daten: Die Datenübertragung muss ausreichend sicher verschlüsselt werden. Dazu gehört neben einem geeigneten Verschlüsselungsverfahren auch ein angepasstes Schlüsselmanagement mit periodischem Schlüsselwechsel.Sicherstellung der Integrität der übertragenen Daten: Mit den eingesetzten Übertragungsprotokollen muss es möglich sein, Veränderungen an den übertragenen Daten zu erkennen und eventuell sogar zu beheben. Solche Veränderungen können beispielsweise durch Übertragungsfehler (technische Probleme) oder durch absichtliche Manipulationen durch einen Angreifer entstehen. Zusätzlich kann der Einsatz digitaler Signaturen sinnvoll sein, um die Datenintegrität sicherzustellen.Sicherstellung der Authentizität der Daten: Bei der Übertragung der Daten muss vertrauenswürdig feststellbar sein, ob die Kommunikation zwischen den richtigen Teilnehmern stattfindet, sodass z. B. ein Man-in-the-Middle-Angriff ausgeschlossen werden kann. Zu diesem Zweck müssen sich die Kommunikationspartner gegenseitig authentisieren, beispielsweise über digitale Zertifikate.Sicherstellung der Nachvollziehbarkeit der Datenübertragung: Um eine Kommunikation nachvollziehbar zu machen, können Protokollierungsfunktionen eingesetzt werden, durch die sich nachträglich feststellen lässt, welche Daten wann und an wen übertragen wurden.
- Sicherstellung der Integrität der übertragenen Daten: Mit den eingesetzten Übertragungsprotokollen muss es möglich sein, Veränderungen an den übertragenen Daten zu erkennen und eventuell sogar zu beheben. Solche Veränderungen können beispielsweise durch Übertragungsfehler (technische Probleme) oder durch absichtliche Manipulationen durch einen Angreifer entstehen. Zusätzlich kann der Einsatz digitaler Signaturen sinnvoll sein, um die Datenintegrität sicherzustellen.Sicherstellung der Authentizität der Daten: Bei der Übertragung der Daten muss vertrauenswürdig feststellbar sein, ob die Kommunikation zwischen den richtigen Teilnehmern stattfindet, sodass z. B. ein Man-in-the-Middle-Angriff ausgeschlossen werden kann. Zu diesem Zweck müssen sich die Kommunikationspartner gegenseitig authentisieren, beispielsweise über digitale Zertifikate.Sicherstellung der Nachvollziehbarkeit der Datenübertragung: Um eine Kommunikation nachvollziehbar zu machen, können Protokollierungsfunktionen eingesetzt werden, durch die sich nachträglich feststellen lässt, welche Daten wann und an wen übertragen wurden.
- Sicherstellung der Authentizität der Daten: Bei der Übertragung der Daten muss vertrauenswürdig feststellbar sein, ob die Kommunikation zwischen den richtigen Teilnehmern stattfindet, sodass z. B. ein Man-in-the-Middle-Angriff ausgeschlossen werden kann. Zu diesem Zweck müssen sich die Kommunikationspartner gegenseitig authentisieren, beispielsweise über digitale Zertifikate.Sicherstellung der Nachvollziehbarkeit der Datenübertragung: Um eine Kommunikation nachvollziehbar zu machen, können Protokollierungsfunktionen eingesetzt werden, durch die sich nachträglich feststellen lässt, welche Daten wann und an wen übertragen wurden.
- Sicherstellung der Nachvollziehbarkeit der Datenübertragung: Um eine Kommunikation nachvollziehbar zu machen, können Protokollierungsfunktionen eingesetzt werden, durch die sich nachträglich feststellen lässt, welche Daten wann und an wen übertragen wurden.

Die Stärke der dazu erforderlichen Mechanismen richtet sich nach dem Schutzbedarf der übertragenen Daten. Wie adäquate kryptografische Verfahren und Systeme ausgewählt und eingesetzt werden können, ist in Baustein CON.1 *Kryptokonzept* beschrieben.

VPN

Zugriffe von einem Laptop von außerhalb auf das interne Netz sollten ausschließlich über ein Virtual Private Network (VPN) erfolgen (siehe NET.3.3 Virtual Private Networks (VPN)). Entsprechende Produkte sind von diversen Herstellern und für praktisch alle gebräuchlichen Plattformen verfügbar. Auf Daten oder Systeme mit hohem Schutzbedarf darf nicht ohne entsprechende Sicherungsmaßnahmen zugegriffen werden. Betreibt die Institution in ihrem Netz einen Filter für Schadsoftware, so sollte die Netzverbindung des Laptops durch diesen Filter geleitet werden, um so das Endgerät besser vor Schadsoftware zu schützen.

Ermöglicht es die Institution dienstliche E-Mails über das Internet mittels einer Web-Mail-Lösung abzurufen, so ist sicherzustellen, dass die E-Mails ausschließlich verschlüsselt vom Server auf den Laptop übertragen werden, z. B. mittels TLS. Allerdings muss hierbei nicht nur der Transportkanal, sondern auch das Endsystem selbst besonders abgesichert werden. Ein Laptop kann kompromittiert werden, wenn neben der VPN-Nutzung gleichzeitig auch noch Standardprotokolle wie z. B. HTTP oder SMTP im Internet genutzt werden. Daher sollten Laptops möglichst so abgesichert werden, dass bei bestehender VPN-Verbindung in das interne Netz keine anderen Verbindungen möglich sind (Split-Tunneling). Dabei muss gewährleistet sein, dass alle abgehenden Datenpakete des Clients in den Tunnel gehen und ausschließlich Datenpakete aus dem Tunnel akzeptiert werden.

Es sollte in diesem Zusammenhang auch darauf geachtet werden, dass neben dem VPN-gesicherten Laptop-Zugriff nicht gleichzeitig andere Netzzugriffe auf das interne Netz möglich sind. Insbesondere darf während der VPN-Zugriffe kein WLAN oder Bluetooth auf dem Laptop aktiv sein.

Authentisierung der VPN-Nutzung

Ein Laptop kann leicht in falsche Hände geraten. Bevor ein VPN aufgebaut wird, sollte die Authentizität des Benutzers mit starken Authentisierungsverfahren sichergestellt werden. Starke Authentisierungsverfahren sind beispielsweise Einmal-Passwort- oder Challenge-Response-Verfahren.

Protokollierung

Die Zugriffe auf Server-Dienste sollten protokolliert werden. Dabei sollte auch erkennbar sein, ob der Laptop-Zugriff aus der Institution oder von extern erfolgte. Vertiefende Informationen zur Protokollierung sind in OPS.1.1.6 Protokollierung zu finden.

Temporäre Daten

Es sollte sichergestellt werden, dass alle zwischengespeicherten Authentisierungsinformationen, die den Aufbau eines VPNs ermöglichen, nach dem Ende der VPN-Nutzung automatisch gelöscht werden. Das gilt sowohl für absichtlich als auch unabsichtlich beendete VPN-Verbindungen. Zusätzlich sollte beispielsweise bei Browser-basierten SSL-VPNs darauf geachtet werden, dass sämtliche Zwischenspeicher deaktiviert werden, damit Authentisierungsinformationen erst gar nicht temporär gespeichert werden. Dies könnte sonst einem Angreifer ermöglichen, die VPN-Verbindung wiederherzustellen.

Weitere Empfehlungen des BSI zum sicheren Fernzugriff finden sich im Dokument "Sicherer Fernzugriff auf das interne Netz (ISi-S)" [SFIN].

SYS.3.1.M10 Abgleich der Datenbestände von Laptops [Benutzer]

Wenn ein Laptop unterwegs eingesetzt wird und nicht über ein VPN direkt auf den Dateiservern der Institution gearbeitet wird, ist es wichtig, dass alle erforderlichen Daten und Anwendungen aktuell sind. Ebenso sollten unterwegs bearbeitete Daten zügig auf IT-Systemen innerhalb des Informationsverbunds der Institution gespeichert werden, damit es nicht zu inkonsistenten Datenbeständen kommt. Der einfachste Weg hierfür ist, regelmäßig Datenbestände von Laptops abzugleichen, beispielsweise über Tools zur Synchronisation von Dateien und Verzeichnissen zwischen Laptops und Arbeitsplatzrechnern oder Servern.

Dafür sollte überlegt werden, welche Informationen an welchen Stellen gespeichert sind, also auf welchen Servern und in welchen Verzeichnissen. Bei der ersten Sichtung zeigt sich meist, an wie vielen verschiedenen Stellen in einem Informationsverbund sich die für einen Arbeitsplatz relevanten Informationen befinden.

Damit Synchronisationsvorgänge nicht zu lange dauern, sollten dafür Tools ausgewählt werden,

- über die Dateien und Verzeichnisse nach vorher festgelegten Kriterien automatisch abgeglichen und aktualisiert werden können,die über Filtermöglichkeiten komplette Verzeichnisse oder auch einzelne Dateien von einem Kopiervorgang ausschließen können,die Synchronisationskonflikte auflösen können. Synchronisationskonflikte können auftreten, wenn seit der letzten Synchronisation eine Datei in verschiedenen Verzeichnissen geändert wurde.
- die über Filtermöglichkeiten komplette Verzeichnisse oder auch einzelne Dateien von einem Kopiervorgang ausschließen können,die Synchronisationskonflikte auflösen können. Synchronisationskonflikte können auftreten, wenn seit der letzten Synchronisation eine Datei in verschiedenen Verzeichnissen geändert wurde.
- die Synchronisationskonflikte auflösen können. Synchronisationskonflikte können auftreten, wenn seit der letzten Synchronisation eine Datei in verschiedenen Verzeichnissen geändert wurde.

Synchronisationstools sollten außerdem möglichst benutzerfreundlich sein und trotzdem vor fehlerhafter Bedienung schützen. Synchronisationsvorgänge sollten zugriffsgeschützt sein, bei Laptops kann das über bereits vorhandene Zugriffsschutz-Verfahren erfolgen.

Damit Angreifer die Synchronisation nicht manipulieren können, sollten die Benutzer regelmäßig die relevanten Verzeichnisse daraufhin inspizieren, ob sich dort ihnen unbekannte Dateien befinden. Die Synchronisationssoftware sollte so konfiguriert werden, dass sie, bevor Programme installiert werden, den Benutzer fragt. Der Synchronisationsvorgang sollte nicht unbeobachtet ablaufen, auch die Informationen, welche Dateien jeweils transferiert werden, können entscheidende Hinweise enthalten. Die Synchronisation sollte protokolliert werden. Die Protokolle sollten dann regelmäßig zumindest überflogen werden, um festzustellen, ob unbefugte Synchronisationsvorgänge stattgefunden haben.

SYS.3.1.M11 Sicherstellung der Energieversorgung [Benutzer]

Um die Energieversorgung eines Laptops auch unterwegs aufrechterhalten zu können, werden üblicherweise Akkus eingesetzt. Diese können den Laptop je nach Kapazität und Bauweise für einen beschränkten Zeitraum, üblicherweise einige Stunden, mit Energie versorgen. Es ist schwierig, diesen Zeitraum genauer abzuschätzen, da er stark vom Alter des Akkumulators und von der Intensität der Nutzung abhängt. Damit keine Daten in flüchtigen Speichern verloren gehen, wenn der Akku leer ist, sollten einige Randbedingungen eingehalten werden:

- Die Warnanzeigen des Laptops, die den Spannungsabfall anzeigen, dürfen nicht ignoriert werden. Sie sollten so konfiguriert sein, dass nach der ersten Warnung noch genügend Zeit vorhanden ist, um z. B. wichtige Daten abzuspeichern oder offene Programme zu schließen.
- Falls ein längerfristiger mobiler Einsatz absehbar ist, sind die Akkus vorher vollständig aufzuladen und eventuell Ersatzakkus mitzuführen. Zusätzlich gibt es für viele Laptops sogenannte Akku-Packs, die über eine externe Schnittstelle angeschlossen werden können. Ein Ersatzakku sollte in einer Schutzhülle verwahrt werden, da Schäden durch Überhitzung oder Brand entstehen können, wenn die Kontakte des Akkus mit leitenden Materialien in Berührung kommen. Dies kann durch viele Gegenstände des täglichen Gebrauchs verursacht werden, z. B. durch Schlüssel oder Ketten.
- Gerade bei älteren Akkus sind die Gebrauchszeiten verkürzt und sie entladen sich gegen Ende der Kapazität sehr schnell. Geöffnete Dateien müssen daher regelmäßig abgespeichert werden, um Datenverluste zu vermeiden. Da sich solche Akkus auch im Stand-by-Modus schnell entladen können, sollte der Ladezustand regelmäßig kontrolliert werden. Für den Notfall sollten Sicherungen der Konfigurationsdaten des Laptops mitgeführt werden. Es wird empfohlen, den Akku auszutauschen, sobald solche Alterungserscheinungen auftreten.
- Der Laptop sollte so aufgeladen werden, wie es im Handbuch empfohlen wird, damit die Lebensdauer des Akkus nicht beeinträchtigt wird.
- Vor einer Reise bzw. wenn ein Laptop übergeben wird, ist der ausreichende Ladezustand der Akkus oder Batterien sicherzustellen. Der Ladezustand sollte regelmäßig überprüft werden, da sich ein Akku auch entlädt, wenn er nicht verwendet wird.
- Das Ladegerät sollte immer mitgeführt werden. Nur im Ausnahmefall, beispielsweise bei voraussehbar kurzem mobilen Einsatz, ist es entbehrlich.

Es empfiehlt sich darüber hinaus, in kurzen Abständen die verarbeiteten Daten zusätzlich auf einem nichtflüchtigen Medium zu speichern. Dazu können auch automatische Datensicherungen in Standardprogrammen benutzt werden.

Bevor der Akku gewechselt wird, sollte der Laptop ausgeschaltet werden, damit der Speicher nicht beschädigt wird.

SYS.3.1.M12 Verlustmeldung [Benutzer]

Fällt ein dienstlich genutzter Laptop aus, ist er defekt, zerstört, geht verloren oder wird gestohlen, sollte dies umgehend gemeldet werden. Das gilt auch für private Geräte, die dienstlich genutzt werden. Hierfür sollte es in jeder Institution klare Meldewege und Ansprechpartner geben.

Insbesondere wenn ein Laptop verloren geht oder gestohlen wird, muss schnell gehandelt werden, da es hier nicht nur um die Wiederbeschaffung der Geräte geht, sondern auch darum, dass die betroffenen Informationen nicht missbraucht werden. Auf Laptops können sich vertrauliche Daten befinden, nach deren Verlust umgehend gehandelt werden muss, beispielsweise:

- Zugangsdaten wie Passwörter: Alle Zugangsdaten im eventuell betroffenen IT-System müssen umgehend geändert werden.Als vertraulich eingestufte Informationen: Alle betroffenen Bereiche (z. B. Fachabteilung, Kunden) müssen benachrichtigt werden, um entsprechende Maßnahmen ergreifen zu können.
- Als vertraulich eingestufte Informationen: Alle betroffenen Bereiche (z. B. Fachabteilung, Kunden) müssen benachrichtigt werden, um entsprechende Maßnahmen ergreifen zu können.

Falls möglich, sollten, nachdem ein Laptop verloren gegangen ist, auch Maßnahmen ergriffen werden, mit denen sich das Gerät sperren, löschen oder lokalisieren lässt. Die meisten Mobile-Device-Management-(MDM)-Lösungen (siehe SYS.3.2.2 Mobile Device Management) bieten diese Funktionen an. Dafür sind vorher klare Regeln zu definieren und entsprechende Maßnahmen in Absprache mit dem Benutzer, dessen Endgerät verloren ging, unverzüglich zu ergreifen.

Wenn verlorene Geräte wieder auftauchen, sollten sie auf eventuelle Manipulationen untersucht werden, z. B. ob Schrauben geöffnet, Siegel entfernt wurden oder sich das Gewicht gegenüber dem Auslieferungszustand geändert hat. Besteht ein Verdacht, sollte das Gerät entweder gleich entsorgt oder von einem Spezialisten weiter untersucht werden. Um sicherzustellen, dass sich keine manipulierten Programme auf den wiedererlangten Geräten befinden, müssen die Geräte zumindest neu installiert werden (SYS.3.1.M7 *Geregelte Übergabe und Rücknahme eines Laptops*).

SYS.3.1.M13 Verschlüsselung von Laptops

Um zu verhindern, dass aus einem gestohlenen Laptop schutzbedürftige Daten ausgelesen werden können, sollte ein Verschlüsselungsprogramm eingesetzt werden. Mithilfe der marktgängigen Produkte ist es möglich, einzelne Dateien, bestimmte Bereiche oder die ganze Festplatte so zu verschlüsseln, dass nur derjenige, der über den geheimen Schlüssel verfügt, die Daten lesen und bearbeiten kann.

Die Sicherheit der Verschlüsselung hängt dabei von drei verschiedenen Punkten zentral ab:

- Der verwendete Verschlüsselungsalgorithmus muss so konstruiert sein, dass es ohne den verwendeten Schlüssel zu kennen, nicht möglich ist, den Klartext aus dem verschlüsselten Text zu rekonstruieren. Nicht möglich bedeutet dabei, dass der erforderliche Aufwand, mit dem der Algorithmus gebrochen bzw. entschlüsselt werden kann, in keinem Verhältnis steht zum dadurch erzielbaren Informationsgewinn.
- Der Schlüssel ist geeignet zu wählen. Er sollte zufällig erzeugt werden. Wenn es möglich ist, einen Schlüssel wie ein Passwort zu wählen, sollten die Regelungen der Institution zum Passwortgebrauch beachtet werden.
- Der Verschlüsselungsalgorithmus (das Programm), der verschlüsselte Text und die Schlüssel dürfen nicht zusammen auf einem Datenträger gespeichert werden. Es bietet sich an, den Schlüssel einzeln aufzubewahren. Das kann dadurch geschehen, dass er auf einer Pappkarte in Form einer Scheckkarte aufgeschrieben und anschließend wie eine Scheckkarte im Portemonnaie aufbewahrt wird. Die kryptografischen Schlüssel sollten auf einem auswechselbaren Datenträger wie z. B. auf einem USB-Stick gespeichert und getrennt vom Laptop aufbewahrt werden.

Eine Verschlüsselung kann online oder offline vorgenommen werden. Online bedeutet, dass sämtliche Daten der Festplatte (bzw. einer Partition) verschlüsselt werden, ohne dass der Benutzer dies aktiv veranlassen muss. Eine Offline-Verschlüsselung wird explizit vom Benutzer initiiert. Er muss dann auch entscheiden, welche Dateien verschlüsselt werden sollen. Zur Auswahl und Nutzung von kryptografischen Verfahren sollte auch Baustein CON.1 *Kryptokonzept* beachtet werden.

SYS.3.1.M14 Geeignete Aufbewahrung von Laptops [Benutzer]

Benutzer müssen darauf achten, dass sie ihre Laptops auch außerhalb der Institution sicher aufbewahren. Hierfür können nur einige Hinweise gegeben werden, die dabei zu beachten sind:

- Laptops sollten möglichst nicht unbeaufsichtigt bleiben.
- Wird ein Laptop in einem Kraftfahrzeug aufbewahrt, sollte das Gerät von außen nicht sichtbar sein. Zum Beispiel sollte es abgedeckt oder in den Kofferraum eingeschlossen werden. Ein Laptop kann einen hohen Wert darstellen, der potenzielle Diebe anlockt, zumal solche IT-Systeme leicht veräußert werden können.
- Wird der Laptop in fremden Büroräumen benutzt, so ist sollte der Mitarbeiter ihn auch mitnehmen, wenn er den Raum nur kurz verlässt oder er schließt das Gerät ein. Es sollte mindestens ein Zugriffsschutz aktiviert werden, um eine unerlaubte Nutzung zu verhindern. Wird der Raum für längere Zeit verlassen, sollte der Laptop zusätzlich ausgeschaltet sein.
- In Hotelräumen sollte der Laptop nicht unbeaufsichtigt herumliegen. Wird das Gerät in einen Schrank eingeschlossen, hält das zumindest Gelegenheitsdiebe ab.
- Ein Laptop kann zusätzlich durch ein Schloss gesichert werden. Ein Dieb braucht dann Werkzeug, um ihn zu stehlen.
- Ein Laptop sollte nie extremen Temperaturen ausgesetzt werden. Insbesondere der Akku und das Display können dadurch beschädigt werden. Auch sollten weder Laptops noch Akkus in geparkten Autos zurückgelassen werden, wenn die Außentemperatur extrem hoch oder niedrig ist.
- Ebenso sollten Laptops vor schädlichen Umwelteinflüssen geschützt werden, beispielsweise vor Feuchtigkeit durch Regen oder Spritzwasser.
- Laptops sind nicht unzerstörbar, daher sollten sie auch bei kürzeren Transportwegen möglichst stoßgeschützt befördert werden. So sollten sie beispielsweise immer zusammengeklappt werden, da sowohl die Scharniere als auch der Bildschirm bei einem Sturz leicht beschädigt werden können. Grundsätzlich sollte für den Transport ein schützendes Behältnis verwenden werden, beispielsweise Taschen oder Rucksäcke mit eigenen Fächern und Polsterungen für Laptops.

Es ist empfehlenswert, für die Benutzer von Laptops ein Merkblatt zu erstellen, das die wichtigsten Hinweise und Vorsichtsmaßnahmen enthält, wie die Geräte geeignet aufzubewahren und zu transportieren sind.

Geeignete Aufbewahrung von Laptops im stationären Einsatz

Laptops sind durch ihre Bauform immer beliebte Ziele für Diebstähle. Daher müssen sie auch dann sicher aufbewahrt werden, wenn sie sich im vermeintlichen sicheren Büro befinden. Deshalb sind die in Baustein INF.8 *Arbeitsplatz* beschriebenen Anforderungen zu beachten. Da ein Laptop jedoch besonders leicht zu transportieren und zu verbergen ist, kann das Gerät außerhalb der Nutzungszeiten weggeschlossen werden, also beispielsweise in einem Schrank oder Schreibtisch verschlossen oder angekettet werden.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

SYS.3.1.M15 Geeignete Auswahl von Laptops [Beschaffungsstelle] (A)

Laptops gibt es in verschiedensten Varianten und Geräteklassen. Diese unterscheiden sich nicht nur in ihren Abmessungen und Leistungsmerkmalen, sondern auch bei den Sicherheitsmechanismen und dem Bedienkomfort. Zudem stellen sie unterschiedliche Anforderungen an Hard- und Software-Komponenten im Einsatzumfeld.

Bei der Vielzahl verschiedener Laptop-Modelle mit den unterschiedlichsten Betriebssystemen sind Kompatibilitätsprobleme bei Hardware, Software auf Laptop und PC sowie Schnittstellen naheliegend.

Zunächst sollte eine Anforderungsanalyse durchgeführt werden. Ziel ist es hier einerseits, alle infrage kommenden Einsatzszenarien zu bestimmen und andererseits daraus Anforderungen an die benötigten Hard- und Softwarekomponenten abzuleiten.

Die folgende Liste gibt einen groben Überblick über mögliche allgemeine Bewertungskriterien. Sie erhebt jedoch keinen Anspruch auf Vollständigkeit und kann um weitere allgemeine Anforderungen erweitert werden.

Allgemeine Kriterien

- Wartbarkeit
  - Ist das Produkt einfach wartbar?
  - Wird das Gerät über den geplanten Nutzungszeitraum vom Hersteller unterstützt? Bietet der Hersteller regelmäßige Software-Updates an?
  - Werden für das Produkt Wartungsverträge angeboten?
- Zuverlässigkeit/Ausfallsicherheit
  - Wie zuverlässig und ausfallsicher ist das Produkt?
  - Ist das Produkt im Dauerbetrieb einsetzbar?
  - Gibt es einen im Produkt integrierte Backup-Mechanismus? Kann eine automatische Datensicherung durchgeführt werden?
- Benutzerfreundlichkeit
  - Lässt sich das Produkt einfach installieren, konfigurieren und nutzen?
  - Ist die Synchronisations-Software so konfigurierbar, dass die Benutzer möglichst wenig mit technischen Details belastet werden? Ist die Sicherheit dabei trotzdem immer gewährleistet?
  - Sind Abmessungen und Gewicht bezogen auf den Einsatzzweck angemessen? Ist die Akku-Laufzeit ausreichend für die tägliche Arbeit? Kann der Akku gewechselt werden, wenn die Akku-Laufzeit nicht ausreichend ist und das Gerät zwischenzeitlich nicht geladen werden kann?
- Kosten

- Wie hoch sind die Anschaffungskosten der Hard- und Software?
- Wie hoch sind die voraussichtlichen laufenden Kosten der Hard- und Software (Wartung, Betrieb, Support)?
- Wie hoch sind die voraussichtlichen laufenden Kosten für das Personal (Administrator/Support)?
- Müssen zusätzliche Soft- oder Hardware-Komponenten angeschafft werden (z. B. Docking-Station, Konvertierungssoftware)?

Funktion

- Installation und Inbetriebnahme
  - Kann das Gerät sowie die Synchronisations-Software so konfiguriert werden, dass die vorgegebenen Sicherheitsziele erreicht werden können?
  - Können wichtige Konfigurationsparameter vor Veränderungen durch Benutzer geschützt werden?
  - Arbeitet das Produkt mit gängiger Hard- und Software zusammen (Betriebssysteme, Treiber)?
- Administration
  - Enthält die mitgelieferte Produktdokumentation eine genaue Darstellung aller technischen und administrativen Details?
  - Können die Laptops über eine zentral gesteuerte Management-Software administriert werden? Ist die administrative Schnittstelle so gestaltet, dass auf fehlerhafte, unsichere oder inkonsistente Konfigurationen hingewiesen wird oder diese verhindert werden?
- Sicherheit: Kommunikation, Authentisierung, Zugriff und Protokollierung
  - Unterstützt der Laptop alle benötigten Datenübertragungstechnologien (z. B. Bluetooth, WLAN, LAN)?
  - Können mit dem Produkt die Daten zu anderen Endgeräten gesichert übertragen werden?
  - Hat der Laptop geeignete Mechanismen zur Identifikation und Authentisierung der Benutzer?
  - Können zusätzliche Sicherungsmechanismen (z. B. Verschlüsselungs- oder Antivirenprogramme) genutzt werden?
  - Erlaubt die Produktarchitektur die nachträgliche Installation neuer Sicherheitsmechanismen?
  - Wird dem mobilen Benutzer nur nach erfolgreicher Authentisierung der Zugang zu lokalen Endgeräten erlaubt?
  - Ist die Systemarchitektur so aufgebaut, dass neue Authentisierungsmechanismen nachträglich integriert werden können?
  - Lässt sich mit dem Laptop eine geeignete Protokollierung durchführen bzw. lässt er sich in bereits bestehende Protokollierungs-Prozesse integrieren?

Sind alle Anforderungen an das zu beschaffende Produkt dokumentiert, so müssen die am Markt erhältlichen Laptops dahin gehend untersucht werden, inwieweit sie diese Anforderungen erfüllen. Es ist zu erwarten, dass nicht jedes Produkt alle Anforderungen gleichzeitig oder gleich gut erfüllt. Daher sollten die einzelnen Anforderungen gewichtet werden. Aufgrund der durchgeführten Produktbewertung kann dann eine fundierte Kaufentscheidung getroffen werden.

Die Praxis zeigt, dass es aufgrund verschiedener Einsatzanforderungen durchaus sinnvoll sein kann, mehrere unterschiedliche Gerätetypen für die Beschaffung auszuwählen. Die Gerätevielfalt sollte aber eingeschränkt werden, damit der Support einfacher ist.

SYS.3.1.M16 Zentrale Administration von Laptops (CI)

Die Administration für mobile Endgeräte ist keine einfache Aufgabe, vor allem bei großen Institutionen und bei Benutzern, die sich häufig und in aller Welt bewegen. Es gibt Tools, die eine zentrale Administration und die Umsetzung von Sicherheitsrichtlinien erleichtern. Durch eine zentrale Administration können nicht nur Software und Informationen verteilt, sondern auch die institutionseigenen Sicherheitsrichtlinien auf den Laptops durchgesetzt werden, z. B. für Authentisierung, Zugriff oder Datensicherung.

Wird eine Software zum zentralen Laptop-Management eingesetzt, synchronisieren sich die Laptops mit einem Server. Dabei lassen sich nicht nur Daten abgleichen, sondern auch Sicherheitsvorgaben technisch forcieren, indem sicherheitsrelevante Einstellungen auf ihre vorgegebenen Werte zurückgesetzt werden. Typische Funktionen solcher Tools zum zentralen Laptop-Management sind unter anderem:

- Datensicherungen können zentral durchgeführt werden, ohne dass die Benutzer sich darum kümmern müssen. Ebenso können Vorgaben gemacht werden, wann bzw. wie oft Daten zu sichern oder zu synchronisieren sind und welche Randbedingungen dabei eingehalten werden müssen.
- Es besteht die Möglichkeit, Rückmeldungen über den Status der Laptops zu erhalten und Diagnosen remote durchführen zu können.
- Es können Benutzerprofile angelegt werden, um die Benutzerverwaltung zu vereinfachen.
- Es lassen sich Passwortregeln und andere Sicherheitsregeln vorgeben.

Ein Tool zum zentralen Laptop-Management sollte möglichst alle in der Institution eingesetzten Betriebssysteme unterstützen, damit nicht mehrere solcher Tools parallel eingesetzt werden müssen. Dasselbe gilt ebenso natürlich für die eingesetzte Groupware und E-Mail-Plattform. Vertiefende Informationen sind auch in SYS.3.2.2 Mobile Device Management zu finden.

SYS.3.1.M17 Sammelaufbewahrung (A)

Sind in einer Institution viele Laptops im mobilen Einsatz und wechseln die Benutzer häufig, kann es angebracht sein, die zeitweise nicht genutzten Geräte in einer Sammelaufbewahrung (Pool) zu halten. Der dafür genutzte Raum sollte den Anforderungen aus INF.5 *Technikraum* entsprechen.

Darüber hinaus ist die Stromversorgung der Laptops sicherzustellen, damit die Batterien dieser Geräte den sofortigen Einsatz erlauben (siehe SYS.3.1.M11 *Sicherstellung der Energieversorgung*). Zusätzlich müssen die Rücknahme und die Ausgabe von tragbaren IT-Systemen dokumentiert werden (siehe SYS.3.1.M7 *Geregelte Übergabe und Rücknahme eines Laptops*).

SYS.3.1.M18 Einsatz von Diebstahl-Sicherungen (CIA)

Diebstahl-Sicherungen sind überall dort einzusetzen, wo große Werte zu schützen sind bzw. dort, wo andere Maßnahmen nicht umgesetzt werden können, wie etwa bei Laptops im mobilen Einsatz. Diebstahl-Sicherungen sind außerdem dort sinnvoll, wo Publikumsverkehr herrscht oder die Fluktuation von Benutzern sehr hoch ist. Dabei sollte immer bedacht werden, dass die zu schützenden Werte nur zu einem kleinen Teil aus den Wiederbeschaffungskosten für das Gerät bestehen, sondern bei Laptops der Wert der darauf gespeicherten Daten berücksichtigt werden muss.

Verhindern einer Cold-Boot-Attacke

In Bereichen, die nicht ausreichend gegen unbefugten Zutritt geschützt sind, könnte beispielsweise durch eine Cold-Boot-Attacke der Arbeitsspeicher ausgelesen werden. Gleiches gilt für Systeme, die durch "Suspend to RAM" in einen Energiesparmodus versetzt wurden.

Bei einer Cold-Boot-Attacke werden die Speicherbausteine stark gekühlt, bevor das System ausgeschaltet wird. Der Speicherinhalt bleibt dadurch mehrere Minuten erhalten und kann währenddessen mit geeignetem Gerät ausgelesen werden.

Cold-Boot-Attacken lassen sich nur verhindert, wenn Angreifer nicht ungestört auf den Arbeitsspeicher eines aktiven IT-Systems zugreifen können. Ein Zugriffsschutz, wie ein physisch verriegeltes Computer-Gehäuse, erschwert es, ein IT-System unbefugt zu öffnen, um den Arbeitsspeicher zu kühlen und auszubauen, kann es aber nicht dauerhaft unterbinden. Daher sollte ein unbenutzter Laptop stets ausgeschaltet werden, wenn er nicht in einem zutrittsgeschützten Bereich steht.

Arten von Diebstahl-Sicherungen

Auf dem Markt sind die unterschiedlichsten Diebstahl-Sicherungen erhältlich. Diese können zunächst in mechanische und elektronische Sicherungen unterteilt werden.

Zu den mechanischen Sicherungen gehören unter anderem Kabelsicherungen, Gehäusesicherungen (um das Gehäuse gegen Öffnung zu schützen), Sicherheitsplatten und Sicherheitsgehäuse. Es gibt hier zum einem Hardware-Sicherungen, die dem Diebstahl von IT-Geräten vorbeugen, z. B. indem der Laptop mit dem Schreibtisch verbunden wird. Es gibt zum anderen auch eine Reihe von Sicherungsmechanismen, die verhindern sollen, dass das Gehäuse geöffnet wird. Damit soll vorgebeugt werden, dass Angreifer Teile stehlen oder sicherheitsrelevante Einstellungen manipulieren, wie zum Beispiel Sicherheitskarten entfernen.

Bei der Beschaffung mechanischer Sicherungen ist die Wahl eines guten Schlosses wichtig, das über eine auf die jeweiligen Bedürfnisse abgestimmte Schließanlage verfügt. Je nach Produkt sind verschiedene Schließanlagen möglich:

- gleichschließend: Ein Schlüssel passt auf alle Gerätesicherungen einer Institution, Abteilung etc. Das hat den Vorteil, dass der Aufwand für die Schlüsselverwaltung geringer ist. Es bedeutet jedoch auch, dass sehr viele gleichartige Schlüssel im Umlauf sein können und dass im Schadensfall häufig keine Beweissicherung möglich ist.
- verschiedenschließend: Jede Gerätesicherung hat einen individuellen Schlüssel. Das hat den Nachteil, dass der Aufwand für die Schlüsselverwaltung höher ist. Es hat aber den Vorteil, dass es weniger Schlüsseldubletten gibt.
- Hauptschlüsselsystem: Jede Gerätesicherung hat einen individuellen Schlüssel, kann zusätzlich aber auch durch einen Hauptschlüssel geöffnet werden. Das hat den Vorteil, dass der Aufwand für die Schlüsselverwaltung geringer ist. Es hat aber den Nachteil, dass solche Systeme teurer in der Anschaffung sind.

Die meisten Laptops haben einen kleinen Schlitz, der mit einem Ketten- oder Schloss-Symbol gekennzeichnet ist. Diese kleine Öffnung befindet sich seitlich oder hinten am Gerät. Es gibt eine breite Palette von Kabelsicherungen und anderen Produkten, die diese Öffnung für die Sicherung von Geräten nutzt.

Bei Kabelsicherungen muss dann nur eine Kabelschlinge um ein solides Objekt in der Nähe des Gerätes gelegt, das zugehörige Schloss durch die entstandene Lasche gezogen und abgeschlossen werden.

Für Geräte, die diese Öffnung nicht haben, oder bei denen diese nicht stark genug ist, gibt es Sicherungsprodukte, bei denen eine stabile Platte auf das Gerät geklebt wird. An dieser wird dann das Sicherungskabel befestigt.

Daneben gibt es elektronische Sicherungen, die beispielsweise einen akustischen Abschreckungs-Alarm am Gerät selber auslösen, der potenzielle Diebe dazu bringen soll, den Laptop liegen zu lassen.

Bei Neuanschaffung von Laptops sollte darauf geachtet werden, dass sie Ösen am Gehäuse besitzen, um sie an anderen Gegenständen befestigen zu können.

3 Weiterführende Informationen

3.1 Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Laptops" finden sich unter anderem in folgenden Veröffentlichungen:

[KNOP] KNOPPIX

Live Linux File System On CD, http://www.knoppix.org, zuletzt abgerufen am 05.10.2018

[SFiN] Sicherer Fernzugriff auf das interne Netz (ISi-S)

BSI-Studie zur Internet-Sicherheit (ISi-S), Bundesamt für Sicherheit in der Informationstechnik (BSI), September 2010, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_fern_studie_pdf.html, zuletzt abgerufen am 05.10.2018

SYS.3: Mobile Devices

Umsetzungshinweise zum Baustein SYS.3.3 Mobiltelefon

1 Beschreibung

1.1 Einleitung

In diesem Baustein werden Mobiltelefone nach dem GSM-Standard (Global System for Mobile communication), UMTS (Universal Mobile Telecommunications System) und LTE (Long Term Evolution) betrachtet.

Die in diesem Baustein betrachteten Mobiltelefone, die auch Feature-Phones oder Dumbphones genannt werden, besitzen weniger Eigenschaften als ein Smartphone, bieten aber mehr als nur die reine Telefonfunktion. So können diese Mobiltelefone zusätzlich über eine Kamera für Videos und Fotos, Terminplaner, E-Mail-Programme, Spiele, einen MP3-Spieler oder ein Radio verfügen. "Klassische" Mobiltelefone verfügen in der Regel nicht über ein Touchscreen und einem Betriebssystem, auf das Apps installiert werden können. Diese fehlenden Funktionen unterscheidet das Mobiltelefon von einem Smartphone.

Die Mobiltelefone sind durch eine international eindeutige Seriennummer (IMEI) gekennzeichnet. Die Identifizierung der Benutzer des Mobiltelefons erfolgt durch die SIM-Karte, die bei Vertragsabschluss vom Mobilfunkanbieter zugeteilt wird.

1.2 Lebenszyklus

Planung und Konzeption

Es muss eine Sicherheitsrichtlinie erstellt werden, die umzusetzende Maßnahmen zum sicheren Umgang mit Mobiltelefonen beschreibt (siehe SYS.3.3.M.1 *Sicherheitsrichtlinie und Regelungen für die Mobiltelefon-Nutzung*). Bei häufigem und wechselndem dienstlichen Gebrauch von Mobiltelefonen, die von der Institution oder der Behörde zur Verfügung gestellt werden, kann es sinnvoll sein, diese Telefone in einer Sammelaufbewahrung zu halten (siehe *SYS.3.3.*M12 *Einrichtung eines Mobiltelefon-Pools).*

Umsetzung

Es gibt verschiedene Sicherheitsmechanismen bei Mobiltelefonen, abhängig vom eingesetzten Mobiltelefon, von der SIM-Karte und vom gewählten Netzbetreiber. SYS.3.3.M5 *Nutzung der Sicherheitsmechanismen von Mobiltelefonen* gibt einen Überblick über die wichtigsten Sicherheitsfunktionen dieser Geräte und beschreibt, wie diese genutzt werden könnten.

Betrieb

Damit Mobiltelefone geordnet und zuverlässig genutzt werden können, müssen einige Maßnahmen umgesetzt werden, zu denen die Sicherstellung der Energieversorgung und bei Bedarf auch der Schutz vor Rufnummernermittlung gehören (siehe SYS.3.3.M9 *Sicherstellung der Energieversorgung* und SYS.3.3.M14 *Schutz vor Rufnummernermittlung bei der Mobiltelefon-Nutzung*). Falls mit dem Gerät Daten übertragen werden, sind ebenfalls einige spezifische Maßnahmen zu beachten, um einerseits eine zuverlässige Funktionsweise zu gewährleisten und andererseits gegen Missbrauch geschützt zu sein (siehe SYS.3.3.M10 *Sichere Datenübertragung über Mobiltelefone*). Wird das Telefon verloren, sollte die SIM-Karte dieses Telefons unverzüglich gesperrt werden, um Missbrauch und unnötige Kosten zu verhindern (siehe SYS.3.3.M2 *Sperrmaßnahmen bei Verlust*). Für die speziellen Gefährdungen der Informationssicherheit durch Mobiltelefone müssen die betreffenden Mitarbeiter besonders sensibilisiert werden (siehe SYS.3.3.M3 *Sensibliliserung und Schulung der Mitarbeiter im Umgang mit Mobiltelefonen).*

Aussonderung

Da sich auf Mobiltelefonen in der Regel vertrauliche Daten befinden, muss geregelt werden, wie die Geräte auszusondern sind. In Maßnahme SYS.3.3.M4 *Aussonderung und ordnungsgemäße Entsorgung von Mobiltelefonen und Speicherkarten* werden Empfehlungen gegeben. Falls die Geräte herausnehmbare Speicherkarten besitzen, ist für diese Karten ebenfalls Maßnahme SYS.3.3.M4 *Aussonderung und ordnungsgemäße Entsorgung von Mobiltelefonen und Speicherkarten* anzuwenden, die beschreibt, wie Mobiltelefone ausgesondert und die herausnehmbaren Speicherkarten entsorgt werden.

Notfallvorsorge

In der Maßnahme SYS.3.3.M11 *Ausfallvorsorge bei Mobiltelefonen* werden wichtige Vorkehrungen beschrieben, durch die sich der Benutzer vor Ausfall und bei Verlust eines Mobiltelefons schützen kann.

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Mobiltelefon" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

SYS.3.3.M1 Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung [Informationssicherheitsbeauftragter (ISB)]

Bevor in einer Institution Mobiltelefone verwendet werden, sind die Rahmenbedingungen und der Einsatzzweck zu klären. Ein Grund, Mobiltelefone einzusetzen, können Sicherheitserwägungen sein, da

- Mobiltelefone weniger Angriffsfläche als Smartphones bieten, sowohl auf das Gerät selber als auch indirekt über das Gerät an andere, damit verbundene IT-Systeme,
- Mobiltelefone genau auf ihren Einsatzzweck angepasst sind und damit einfacher zu verwenden und resilienter sind.

Werden in einer Institution Mobiltelefone verwendet, ist dafür eine Sicherheitsrichtlinie zu erstellen, die alle umzusetzenden Maßnahmen beschreibt.

Darüber hinaus muss es für die Benutzer ein kurzes und übersichtliches Merkblatt für die sichere Nutzung von Mobiltelefonen geben. Falls technisch möglich, muss die Anleitung für das Mobiltelefon und die Sicherheitshinweise zusätzlich auf dem Mobiltelefon gespeichert sein. Der Mitarbeiter ist auf den Speicherort hinzuweisen.

Anfallende Datenarten

Sobald ein Mobiltelefon eingeschaltet wird, meldet es sich über die nächstgelegene Basisstation beim Netzbetreiber an. Bei diesem werden Daten der SIM-Karte, die Seriennummer des Mobiltelefons und die Kennung der Basisstation, über die die Anmeldung erfolgt ist, protokolliert und gespeichert. Das erfolgt auch dann, wenn kein Gespräch geführt wird. Weiterhin wird jeder Verbindungsversuch, unabhängig vom Zustandekommen der Verbindung, gespeichert.

Die bei der Telekommunikation anfallenden Datenarten lassen sich grob in drei Gruppen untergliedern:

- Bestandsdaten (oder auch Stammdaten) sind diejenigen Daten, die in einem Dienst oder Netz dauerhaft gespeichert und bereit gehalten werden. Hierzu gehören die Rufnummer und gegebenenfalls der Name und die Anschrift des Teilnehmers, Informationen über die Art des Endgerätes, gegebenenfalls für den Anschluss jeweils verfügbare Leistungsmerkmale und Berechtigungen sowie Daten über die Zuordnung zu Teilnehmergruppen.
- Inhaltsdaten sind die eigentlichen "Nutzdaten", d.h. die übertragenen Informationen und Nachrichten.
- Verbindungsdaten geben Auskunft über die näheren Umstände von Kommunikationsvorgängen. Hierzu gehören Angaben über Kommunikationspartner (z.B. Rufnummern des rufenden und des angerufenen Anschlusses), Zeitpunkt und Dauer der Verbindung, in Anspruch genommene Systemleistungen, benutzte Anschlüsse, Leitungen und sonstige technische Einrichtungen, Dienste und, bei mobilen Diensten, die Standortkennungen der mobilen Endgeräte.

Im Folgenden werden Empfehlungen gegeben, wie diese Daten vor Missbrauch geschützt werden können.

Schutz vor Kartenmissbrauch

Das Mobiltelefon und die SIM-Karte müssen stets sicher aufbewahrt werden. Bei Dienstreisen müssen sie beaufsichtigt werden. Insbesondere müssen sie aus Fahrzeugen mitgenommen werden. In den Sicherheitsrichtlinien muss festgehalten werden, wie die SIM-Karten vor Missbrauch geschützt werden können.

Mobiltelefone und dazu angebotene Dienstleistungen können an verschiedenen Stellen durch PINs oder Passwörter abgesichert werden. Dazu gehören:

- der Zugriff auf die SIM-Karte,
- der Zugriff auf das eigentliche Endgerät, also das Mobiltelefon,
- der Zugriff auf bestimmte Funktionen des Mobiltelefons, z.B. das Telefonbuch,
- der Zugriff auf die Mailbox, also die Anrufbeantworterfunktion, oder andere Dienstleistungen des Netzbetreibers,
- der Zugriff auf Daten beim Netzbetreiber (bei Fragen an die Hotline wegen der Abrechnung muss unter Umständen ein Kennwort genannt werden).

Alle diese Sicherheitsmechanismen sollten auch genutzt werden. Am wichtigsten ist dabei sicherlich der Schutz der SIM-Karte, da deren Missbrauch zu hohen finanziellen Schäden führen kann. Die persönliche Geheimzahl (PIN) darf keinesfalls zusammen mit der zum Mobiltelefon gehörigen SIM-Karte aufbewahrt werden ebenso wenig der PUK.

Bei Smartphones ist auch der Schutz des Endgerätes durch PIN oder Passwörter von entscheidender Bedeutung, da hier die Applikationen vertrauliche Daten, wie zum Beispiel Authentisierungstoken oder Passwörter, enthalten können. Daher muss ein solcher Schutz bei allen Geräten eingerichtet sein und darf sich nicht deaktivieren lassen. Ferner muss sich das Gerät automatisch (zum Beispiel nach zehn Minuten Untätigkeit) selbst sperren.

Bei Verlust der SIM-Karte muss sofort beim Netzbetreiber eine Kartensperre veranlasst werden, um einen eventuellen Missbrauch und damit auch einen finanziellen Schaden abzuwehren (siehe SYS.3.3.M2 *Sperrmaßnahmen bei Verlust*).

Um die missbräuchliche Benutzung der SIM-Karte rechtzeitig zu bemerken, muss in jedem Fall der Einzelverbindungsnachweis auf unerklärliche Gebühren und Zielrufnummern geprüft werden.

Einzelverbindungsnachweis

Der Netzbetreiber speichert die Anrufdaten für die Abrechnung. In Deutschland darf er sie nur bis zur Rechnungsstellung speichern, maximal aber 80 Tage gemäß Telekommunikationsdienstunternehmen-Datenschutzverordnung - Verordnung über den Datenschutz für Institutionen, die Telekommunikationsdienstleistungen erbringen (siehe [TDSV]). Es kann aber für den Kunden sinnvoll sein, dem Netzbetreiber zu erlauben, die Anrufdaten länger zu speichern, falls nachträglich Probleme mit der Rechnung auftreten.

Jeder Kunde muss einen Einzelverbindungsnachweis verlangen, um die Mobiltelefon-Nutzung kontrollieren zu können. In Deutschland haben die Kunden das Recht auf einen kostenlosen Einzelverbindungsnachweis. Aus diesem können z.B. folgende Daten entnommen werden:

- Rechnungsdatum,
- angerufene Rufnummer (vollständig bzw. die letzten Ziffern unkenntlich),
- Beginn, Ende oder Dauer der Verbindung sowie
- Kosten des Gesprächs.

Alle Mitbenutzer des Telefons müssen darüber informiert werden, dass ein Einzelverbindungsnachweis beantragt wurde und welche Daten dadurch erfasst werden.

Wenn in einer Behörde bzw. einer Institution zur Kostenkontrolle Einzelverbindungsnachweise geführt und ausgewertet werden, ist das Verfahren mit dem Betriebs- Personalrat und dem Datenschutzbeauftragten abzustimmen und den Benutzern bekannt zu geben.

Immer nach Erhalt der Einzelverbindungsnachweise sollte überprüft werden, ob sie korrekt sind. Hierdurch lässt sich auch ersehen, wo eventuell Kosten reduziert werden können.

Weitergabe der Rufnummer

Es kann gewählt werden, ob und welche Daten zu dem Mobiltelefon-Anschluss in öffentliche Telefonbücher eingetragen werden beziehungsweise für Abfragen über Telefonauskünfte zur Verfügung stehen. Ein solcher Eintrag ist jedoch nicht immer sinnvoll, zum Beispiel bei Mobiltelefonen aus einem Pool oder wenn die Zahl der Anrufer klein gehalten werden soll.

Wenn die Rufnummernanzeige aktiviert ist, können die Gesprächspartner (je nach Ausstattung) sehen, von welcher Telefonnummer sie angerufen werden. Dieser Dienst kann vom Netzbetreiber generell für ein Mobiltelefon an- oder abgeschaltet werden.

Rufnummernunterdrückung

Im Mobilfunk-Netz können den beteiligten Kommunikationspartnern die jeweiligen Rufnummern signalisiert werden. Wenn dies nicht gewünscht ist, sollte *SYS.3.3.M14* beachtet werden. Die Regelung für die Mobiltelefon-Nutzung sollten auf die Rufnummernunterdrückung eingehen.

Schutz vor Abhören von Telefonaten

Der einzige wirksame Schutz gegen das Abhören von Telefonaten ist die interoperable, netzübergreifende Ende-zu-Ende-Verschlüsselung. Da diese Verschlüsselung nur bei wenig handelsüblichen Geräten realisiert ist, kann jede Verbindung, ob im Festnetz oder im Mobilfunknetz, potenziell abgehört werden. Die Kommunikation zwischen Mobiltelefon und Basisstation wird aber in Deutschland und den meisten anderen Ländern verschlüsselt. Diese Verschlüsselung in Mobilfunknetzen ist jedoch mit entsprechendem Aufwand zu brechen und bietet daher nur mittelmäßigen Schutz.

Folgende Maßnahmen werden zum Schutz vor dem Abhören empfohlen, die in einer Regelung für die Mobiltelefon-Nutzung festgehalten werden muss:

- Es sollte nicht immer und überall telefoniert werden. Zum Telefonieren muss ein ungestörter Bereich aufgesucht werden (dadurch werden auch andere weniger gestört).
- Grundsätzlich muss keine Telefongespräche mit vertraulichem Inhalt geführt werden.
- Manche Mobiltelefone zeigen auf dem Display an, wenn die Übertragung zwischen Mobiltelefon und Basisstation nicht verschlüsselt wird. Wenn diese Anzeige vorgesehen ist, müssen die Benutzer darüber informiert werden. Ab und zu sollten sie sich durch einen Blick auf das Display davon überzeugen, ob tatsächlich verschlüsselt wird. So gibt es einige Länder, in denen die Kommunikation zwischen Mobiltelefon und Basisstation nicht verschlüsselt wird.
- Es gibt auch einige wenige und verhältnismäßig teure Mobiltelefone, mit denen die Kommunikation von Ende zu Ende verschlüsselt werden kann. Dafür müssen aber beide Gesprächspartner kompatible Geräte einsetzen. Wenn häufiger hochsensitive Informationen über Mobiltelefon weitergegeben werden sollen, kann dies sinnvoll sein.
- Bei der Datenübertragung zum Beispiel von einem Laptop über ein Mobilfunknetz sollten die übertragenen Daten vorher auf dem Endgerät verschlüsselt werden. Hierzu gibt es eine Vielzahl von Programmen, die dies einfach ermöglichen. Alternativ kann für die Datenübertragung ein verschlüsselter VPN-Tunnel etabliert werden.
- Wenn Mobiltelefone bzw. SIM-Karten gewechselt werden, ist es enorm aufwendig, gezielt Telefonate abzuhören. Dies kann daher bei der Übertragung hochsensitiver Information bzw. Daten zweckmäßig sein.
- Es sollte geprüft werden, ob alle Gesprächsgebühren dem Teilnehmer in Rechnung gestellt wurden. Fehlende Gebühren für bestimmte Verbindungen können darauf hindeuten, dass abgehört wurde ebenso wie Gebühren für nicht bewusst getätigte Verbindungen.

Sensibilisierung der Benutzer

Die Benutzer von Mobiltelefonen müssen regelmäßig für die speziellen Gefährdungen der Informationssicherheit sensibilisiert werden (siehe SYS.3.3.*3 im Umgang mit Mobiltelefonen).*

Regelungen zur Nutzung privater Mobiltelefone

Werden private Mobiltelefone für dienstliche Zwecke benutzt, sind folgende Aspekte vorher zu regeln:

- Wer bezahlt dienstliche Gespräche und wie werden sie abgerechnet?
- Moderne Mobiltelefone beinhalten Terminkalender, Adressbücher, E Mail-Unterstützung und mehr. Um diese Funktionen sinnvoll einzusetzen, ist im Allgemeinen eine Synchronisation mit einem PC oder einem Internetdienst erforderlich. Daher muss geklärt werden, ob die Installation der dafür benötigten Hard- und Software erlaubt wird, beziehungsweise, ob dienstliche Daten mit diesen Internetdiensten verarbeitet und dort gespeichert werden dürfen.

Regelungen zur Nutzung dienstlicher Mobiltelefone

Notwendige Regeln für die Nutzung von dienstlichen Mobiltelefonen:

- Es muss geklärt werden, ob bzw. in welcher Menge Privatgespräche mit dienstlichen Mobiltelefonen geführt werden dürfen.
- Es muss zudem überlegt werden, die Nutzung der Mobiltelefone auf bestimmte Kommunikationspartner zu begrenzen, um zum Beispiel unnötigen Kosten vorzubeugen oder auch um die Informationsweitergabe einzuschränken. Hierzu kann eine organisatorische Vorgabe erfolgen, es kann aber auch technisch geregelt werden, wie weiter unten unter den Stichworten "Anrufsperrungen" und "Geschlossene Benutzergruppe" beschrieben.
- Auch bei dienstlichen Mobiltelefonen müssen die Benutzer über die Tarifstruktur, Roaming-Abkommen und Kosten informiert werden, damit sie beispielsweise im Ausland die günstigsten Netzbetreiber auswählen können, wobei die sichersten Netzbetreiber Priorität haben.
- Die Benutzer müssen darauf hingewiesen werden, wie sie sorgfältig mit den Mobiltelefonen umgehen, um einem Verlust oder Diebstahl vorzubeugen bzw. um eine lange Lebensdauer zu gewährleisten (z. B. Akkupflege, Aufbewahrung außerhalb von Büro- oder Wohnräumen, Empfindlichkeit gegenüber zu hohen oder zu niedrigen Temperaturen).
- Die Verwaltung, Wartung und Weitergabe von Mobiltelefonen muss geregelt werden. Hierzu empfiehlt sich die Einrichtung eines Mobiltelefon-Pools (siehe SYS.3.3.2).
- Bei jedem Benutzerwechsel müssen alle benötigten PINs gesichert weitergegeben werden.

Generelle Regelungen

Unabhängig davon, ob privat oder dienstlich angeschaffte Mobiltelefone genutzt werden, sollte der Arbeitgeber schriftlich regeln,

- dass der Fahrer in dienstlich genutzten Fahrzeugen während der Fahrt nicht ohne Freisprecheinrichtung telefonieren darf, da sonst bei einem Unfall Mithaftung droht,
- welche Daten auf dem Mobiltelefon gespeichert werden dürfen und ob für die Daten eine Datenverschlüsselung einzurichten ist,
- dass Dienstgeheimnisse nicht über das Mobiltelefon weitergegeben werden dürfen, weil Gespräche auch akustisch durch Personen in der unmittelbaren Umgebung mitgehört werden können,
- dass der Benutzer sich von der Identität seiner Gesprächspartner überzeugen sollte.

Für Endgeräte mit Zugriffsschutz muss es eine Passwortrichtlinie geben, die die Art des Zugriffschutzes (siehe SYS.3.3. *Nutzung von Sicherheitsmechanismen von Mobiltelefonen*) festlegt und die gegebenenfalls Regelungen zur Ausgestaltung enthält (Länge des Passwortes etc.). Es wird meistens als unkomfortabel empfunden, nach wenigen Minuten Untätigkeit immer wieder ein langes Passwort einzugeben. Daher sollten Institutionen einen angemessenen Kompromiss zwischen Sicherheit und Komfort wählen und nicht lediglich die Passwortrichtlinie für den Arbeitsplatz-PC übernehmen.

Wird das Mobiltelefon in fremden Büroräumen vor Ort benutzt, so muss die Sicherheitsregelungen der besuchten Institution zu beachten. Ein Mobiltelefon muss beaufsichtigt bleiben. Falls es in einem Kraftfahrzeug zurückgelassen werden muss, so muss das Gerät von außen nicht sichtbar sein und ausgeschaltet werden (Power Off). Auch in fremden Räumlichkeiten, wie Hotelzimmern, sollten Mobiltelefone bei Abwesenheit nicht ungeschützt herumliegen. Alle Passwort-Schutzmechanismen müssen spätestens jetzt aktiviert werden, bevor das Gerät ausgeschaltet wird (Power Off) und in den Safe oder zumindest an einen nicht sichtbaren Ort gebracht wird (Koffer).

Im Übrigen müssen Regelungen bei Verlust des Mobiltelefons (SYS.3.3.2) getroffen und den Mitarbeitern bekannt gegeben werden. Werden für moderne Mobiltelefone besondere Programme zum Orten, Löschen und Sperren des Endgerätes angeschafft, so sind die Mitarbeiter in der Bedienung dieser Programme zu schulen. Ferner müssen Regelungen geschaffen werden, wie mit zeitweise verlorenen und dann wieder gefundenen Geräten zu verfahren ist, da diese manipuliert sein könnten. Es empfiehlt sich, solche Geräte komplett zu löschen und alle relevanten Daten und Programme neu aufzuspielen.

Benutzungsverbot von Mobiltelefonen

Es muss überlegt werden, ob es in allen oder nur bestimmten Bereichen einer Institution verboten wird, Mobiltelefone zu benutzen oder mitzuführen (siehe SYS.3.3.5). Dies kann zum Beispiel für Besprechungsräume sinnvoll sein. Wenn die Sicherheitsleitlinie der Institution es nicht zulässt, dass Mobiltelefone mitgebracht werden, muss an allen Eingängen deutlich darauf hingewiesen werden. Dies sollte dann auch regelmäßig kontrolliert werden.

Durch Mobiltelefone können unter Umständen auch andere technische Geräte in ihrer Funktion beeinträchtigt werden. So können beispielsweise empfindliche IT Systeme in Serverräumen oder auch auf Intensivstationen durch Mobiltelefone gestört werden. Mögliche Störungen sind umso unwahrscheinlicher, je geringer die Sendeleistung des Mobiltelefons ist beziehungsweise, je weiter dieses entfernt ist.

Bei IT Systemen, auf denen sensitive Daten verarbeitet werden oder die an ein Rechner-Netz angebunden sind, sollten Verbindungen über ein Mobilfunknetz nur mit VPN-Techniken zugelassen werden (siehe SYS.3.3.M10 *Sichere Datenübertragung über Mobiltelefone*).

Telefonbuch

Im Telefonbuch eines Mobiltelefons können Rufnummern und zugehörige Namen oder weitere Details gespeichert werden, und zwar im Endgerät, also dem Mobiltelefon, einer eventuell vorhandenen zusätzlichen Speicherkarte oder auf der SIM-Karte. Das Telefonbuch auf dem Endgerät beziehungsweise der Speicherkarte hat für gewöhnlich eine größere Kapazität und erlaubt mehr Zusatzdaten als der Speicher der SIM-Karte, zum Beispiel Anschrift, Faxnummer, E-Mail-Adresse und weitere Notizen, sodass die Inhalte aus SIM-Karte und Endgerät nicht übereinstimmen müssen. Wo die Telefonnummern bevorzugt gespeichert werden sollen, hängt von verschiedenen Faktoren ab, beispielsweise wie einfach die Daten auf anderen Medien gesichert werden können (siehe SYS.3.3.11) oder wie hoch der Schutzbedarf der Informationen ist. Denn je nach Speicherort sind die Daten durch unterschiedliche Mechanismen geschützt: Liegen sie auf der SIM-Karte, kann auf die Informationen nur durch die korrekte PIN zugegriffen werden. Werden die Daten auf dem Endgerät oder einer externen Speicherkarte im Endgerät gespeichert, liegen sie in der Regel im Klartext vor und können nur durch zusätzliche Verschlüsselung geschützt werden. In diesem Fall bietet es sich an, den Passwortschutz für das Endgerät mit einer Verschlüsselung zu kombinieren.

Im Telefonbuch müssen alle wichtigen Rufnummern gespeichert werden, damit diese jederzeit verfügbar sind. Die gespeicherten Rufnummern müssen gelegentlich kontrolliert werden, ob sie noch korrekt beziehungsweise notwendig sind. Alle Rufnummern müssen so gespeichert werden, dass sie weltweit angerufen werden können, das heißt inklusive Landes- und Ortsvorwahl. Da nur der Ländercode international abgestimmt ist, nicht die Null, sollte dazu jede Rufnummer mit einem "+" am Anfang, gefolgt vom Ländercode (zum Beispiel +49 für Deutschland), Ortsvorwahl ohne führende Null und dann Telefonnummer eingegeben werden. Ein Eintrag könnte also wie folgt aussehen: +49228 999582-5369 GS-Hotline.

Wenn das Mobiltelefon von mehreren Benutzern eingesetzt wird, muss das Telefonbuch vor der Übergabe gelöscht und das Telefonbuch des neuen Benutzers aufgespielt werden. Die Telefonbücher aller Benutzer müssen dafür zentral vom Verwalter des Mobiltelefon-Pools gespeichert werden (siehe SYS.3.3.).

Anrufbeantworter

Über die Netzbetreiber kann im Allgemeinen zu einem Mobiltelefon eine Anrufbeantworter-Funktionalität aktiviert werden. Eingehende Anrufe werden dabei beim Netzbetreiber in einer so genannten Mail- oder Mobilbox gespeichert, die vom Benutzer jederzeit abgerufen werden kann. Dies kann sehr sinnvoll sein, verursacht aber in der Regel zusätzliche Kosten.

Der Zugriff auf die Mailbox sollte durch eine PIN geschützt werden. Auch wenn die Mailbox nicht genutzt wird, sollte die voreingestellte PIN schnell geändert werden, um eine Fremdnutzung zu verhindern.

Eingegangene Aufzeichnungen sollten regelmäßig abgehört werden. Alle Benutzer müssen darüber informiert werden, wie dies funktioniert.

Rufumleitung

Mit der Funktion Rufumleitung können eingehende Anrufe auf die Mailbox oder auf eine andere Rufnummer weitergeleitet werden. Dafür gibt es mehrere Varianten:

- Es können alle eingehenden Anrufe weitergeleitet werden.
- Anrufe werden nur dann weitergeleitet, wenn besetzt ist.
- Anrufe werden nur dann weitergeleitet, wenn der Anschluss nicht erreichbar ist, z. B. wegen eines Funklochs oder weil das Mobiltelefon ausgeschaltet ist.
- Es können bestimmte Arten von Anrufen weitergeleitet werden, z. B. Sprach-, Daten- oder Faxanrufe.
- Viele Smartphones gestatten sogar eine telefonnummerngenaue Einrichtung von Weiterleitungen auf andere Anschlüsse oder den Anrufbeantworter.

Dabei muss allerdings berücksichtigt werden, dass Rufumleitungen auf Festnetzanschlüsse hohe Kosten verursachen können, da der Angerufene die Weiterleitungskosten selbst tragen muss.

Anrufsperrungen

Über Anrufsperrungen können Gespräche zu oder von einer Rufnummer gesperrt werden. Diese Funktionen werden über den Netzbetreiber zur Verfügung gestellt und können über das Mobiltelefon geändert werden. Dafür ist im Allgemeinen ein Passwort erforderlich. Viele Smartphones können Anrufsperrungen ohne Unterstützung des Netzbetreibers durch lokale Software realisieren, die in der Regel viel feinteiliger konfiguriert werden kann.

Anrufsperrungen können sinnvoll sein, wenn das Mobiltelefon an Dritte weitergegeben werden soll. Es gibt verschiedene Möglichkeiten von Anrufsperrungen:

- Sperren aller abgehenden Anrufe (Notrufnummern sind davon ausgenommen)
- Sperren aller abgehenden internationalen Anrufe
- Sperren aller abgehenden internationalen Anrufe außer ins Heimatland
- Sperren aller ankommenden Anrufe
- Sperren aller ankommenden Anrufe bei Aufenthalt im Ausland
- Sperren bestimmter ankommender oder abgehender Anrufe

Ob und welche Art von Anrufsperrungen gewählt werden sollte, hängt von der Einsatzart des jeweiligen Mobiltelefons ab.

Geschlossene Benutzergruppe

Über den Dienst "Geschlossene Benutzergruppe" kann die Kommunikation auf die Mitglieder dieser Gruppe beschränkt werden.

Die Gruppenmitglieder müssen beim Netzbetreiber eingetragen werden. Die Option "Geschlossene Benutzergruppe" kann am Mobiltelefon aktiviert werden. Geschlossene Benutzergruppen sind beispielsweise sinnvoll, um die Datenübertragung über Mobilfunk einzuschränken. Auf vielen Smartphones können solche Benutzergruppen in der Regel auch lokal, ohne Einbindung des Netzbetreibers, umgesetzt werden.

SYS.3.3.M2 Sperrmaßnahmen bei Verlust [Benutzer]

Bei Verlust der SIM-Karte bzw. des Mobiltelefons trägt der Inhaber der SIM-Karte die Kosten für eine missbräuchliche Nutzung des Mobiltelefonanschlusses. Daher muss die SIM-Karte beim Netzbetreiber sofort gesperrt werden, um einen eventuellen Missbrauch, und damit einen zusätzlichen finanziellen Schaden, abzuwehren.

Darüber hinaus muss die PIN-Abfrage der SIM-Karte stets aktiviert sein (siehe SYS.3.3.M5). Bei einem Diebstahl oder Verlust verhindert dies, dass die SIM-Karte von einem Unbefugten benutzt oder ausgewertet werden kann. Bei deaktivierter SIM PIN kann ein nicht legitimierter Nutzer die SIM aktivieren oder die durch mehrfache Falscheingaben unbrauchbar machen. Die PIN wird allerdings nur abgefragt, wenn das Mobiltelefon eingeschaltet wird (Power On). Wird ein eingeschaltetes Mobiltelefon gestohlen, kann hiermit zumindest solange missbräuchlich telefoniert werden, bis der Akku leer ist.

Für Smartphones gibt es auf dem Markt Software zum Diebstahlschutz, die es erlaubt, das Mobiltelefon per GPS-Empfänger oder Mobilfunkzellen zu orten, die Daten auf dem Gerät zu löschen oder das Gerät vollständig zu sperren. Gegebenenfalls können sogar automatisierte Nachrichten an den IT-Betrieb über die Sperrung oder den Aufenthaltsort eines Gerätes versandt werden, wenn beispielsweise die SIM-Karte ausgetauscht wurde. Viele dieser Programme gestatten es auch Nachrichten an das Telefon zu senden oder aktivieren lediglich eine Displayanzeige, die den Finder bitten, die Telefonnummer des IT-Betriebs anzurufen oder das Gerät an einer bestimmten Adresse abzugeben. Die Anschaffung einer solchen Software kann sich schnell bezahlt machen, wenn ein verloren gegangenes Smartphone schneller zurückgegeben werden kann und die Daten besser vor Dieben geschützt sind. Auf der anderen Seite muss permanent das GPS aktiviert und eine Mobilfunk-Verbindung aufgebaut sein. Dies kann zu einem erhöhen Akkuverbrauch führen, zusätzlichen kann die notwendige Geräteortung durch Dritte missbraucht werden (siehe SYS.3.3.M3 und SYS.3.3.9).

Um rechtzeitig zu bemerken, dass die SIM-Karte womöglich missbräuchlich genutzt wurde, muss der Einzelverbindungsnachweis immer auf unerklärliche Gebühren und Zielrufnummern überprüft werden.

Alle Daten, die für die Sperrung der SIM-Karte bzw. des Mobiltelefons benötigt werden, sollten griffbereit, aber getrennt vom Mobiltelefon aufbewahrt werden. Das sind

- die Rufnummer des Mobilfunkanschlusses sowie die zugehörige -Kartennummer,
- die Seriennummer des Mobiltelefons (GSM - USSD -Code *#06#),
- die Servicenummer des Netzbetreibers, unter der der Sperrwunsch gemeldet werden kann sowie
- das Servicenummer-Passwort und die Kundennummer, also die Daten, die für die Authentikation gegenüber dem Netzbetreiber benötigt werden.

SYS.3.3.M3 Sensibilisierung und Schulung der Mitarbeiter im Umgang mit Mobiltelefonen [Personalabteilung, Vorgesetzte]

Zusätzlich zur allgemeinen Schulung und Sensibilisierung zur Informationssicherheit müssen Mitarbeiter, die Mobiltelefone einsetzen, für die besonderen Aspekte der Informationssicherheit bei diesen Geräten sensibilisiert werden. Für die Schulungs- und Sensibilisierungsplanung sind daher die Mitarbeiter, die diese Geräte nutzen, gesondert zu erfassen und entsprechend diesem Plan zu schulen und zu sensibilisieren.

Mobiltelefone sind durch ihre geringe Größe und den vergleichsweise hohen Preis besonders gefährdet, verloren oder gestohlen zu werden. Mitarbeiter sind daher besonders darauf hinzuweisen, diese Geräte nicht aus den Augen zu lassen und bei einem Verlust umgehend angemessene Maßnahmen wie Ortung, Löschung und Sperrung der Geräte selbst bzw. durch den IT-Betrieb zu veranlassen.

Mit dem Verlust des Gerätes sind, wenn weitere Sicherheitsmaßnahmen fehlen, auch die Daten auf dem Gerät verloren. Heutige Endgeräte können Datenmengen im mehrstelligen Gigabyte-Bereich speichern, was ausreichend Platz für vertrauliche Geschäftsdaten, Preiskalkulationen, Adressbücher und E-Mails bietet. Deswegen müssen Sicherheitsmaßnahmen ergriffen werden, wie z.B. die vollständige Verschlüsselung aller Daten auf dem Endgerät und die Sperrung des Gerätes durch ein Passwort, nachdem es mehrere Minuten nicht benutzt wurde. Erfahrungsgemäß werden solche notwendigen Maßnahmen von den Mitarbeitern kritisch gesehen, da der Aufwand bei der Nutzung der Endgeräte steigt. Daher müssen die Mitarbeiter für die hier genannte Gefährdung der Informationssicherheit sensibilisiert und in der zusätzlichen Sicherheitsmaßnahme geschult werden.

Mobiltelefone können in der Regel auf das Internet und auf E-Mails zugreifen. Mitarbeiter müssen die damit verbundenen Gefahren kennen: Das Gerät kann mit Schadsoftware infiziert werden. Schützenswerte Daten können vom Gerät gestohlen bzw. das Gerät kann zum Abhören von Raumgesprächen und Telefonaten genutzt werden. Daher müssen die Geräte vor Schadsoftware geschützt werden, beispielsweise durch die Installation geeigneter Schutzsoftware. Zudem muss überlegt werden, den gesamten Datenverkehr der Mobiltelefone über VPN durch einen Server der Institution zu leiten, um dort bereits Schadsoftware und Angriffe abzuwehren. Auch für diese Gefährdungen und die dadurch entstehenden Einschränkungen müssen die Mitarbeiter entsprechend sensibilisiert werden.

Da oft leichtfertig mit der Abhörgefahr im Telekommunikationsbereich umgegangen wird, müssen Institutionen prüfen, inwieweit die bisherigen Maßnahmen zur Aufklärung ihrer Mitarbeiter über Gefährdungen im Telekommunikationssektor ausreichen. Gegebenenfalls ist es angebracht, die Mitarbeiter regelmäßig über die Abhörgefahren zu informieren und damit auch zu sensibilisieren.

Die Mitarbeiter müssen auch darüber aufgeklärt werden, dass sie vertrauliche Informationen nicht ohne Weiteres telefonisch weitergeben. Insbesondere muss die Identität des Kommunikationspartners hinterfragt werden, bevor detaillierte Auskünfte gegeben werden. Bei der Benutzung von Mobiltelefonen müssen sie außerdem darauf achten, dass vertrauliche Mitteilungen nicht in der Öffentlichkeit besprochen werden. Dies gilt insbesondere auch bei Kurzmitteilungen, die von einer vermeintlich bekannten Nummer abgesendet wurden. Werden über Kurzmitteilungen oder Chats vertrauliche Informationen angefragt, muss immer durch einen Rückruf überprüft werden, ob die Anfrage wirklich vom vorgegebenen Kommunikationspartner stammt. Eine solche Überprüfung sollte auch stattfinden, wenn unerwartet von einer bekannten Nummer ein Dateianhang oder ein Link geschickt wurde.

Immer wieder kursieren spektakuläre, aber falsche Warnmeldungen. Damit nicht wertvolle Arbeitszeit auf die Prüfung des Wahrheitsgehaltes solcher Nachrichten verschwendet wird, müssen alle Mitarbeiter schnellstmöglich über das Auftreten eines neuen Hoax informiert werden. Es gibt verschiedene Informationsdienste, die entsprechende Warnungen weitergeben.

Diese Sicherheitsmaßnahmen schränken den Komfort der Endgeräte in der Regel ein. So führt die vollständige Verschlüsselung zu einer längeren Wartezeit beim Einschalten des Gerätes, ein angemessenes Passwort laufend einzugeben, wird als störend empfunden und den kompletten Datenverkehr durch einen Server der Institution zu leiten, führt zu längerer Wartezeit beim Surfen im Internet. Zudem erhöht jedes zusätzliche Sicherungsprogramm den Stromverbrauch und verkürzt damit die Akkulaufzeit. Diese Einschränkungen können daher dazu führen, dass die Mitarbeiter Sicherheitsmaßnahmen zu umgehen versuchen, weshalb im Rahmen der Sensibilisierung der Mitarbeiter besonders auf die Gefährdung der Informationssicherheit durch mobile Endgeräte wie Mobiltelefone eingegangen werden muss, damit die Maßnahmen auch dauerhaft wirksam sein können.

SYS.3.3.M4 Aussonderung und ordnungsgemäße Entsorgung von Mobiltelefonen und Speicherkarten

Immer wieder werden auf gebrauchten Mobiltelefonen vertrauliche Daten der Vorbesitzer entdeckt und so die Informationssicherheit der Institution, die das Gerät verkauft oder ungenügend ausgesondert hat, verletzt. Auch für gezielte Angriffe werden Endgeräte von Institutionen aufgekauft und auf sensitive Daten hin untersucht.

Auf ausgesonderten Mobiltelefone müssen alle schützenswerten Informationen auf geeignete Weise vernichtet werden. Dazu muss der Gerätespeicher und die gegebenenfalls vorhandene Speicherkarte mit einer speziellen Software gelöscht werden. Das Gerät ist auf den Werkszustand zurückzusetzen. Außerdem muss überprüft werden, ob alle Daten auch wirklich gelöscht wurden, dazu kann der Verantwortliche spezielle Computer-Forensik-Software und Geräte einsetzen. Werden mittels forensischem Ansatz dennoch entsprechend kritische Daten gefunden und es existiert für das spezielle Mobiltelefon keine Methode zum sicheren Löschen, wird empfohlen, das Gerät zu vernichten. Wird nur die externe Speicherkarte ausgesondert oder entsorgt, muss SYS.3.3.*M4 Aussonderung und ordnungsgemäße Entsorgung von Mobiltelefonen und Speicherkarten* beachtet werden.

Soll ein Mobiltelefon verkauft werden, bei dem durch Maßnahmen zur Informationssicherheit der Betriebssystemkern oder das Betriebssystem verändert wurde, so muss berücksichtigt werden, dass durch diese Maßnahme in der Regel die Garantie bzw. der Support durch den Hersteller erlischt. Daher ist zu überlegen, ob diese Maßnahmen vor einem Verkauf rückgängig gemacht werden müssen.

Mobiltelefons dürfen in der Regel nicht über den Hausmüll entsorgt werden. Entsprechende Regelungen zur Entsorgung müssen beachtet und kontrolliert werden.

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich SYS.3.3 *Mobiltelefon*.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Mobiltelefon".

SYS.3.3.M5 Nutzung der Sicherheitsmechanismen von Mobiltelefonen [Benutzer]

Mobiltelefone und dazu angebotene Dienstleistungen können an verschiedenen Stellen durch PINs oder Passwörter abgesichert werden. Hierzu gehören:

Zugriff auf die SIM-Karte

Die SIM-Karte sollte durch eine vier- bis achtstellige PIN gegen unberechtigten Zugriff geschützt werden. Mit dieser PIN identifiziert sich der Teilnehmer gegenüber der Karte. Gelangt ein Unbefugter in den Besitz einer SIM-Karte, kann er ohne Kenntnis der PIN diese Karte nicht aktivieren. Um eine missbräuchliche Benutzung der SIM-Karte zu verhindern, sollte daher unbedingt die PIN-Abfrage aktiviert werden, sodass die PIN nach dem Einschalten des Mobiltelefons eingegeben werden sollte. Die PIN sollte nicht zusammen mit dem Mobiltelefon bzw. der SIM-Karte aufbewahrt werden.

Bei der Auslieferung ist meist die PIN-Abfrage deaktiviert und eine PIN voreingestellt. Bei der ersten Benutzung sollte unbedingt die PIN geändert und aktiviert werden. Hierbei sollte keine triviale oder leicht vorhersagbare PIN gewählt werden (1111, Geburtsdatum, etc.).

Hinweis: Auf der Tastatur der meisten Mobiltelefone sind unter den Ziffern Buchstaben unterlegt. Dies kann dazu benutzt werden, sich statt PINs Passwörter auszuwählen, die leichter zu merken sind, aber natürlich auch wieder nicht zu einfach sein sollten. Beispiel: "4AUGEN" entspricht der PIN "428436".

Nach dreimaliger falscher PIN-Eingabe wird die SIM-Karte in der Regel gesperrt. Um diese Sperre aufheben zu können, muss ein achtstelliger Entsperrcode eingegeben werden. Dieser wird häufig auch als PUK (Personal Unblocking Key) oder Super- bezeichnet. Nach zehnmaliger Falscheingabe der PUK wird die Karte unbrauchbar. Dieser Entsperrcode wird normalerweise in einem PIN-Brief zusammen mit der SIM-Karte ausgeliefert. Er sollte äußerst sorgfältig und vor unbefugtem Zugriff geschützt aufbewahrt werden. Die PUK darf auf keinen Fall zusammen mit dem Mobiltelefon aufbewahrt werden.

Neben der PIN gibt es mit der PIN 2 noch eine weitere Geheimzahl, mit der der Zugriff auf bestimmte Funktionen der SIM-Karte abgesichert werden kann. Sie wird häufig benutzt für Konfigurationsänderungen der SIM-Karte, die nicht vom Benutzer selbst durchgeführt werden können, z.B. Nutzungsrestriktionen. Dies kann aber beispielsweise auch ein Firmentelefonbuch sein, das nur nach der Eingabe der PIN 2 geändert werden kann. Die PIN 2 hat einen eigenen Entsperrcode (PUK2).

Zugriff auf das Mobiltelefon

Darüber hinaus gibt es im Allgemeinen noch einen Sicherheitscode für das Mobiltelefon (Geräte- PIN), um den Zugriff auf bestimmte Funktionen zu schützen. Auch dieser sollte schnellstmöglich auf einen individuell gewählten Wert gesetzt werden. Er sollte notiert und vor unbefugtem Zugriff geschützt aufbewahrt werden. Alternativ bieten moderne Mobiltelefone einen Zugriffsschutz per Passwort, Gesten, Fingerabdruck oder Gesichtserkennung. Das Mobiltelefon sollte so eingestellt werden, dass der Sicherheitscode nach einigen Minuten Untätigkeit erneut eingegeben werden muss. Es sollte eine PIN, ein Passwort oder, eine Geste nach der jeweiligen Sicherheitsrichtlinie der Institution gewählt werden. Alternativ kann ein Fingerabdruckscanner benutzt werden. Da eine Gesichtserkennung bereits mit einfachen Fotos vom Gesicht des Benutzers getäuscht werden kann, sollte dieses Verfahren nicht eingesetzt werden.

Diebstahlschutz durch zusätzliche Applikationen

Moderne Mobiltelefone bieten die Möglichkeit, durch zusätzliche Applikationen das Mobiltelefon bei Verlust oder Diebstahl zu orten, seine Daten zu löschen bzw. es komplett zu sperren. Es sollte eine passende Applikation ausgewählt und eingesetzt werden. Die betreffenden Mitarbeiter sollten im Umgang mit dieser Applikation geschult werden.

Zugriff auf Mailbox

Beim Netzbetreiber kann für jeden Teilnehmer eine Mailbox eingerichtet werden, die unter anderem als Anrufbeantworter dient. Da die Mailbox von überall und auch von beliebigen Endgeräten aus abgefragt werden kann, sollte sie mit einer PIN vor unbefugtem Zugriff geschützt werden. Bei der Neueinrichtung vergibt der Netzbetreiber hierzu eine voreingestellte PIN. Diese sollte unbedingt sofort geändert werden.

Weitere Kennwörter

Neben den diversen oben aufgeführten Geheimnummern kann es für verschiedene Nutzungsarten noch weitere Kennwörter geben. Dies ist z.B. der Fall beim Zugriff auf Benutzerdaten beim Netzbetreiber. So sollte bei Fragen an die Hotline wegen der Abrechnung unter Umständen ein Kennwort genannt werden. Auch kostenpflichtige Dienstleistungen wie z.B. der Abruf von Informationen oder die Durchführung bestimmter Konfigurationen seitens des Netzbetreibers bzw. Mobilfunkanbieters werden häufig durch zusätzliche Kennwörter geschützt. Diese sollten, wie alle anderen Passwörter auch, sorgfältig ausgewählt, sicher aufbewahrt und nicht an Dritte weitergegeben werden.

Generell sollte mit allen PINs und Passwörtern sorgfältig umgegangen werden.

SYS.3.3.M6 Updates von Mobiltelefonen [Benutzer]

Es sollte regelmäßig geprüft werden, ob es Softwareupdates für die Mobiltelefone gibt. Der Umgang mit Updates sollte geregelt werden. Wenn es neue Softwareupdates gibt, sollte festgelegt werden, wie die Benutzer darüber informiert werden. Zudem sollte festgelegt werden, ob die Benutzer die Updates selbständig installieren dürfen oder ob die Mobiltelefone an einer zentralen Stelle hierfür abgegeben werden sollen. Wenn die Benutzer die Updates selbständig installieren sollen, ist zu klären, ob sie hierzu das notwendige Wissen haben. Außerdem sollte dann nachgehalten werden, dass die Updates auch zeitnah eingespielt werden.

SYS.3.3.M7 Beschaffung von Mobiltelefonen

Wie bei allen anderen Geräten auch, sollte eine Anforderungsliste erstellt werden, bevor Mobiltelefone beschafft werden. Anhand dieser Anforderungsliste sollten die am Markt erhältlichen Produkte bewertet werden.

SYS.3.3.M8 Nutzung von drahtlosen Schnittstellen [Benutzer]

tbd

SYS.3.3.M9 Sicherstellung der Energieversorgung [Benutzer]

Akkus von Mobiltelefonen können das Gerät je nach Kapazität und Bauweise des Telefons für einen beschränkten Zeitraum, üblicherweise einige Stunden, mit Energie versorgen. Damit ein Mobiltelefon im Bedarfsfall jederzeit verfügbar ist bzw. keine Daten in flüchtigen Speichern verloren gehen, sollten einige Randbedingungen beachtet werden:

- Die Warnanzeigen des Mobiltelefons, die den Spannungsabfall anzeigen, dürfen nicht ignoriert werden.
- Falls ein längerfristiger mobiler Einsatz absehbar ist, sollte ein Ladegerät mitgeführt werden. Ist kein Ladegerät verfügbar, kann das Mobiltelefon gegebenenfalls über das Datenkabel an einer USB-Schnittstelle eines PCs oder Laptops aufgeladen werden. Dies dauert in der Regel deutlich länger als mit einem Ladegerät. Es sollte auch bedacht werden, dass durch diese Form des Aufladens auch eine Datenverbindung möglich ist und Daten abfließen oder verändert werden können.
- Beim Laden sollten die Hinweise im Handbuch zum Mobiltelefon beachtet werden, insbesondere sollte die Lebensdauer des Akkus nicht beeinträchtigt werden.
- Bei der Übergabe eines Mobiltelefons ist der ausreichende Ladezustand der Akkus sicherzustellen. Der Ladezustand der Akkus sollte regelmäßig überprüft werden, da sich ein Akku im Laufe der Zeit entlädt, auch wenn er nicht verwendet wird.

Wenn eine längere Nutzung des Mobiltelefons absehbar ist, z.B. bei Dienstreisen, kann auch gegebenenfalls ein geladener Ersatzakku mitgeführt werden. Der Ersatzakku sollte in einer Schutzhülle verwahrt werden, da Schäden durch Überhitzung oder Brand entstehen können, wenn die Kontakte des Akkus mit leitenden Materialien in Berührung kommen. Dies kann durch viele Gegenstände des täglichen Gebrauchs wie Schlüssel oder Ketten verursacht werden. Wenn die Akkus nicht getauscht werden können, z.B. weil dieser fest verbaut ist, könnte auch auf externe Akku-Packs zurückgegriffen werden.

Ein Mobiltelefon sollte ausgeschaltet werden, bevor der Akku gewechselt wird, damit der Speicher nicht beschädigt wird.

Ein Mobiltelefon sollte keinen extremen Temperaturen ausgesetzt werden. Insbesondere der Akku, aber auch das Display können anderenfalls ihre Funktionsfähigkeit einbüßen. Da die Temperatur in Autos über Nacht oder beim Parken in der Sonne stark schwanken kann, sollten weder Mobiltelefone noch Akkus in geparkten Autos zurückgelassen werden.

Um den Akku des Mobiltelefons zu schonen, sollten Bluetooth, IrDA, WLAN, GPS und Mobilfunk-Internetverbindung nur bei Bedarf aktiviert werden.

SYS.3.3.M10 Sichere Datenübertragung über Mobiltelefone [Benutzer]

Mobiltelefone werden für die Sprachübertragung eingesetzt, es können aber auch Daten und Faxe damit übermittelt werden. Für einige dieser Dienste wird zusätzliches Zubehör benötigt. Moderne Mobiltelefone sind in der Regel dauerhaft mit dem Internet verbunden, um Chat-Nachrichten oder E-Mails zu empfangen. Benutzen Mobiltelefone den LTE-Standard, wird jegliche Kommunikation als Datenübertragung über das Internet-Protokoll (IP) realisiert.

Kurzmitteilungen

Mit dem Kurznachrichtendienst (Short Message Service, SMS) lassen sich Texte mit maximal 160 Zeichen von einem Mobiltelefon zum anderen oder auch an E-Mail-Adressen senden. Längere Nachrichten werden dabei in der Regel automatisch vom Mobiltelefon in mehrere Kurzmitteilungen aufgeteilt. Die Übertragung von Kurzmitteilungen erfolgt immer über eine Kurzmitteilungs-Zentrale, die die Nachrichten an den jeweiligen Empfänger weiterleitet.

Kurzmitteilungen werden im Mobiltelefon gespeichert, solange Speicherplatz verfügbar ist. Wenn kein ausreichender Speicherplatz (oft bei älteren oder extrem preisgünstigen Modellen) mehr frei ist, können keine weiteren Kurzmitteilungen empfangen werden. Der Netzbetreiber versucht nur über einen begrenzten Zeitraum, weitere Nachrichten abzusetzen. Wenn nicht rechtzeitig Speicherplatz freigemacht wird, werden die Kurzmitteilungen beim Netzbetreiber gelöscht.

Teilweise kann auch über das Mobiltelefon der Zeitraum, über den Kurzmitteilungen beim Netzbetreiber zwischengespeichert werden, verändert werden. Die Voreinstellung liegt im Allgemeinen zwischen 24 und 48 Stunden. Wenn der Vertrag mit dem Netzbetreiber es nicht vorsieht, kann hierüber allerdings der Speicherungszeitraum nicht erhöht werden. Er sollte auch nicht verringert werden.

Je nach Mobilfunkanbieter besteht die Möglichkeit, dass der Absender der Kurznachricht eine automatische Empfangsbestätigung erhält. Damit sichergestellt wird, ob die Nachrichten empfangen wurden, sollten Empfangsbestätigungen aktiviert werden. Damit lässt sich zusätzlich auch nachvollziehen, ob die Nachricht wegen zu kurzer Speicherfristen bei der Kurzmitteilungs-Zentrale womöglich nicht zugestellt wurde. Die Empfangsbestätigungen sollten so lange wie nötig auf dem Mobiltelefon gespeichert werden.

Um Kurzmitteilungen verschicken zu können, sollte die Rufnummer der Kurzmitteilungs-Zentrale (SMS-Gateway) über das entsprechende Menü am Mobiltelefon voreingestellt werden. Meist ist dies schon auf der SIM-Karte vom Netzbetreiber vorkonfiguriert worden.

Im Internet gibt es diverse Angebote, Kurzmitteilungen mit minimalen Kosten zu versenden. Ein Angreifer kann also ohne großen Aufwand eine große Anzahl von SMS-Nachrichten an ein Mobiltelefon versenden. SMS-Spam wirkt sich ebenso aus wie E-Mail-Spam. Die Mailbox bzw. der Speicherplatz reicht nicht aus und ernsthafte Nachrichten kommen nicht durch. Darüber hinaus entstehen dem Benutzer eventuell hohe Kosten. Hiergegen hilft neben der Sperrung von Drittanbieter-Diensten durch den Provider bzw. Mobilfunkanbieter, im Vorfeld die eigene Rufnummer nicht zu breit zu streuen, also auf den Eintrag in Telefonbücher zu verzichten, bzw. im Schadensfall eine Zeit lang ganz auf SMS-Empfang zu verzichten.

Eine Identifikation des Absenders ist bei SMS nicht zuverlässig möglich. Sie erfolgt maximal über die Rufnummer des Absenders und diese wird je nach Netzbetreiber bzw. Konfiguration des Mobiltelefons nicht immer mit übertragen. Beim Versand von Kurzmitteilungen über das Internet erfolgt im Allgemeinen überhaupt keine eindeutige Identifizierung. Dies sollte allen Benutzern klar sein, um die Echtheit einer Nachricht richtig einschätzen zu können. Je nach Inhalt einer empfangenen Kurzmitteilung ist es sinnvoll nachzufragen, ob diese wirklich vom angegebenen Absender stammt.

Faxe

Es können Faxe über ein mit dem Mobiltelefon gekoppeltes IT-System (z.B. Notebook) gesendet und empfangen werden.

Dabei ist ähnlich wie bei herkömmlichen Faxgeräten zu beachten, dass

- der Speicherplatz des Mobiltelefons durch empfangene Faxe überlastet werden kann,
- es je nach Bedeutung von Faxen erforderlich sein kann, davon Kopien anzufertigen, was beim Mobiltelefon unter Umständen schwierig ist,
- es sinnvoll sein kann, die Rufnummern von bestimmten Faxempfängern bzw. Absendern zu sperren.

Außerdem empfiehlt sich,

- nach dem Versand nachzufragen, ob das Fax lesbar angekommen ist,
- nach dem Empfang nachzufragen, ob das Fax wirklich vom angegebenen Absender stammt,
- ab und zu die programmierten Zieladressen zu kontrollieren.

E-Mail

Über Mobiltelefone können neben Kurzmitteilungen auch E-Mails empfangen und verschickt werden. Bei älteren Endgeräten sind E-Mails wie Kurzmitteilungen auf 160 Zeichen begrenzt. Wenn dieser Service vom Netzbetreiber eingerichtet worden ist, erhält das Mobiltelefon eine eigene E-Mail-Adresse. In der Regel besitzen Mobiltelefone heute jedoch E-Mail-Clients, die E-Mails wie ein PC verarbeiten können. Besitzen Mobiltelefone keinen E-Mail-Client aber einen Browser, so können E-Mails in der Regel über eine Web-Oberfläche verarbeitet werden.

Bei einigen Netzbetreibern können E-Mail-Dienste mit anderen Diensten kombiniert werden. So können eingehende E-Mails von einem Sprachcomputer vorgelesen werden, an ein Faxgerät oder eine andere E-Mail-Adresse weitergeleitet werden. Ausgehende E-Mails können ins Mobiltelefon gesprochen und als Audiodatei versandt werden.

Wie Kurzmitteilungen und Faxe können auch E-Mails schnell den vorhandenen Speicherplatz (bei älteren oder extrem preisgünstigen Geräten) ausschöpfen. Der E-Mail-Client sollte daher so eingestellt werden, dass Dateianhänge nur bei Bedarf, also wenn der Benutzer sie explizit anfragt, nachgeladen werden.

Potenzielle Sicherheitsprobleme und Anforderungen für E-Mail sind in Baustein APP.5.1. *Allgemeine Groupware* beschrieben. Dabei ist zu beachten, dass die E-Mail-Funktionalität bei Mobiltelefonen stark eingeschränkt ist gegenüber anderen E-Mail-Anwendungen. Ebenso wie SMS ist E-Mail hier eher für die Übermittlung kurzer und kurzlebiger Nachrichten gedacht. Sicherheitsmaßnahmen, wie Verschlüsselung oder Signatur, sind in der Regel nur mit Smartphones möglich. Alternativ gibt es noch spezielle Geräte oder zusätzliche Module, mit denen verschlüsselte oder signierte Nachrichten mit einem Mobiltelefon übermittelt werden können.

Instant Messenger

Auf einigen Mobiltelefonen und den meisten Smartphones sind Instant Messenger vorhanden oder lassen sich nachträglich installieren. Mit Instant Messengern können Nachrichten, aber auch Dateien wie z.B. Bilder, Filme, und Office-Dokumente übertragen werden. Auch Instant Messenger, die über das Internet-Relay-Chat-(IRC)-System funktionieren, werden vielfach eingesetzt. Die Kommunikation über Instant Messenger sollte, wenn möglich, Ende-zu-Ende-verschlüsselt erfolgen. Es dürfen nur vertrauenswürdige IRC-Server bzw. Instant-Message-Provider verwendet werden. In diesem Fall ist die Vertraulichkeit der Kommunikation gegenüber Kurznachrichten deutlich erhöht. Dubiose Dateiübertragungen sollten abgelehnt werden. Instant Messenger haben zudem gegenüber den Kurznachrichten den Vorteil, dass Kosten nach Datenmenge und nicht nach Anzahl der Nachrichten entstehen. Zusätzlich besitzen viele Instant Messenger die Funktion der Empfangsbestätigung, die auch genutzt werden sollte, um der Gefahr der Nichtanerkennung von Nachrichten zu begegnen.

Datenübertragung

Ein Mobiltelefon kann je nach Modell mit einem weiteren IT-System (z.B. einem Notebook oder einem Organizer) gekoppelt werden und dann leichter auch größere Datenmengen übertragen. Dabei kann die Kopplung auf verschiedene Arten erfolgen, je nachdem, welche Techniken die beiden Geräte unterstützen.

Einsteckkarte: Eine Einsteckkarte (PC-Card, PCMCIA) ist die ursprünglich konventionelle, aber mittlerweile kaum noch eingesetzte Lösung zur Verbindung von Mobiltelefon und Notebook. Die meisten Einsteckkarten können allerdings nur an Mobiltelefone eines bestimmten Herstellers angeschlossen werden.

Softmodem: Bei dieser Lösung wird statt einer Einsteckkarte eine spezielle Software auf dem Notebook installiert. Das Mobiltelefon wird dann einfach über die serielle (oder USB) Schnittstelle mit dem Notebook verbunden. Diese Lösung ist meist preiswerter als eine Einsteckkarte.

Infrarot: Über eine Infrarot-Schnittstelle können Daten auch ohne Kabel vom Mobiltelefon zu einem anderen Gerät (z.B. Laptop oder Organizer) übertragen werden. Dazu sollte sowohl das Mobiltelefon als auch das Partnergerät den Infrarot Übertragungsstandard IrDA unterstützen. IrDA ist ein weltweiter Standard für die Datenübertragung über Infrarot, wird aber für Datenübertragungen heute kaum noch eingesetzt (siehe SYS.3.3.8).

Bluetooth: Bluetooth ist ein etablierter Standard, nach dem Geräte per Funk über Entfernungen von 1 bis 100m (je nach Bluetooth-Klasse) miteinander Daten austauschen können.

WLAN: Über Wireless- LAN kann ein Mobiltelefon mit einem Rechnernetz verbunden werden oder es kann selbst als sogenannter WLAN-Hotspot fungieren ("Tethering") und eine Internetverbindung für andere IT-Systeme bereitstellen. Die WLAN-Verbindung sollte dabei über kryptografisch abgesichert werden. Weitere Details zum Einsatz von WLAN sind im Baustein NET.2.1 *WLAN-Betrieb* und NET.2.2 *WLAN-Nutzung* zu finden.

Bei der Datenübertragung z.B. von einem Laptop über das Mobilfunknetz sollten die übertragenen Daten vorher auf dem Endgerät verschlüsselt werden. Hierzu gibt es eine Vielzahl von Applikationen, die dies einfach ermöglichen. Die Verschlüsselung vor der Übertragung sichert die Informationen auf der gesamten Strecke zwischen Absender und Empfänger. Dies geht über die bei GSM standardmäßige Absicherung der Luftschnittstelle zwischen Mobiltelefon und Basisstation hinaus. Das ist notwendig, weil die Verschlüsselung über das GSM-Netz auf der Luftschnittstelle als gebrochen gilt. Bei schlechter Umsetzung bietet die Verschlüsselung bei der Übertragung mit UMTS auch keinen besseren Schutz als bei der Übertragung mit GSM. Werden die Daten hingegen mithilfe von Programmen auf dem Endgerät verschlüsselt, können die Nachrichten zudem noch digital signiert werden. Wie adäquate kryptografische Verfahren und Systeme ausgewählt und eingesetzt werden können, ist im *CON.1 Kryptokonzept* beschrieben. Alternativ zur Verschlüsselung der Daten bieten moderne Mobiltelefone vielfach die Möglichkeit, verschlüsselte VPN-Tunnel zu etablieren, womit die Datenübertragung zwischen Mobiltelefon und anderen Netzteilnehmern ebenfalls hinreichend abgesichert werden kann. Alternativ könnte ein vorhandener Laptop auch als VPN-Endpunkt verwendet werden, über diesen das Mobiltelefon eine geschützte Datenverbindung aufbauen kann. Wird VPN verwendet, besteht überdies der Vorteil, dass die Verschlüsselung transparent ist und keine weitere Benutzerinteraktion benötigt.

Besitzt das Mobiltelefon einen Browser und E-Mail-Client, so ist es über diese Kanäle so verwundbar wie ein PC. Unbedacht heruntergeladene Dateien, Klingeltöne, aber auch Drive-by-Infektionen können die Geräte ebenso funktionsuntüchtig machen wie stationäre Computer.

Die Datenübertragung sollte in allen Organisationen klar geregelt sein. Alle Datenübertragungseinrichtungen sollten genehmigt sein und deren Nutzung klaren Regelungen unterliegen.

Damit durch die Datenübertragung über GSM-Schnittstellen keine Sicherheitslücken entstehen, sollte diese restriktiv gehandhabt werden. So sollten bei IT-Systemen, auf denen sensitive Daten verarbeitet werden, keine Mobilfunkkarten zugelassen werden bzw. Verbindungen über das Mobilfunknetz immer mit verschlüsselten VPN-Tunneln abgesichert sein. Dies gilt ebenso bei allen IT-Systemen, die an einem Datennetz angebunden sind, damit hier nicht der durch eine Firewall eigentlich vorhandene Schutz unterhöhlt werden kann.

SYS.3.3.M11 Ausfallvorsorge bei Mobiltelefonen [Benutzer]

Ein Mobiltelefon kann aus verschiedenen Gründen ausfallen oder in seiner Funktionsfähigkeit gestört sein. Dies ist natürlich besonders ärgerlich, wenn es dringend benötigt wird oder dadurch wichtige Daten verloren gehen. Daher sollten von vornherein entsprechende Vorkehrungen getroffen werden, um einem Ausfall vorzubeugen bzw. die Probleme zu minimieren.

Der Ladezustand und die Funktionsfähigkeit des Mobiltelefon-Akkus sollten regelmäßig überprüft werden (siehe auch SYS.3.3.9).

Alle auf dem Mobiltelefon gespeicherten Daten wie Telefonbucheintragungen, Nachrichten, etc. sollten in regelmäßigen Abständen auf einem anderen Medium gespeichert werden, damit sie im Zweifelsfall rekonstruiert werden können. Hierzu gibt es mehrere Möglichkeiten:

- Die wichtigsten Einstellungen wie PINs und die Konfiguration von Sicherheitsmechanismen sollten schriftlich dokumentiert und entsprechend ihrem Schutzbedarf sicher aufbewahrt werden
- Alle Daten, die auf der SIM-Karte gespeichert sind, also z. B. Telefonbücher, können über SIM-Kartenleser und entsprechende Software in einen PC eingelesen und dort verwaltet werden. Dies hat außerdem den Vorteil, dass Adressdaten auf dem PC leichter gepflegt und mit anderen Adressdatenbanken synchronisiert werden können. Insbesondere wenn mehrere Mobiltelefone benutzt werden (siehe auch SYS.3.3.12) ist ein Abgleich der Telefonbücher auf diesem Weg sinnvoll. Wenn nur die Daten auf der SIM-Karte gesichert werden, sind alle Benutzer darauf hinzuweisen, dass sie auch nur dort Rufnummern und Ähnliches speichern sollten. Da diese Methode in der Regel weitere Hardware (den SIM-Kartenleser) benötigt und die Speicherkapazität der SIM-Karte gegenüber dem Telefonspeicher deutlich geringer ist, sollte aber besser der Telefonspeicher für Adressbücher verwendet werden. Diese Variante hat überdies den Vorteil, dass die Kontakt-Daten dabei je nach Modell im vCard-Format vorliegen können, das von vielen verschiedenen IT-Systemen (Mobiltelefonen, Smartphones und PCs) verarbeitet werden kann.
- Das Mobiltelefon kann auch mit einem weiteren IT System, z. B. Notebooks oder Organizern, gekoppelt werden, sodass die zu sichernden Daten auf diesem Weg ausgetauscht werden, falls eine geeignete Synchronisations-Software für das gewählte Mobiltelefon existiert (siehe auch SYS.3.3.M10). Dabei können sowohl die auf der SIM-Karte als auch die im Gerät gespeicherten Daten gesichert werden.

Wenn ein Mobiltelefon kontinuierlich verfügbar sein soll, sollte ein Ersatz-Mobiltelefon oder aber ein Ersatz-Akku (wenn möglich), mitgeführt werden.

Wenn Mobiltelefone im Rahmen von Alarmierungen eingesetzt werden, also wenn z. B. die Einbruchmeldeanlage Alarmmeldungen über GSM absetzt oder Notfallpersonal über Mobiltelefone benachrichtigt werden soll, sollte immer eine Ausweichmöglichkeit vorgesehen sein.

Reparatur

Bei Defekten des Mobiltelefons oder einzelner Komponenten sollten Reparaturen nur von vertrauenswürdigen Fachbetrieben durchgeführt werden. Daher sollte eine Übersicht über entsprechende Fachbetriebe vorhanden sein.

Viele Händler bieten auch für die Dauer der Reparatur Ersatzgeräte an. Bei schnelllebigen Geräten wie Mobiltelefonen lohnt sich eine Reparatur häufig nicht, sodass auch manchmal ein Tauschgerät angeboten wird. Da gerade ein Mobiltelefon kontinuierlich zur Verfügung stehen sollte, ist bei der Auswahl des Mobiltelefons bzw. des Händlers darauf zu achten, dass solche Dienstleistungen angeboten werden.

Bevor das Mobiltelefon zur Reparatur gegeben wird, sollten alle personenbezogenen Daten, also z. B. der Anrufspeicher, gespeicherte E-Mails und das Telefonbuch im Gerät gelöscht werden, soweit das noch möglich ist. Vorher sollten sie selbstverständlich gesichert werden. Außerdem sollten die SIM-Karte und ggf. entnehmbare Speicherkarten entfernt werden. Bei vielen Mobiltelefon-Modellen empfiehlt es sich, einen dort möglichen Firmware-Reset durchzuführen.

SYS.3.3.M12 Einrichtung eines Mobiltelefon-Pools

Werden in einer Institution eine Vielzahl von Mobiltelefonen eingesetzt und wechseln die Benutzer häufig, kann es angebracht sein, die zeitweise nicht genutzten Mobiltelefone in einer Sammelaufbewahrung (Pool) zu halten.

Für alle Mobiltelefone ist die Stromversorgung sicherzustellen, damit die Akkus dieser Geräte den sofortigen Einsatz erlauben. Dabei ist zu beachten, dass sich ein Akku im Laufe der Zeit entlädt, auch wenn er nicht verwendet wird. Wenn die Mobiltelefone häufiger über längere Zeiträume eingesetzt werden, sollten zusätzlich Ersatzakkus vorrätig gehalten werden, insofern die Akkus austauschbar sind.

Hinweis: Die Ladegeräte sollten den Mobiltelefonen eindeutig und leicht erkennbar zugeordnet werden. Die Ladegeräte sehen sich zwar alle sehr ähnlich, sind aber leider meist nicht austauschbar. Ferner sollten auch die zugehörigen Datenkabel eindeutig den jeweiligen Mobiltelefonen zugeordnet und gemeinsam mit dem Ladegerät aufbewahrt werden.

Zusätzlich sollte die Rücknahme und die Ausgabe von Mobiltelefonen dokumentiert werden, sodass jederzeit nachvollziehbar ist, wer welche Geräte einsetzt bzw. zu einer bestimmten Zeit eingesetzt hat. Jeder Benutzer sollte mit Namen, Organisationseinheit, Datum und Uhrzeit in das Übergabejournal eingetragen werden.

Bei der Übergabe und Rücknahme von Mobiltelefonen sind außerdem folgende Punkte zu beachten:

Übergabe:

- Der neue Benutzer erhält alle benötigten PINs und Passwörter für die Nutzung des Mobiltelefons. Wenn diese auf selbst gewählte Werte geändert werden, sollten die neuen Werte bei der Rückgabe dokumentiert werden.
- Außerdem erhält er die Rufnummer des Mobiltelefons.
- Es sollten alle vom neuen Benutzer benötigten Telefonnummern und gegebenenfalls Programme aufgespielt werden. Ebenso sollten alle Konfigurationseinstellungen vorgenommen werden.
- Dem neuen Benutzer wird ein Merkblatt für den sicheren Umgang mit dem Mobiltelefon übergeben. Der Benutzer sollte außerdem die Bedienungsanleitung des Mobiltelefons bekommen. Neben der normalen Bedienung seines Telefons sollte der Benutzer vor allem in der Lage sein, etwaige Warnanzeigen (wie Piktogramme im Display) zu interpretieren.
- Das Mobiltelefon sollte geladen und zusammen mit dem passenden Ladegerät und falls vorhanden dem Datenkabel übergeben werden. Wenn das Mobiltelefon über längere Zeitspannen einsetzbar sein soll, sollte ein geladener Ersatzakku mit übergeben werden.

Rücknahme bzw. Weitergabe:

- Der Benutzer gibt die zuletzt benutzten PINs und Passwörter bekannt. Es sollte überprüft werden, ob diese korrekt sind. Sie sollten notiert (und sicher verwahrt) werden.
- Der Benutzer sollte das Mobiltelefon vollständig, mit allem Zubehör sowie der Dokumentation zurückgeben. Dies ist zu kontrollieren. Das Gerät sollte zudem auf Defekte, Schadsoftware und gegebenenfalls auch auf Manipulationen der Hardware überprüft werden. Um eventuelle Hardwaremanipulationen aufzudecken, kann das Gewicht des Mobiltelefons bei Rückgabe mit dem Gewicht bei der Übergabe zu verglichen werden. Haben Angreifer das Endgerät mit einem Abhörmikrofon präpariert, so ist es in der Regel messbar schwerer.
- Der Benutzer sollte sicherstellen, dass vor Rückgabe des Gerätes sämtliche Daten (SMS, Fax, E-Mail, Telefonnummern oder sonstige Daten), die der Benutzer noch benötigt, auf ihm zugängliche Datenträger (z.B. seinen PC) übertragen werden.
- Das Gerät sollte komplett auf den Werkszustand zurückgesetzt und alle Daten vom Endgerät und von der Speicher- und SIM-Karte gelöscht werden. Nur so wird wirkungsvoll der Befall durch Schadsoftware und ein unbewusster Datenabfluss vermieden. Danach können wieder alle benötigten Programme und Daten auf das Gerät aufgespielt werden.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

SYS.3.3.M13 Schutz vor Erstellung von Bewegungsprofilen bei der Mobilfunk-Nutzung [Benutzer] (C)

Bei der Mobil-Kommunikation sollten die mobilen Kommunikationspartner aus technischen Gründen geortet werden können, um erreichbar zu sein. Sofern sie selbst eine Verbindung aufbauen, geben sie ebenfalls im Zuge des Verbindungsaufbaus Informationen über ihren Standort ab. Diese Standortinformationen könnten durch den Netz- oder Dienstbetreiber, aber eventuell auch von Dritten, zur Bildung personen- oder gerätebezogener "Bewegungsprofile" verwendet werden.

Bei modernen Mobiltelefonen besitzen gegebenenfalls einige Applikationen Zugriff auf das Internet und den eingebauten GPS-Empfänger und geben Standortinformationen weiter, mit denen Dritte ebenfalls Bewegungsprofile erstellen können. Applikationen, die diese Rechte aus nicht funktionsbezogenen Gründen anfordern, sollten nicht installiert werden. Bei allen anderen Applikationen sollte zwischen der Gefahr, Bewegungsprofile zu ermöglichen, und dem Nutzen der Applikation abgewogen werden.

Werden Bewegungsprofile als Gefährdung angesehen, dann sollten, falls umsetzbar, die Mobiltelefone und auch die SIM-Karten häufiger unter den Mitarbeitern getauscht werden. So wird eine Zuordnung der Geräte und Karten zu einem bestimmten Nutzer zumindest erschwert. Lokalisierungen über das Radio Resource Location Protocol (RRLP) können damit jedoch nicht abgewehrt werden, da hierbei sowohl die Telefonnummer als auch die International Mobile Equipment Identity (IMEI) ermittelt wird.

Soll der Aufenthaltsort zu bestimmten Zeiten unentdeckt bleiben, hilft nur ein Ausschalten des Mobiltelefons. Um ganz sicher zu sein, sollte der Akku entfernt werden.

SYS.3.3.M14 Schutz vor Rufnummernermittlung bei der Mobiltelefon-Nutzung [Benutzer] (C)

Im Mobilfunknetz werden in der Regel den beteiligten Kommunikationspartnern die jeweiligen Rufnummern angezeigt. Ob dies tatsächlich geschieht, hängt von der technischen Ausstattung und der Konfiguration seitens der Mobiltelefone bzw. der Netzbetreiber bzw. Mobilfunkanbieter ab.

Am Mobiltelefon kann mit der Funktion Rufnummernunterdrückung (für den nächsten bzw. alle weiteren Anrufe) verhindert werden, dass die eigene Rufnummer im Display des Angerufenen angezeigt wird. Diese Option ist in den Menüs der Mobiltelefone oft unter Bezeichnungen wie Inkognito oder Anonym zu finden. Beim SMS-Versand mit einem Mobiltelefon ist eine Rufnummernunterdrückung in der Regel nicht möglich. Das Verhalten der Voice-Mailbox sollte im Einzelfall verifiziert werden, ebenso wie das Gesamtverhalten von Rufnummernunterdrückungs-Aktionen im Ausland.

Die Rufnummernunterdrückung kann bei Geräten, die den GSM-Standard unterstützen, mit folgenden GSM-Codes für den nächsten Anruf gesteuert werden:

- Eigene Rufnummer zeigen *31#Rufnummer
- Eigene Rufnummer nicht zeigen #31#Rufnummer

Über den Netzbetreiber kann auch kontinuierlich eine Rufnummernunterdrückung aktiviert werden.

Einen gewissen Schutz gegen die Zuordnung von Rufnummern zu bestimmten Personen gewährt der Austausch von Mobiltelefonen und SIM-Karten. Damit ist keine dauerhafte Zuordnung zwischen Benutzer und Rufnummer bzw. Gerät und Nutzer möglich. Die Zuordnung z. B. zu einer Behörde oder einer bleibt aber bestehen.

Außer über die Signalisierung der Rufnummer kann die Mobiltelefonnummer einer bestimmten Person auch über öffentliche Telefonbücher ermittelt werden, wenn sie dort eingetragen ist. Beim Abschluss eines Mobilfunkvertrages sollte daher genau überlegt werden, ob bzw. in welcher Form eine Eintragung in öffentliche Telefonbücher sinnvoll ist. Auch in internen Telefonbüchern und bei einzelnen Datenabfragen (Formulare, Gewinnspiele, etc.) sollten Mobiltelefonnummern nicht gedankenlos preisgegeben werden.

SYS.3.3.M15 Schutz vor Abhören der Raumgespräche über Mobiltelefone (C)

Wer sicher ausschließen will, dass Raumgespräche über Mobiltelefone abgehört werden, sollte dafür sorgen, dass kein Mobiltelefon in den zu schützenden Raum mitgenommen wird. Wenn die Sicherheitsleitlinie einer Institution es nicht zulässt, dass Mobiltelefone mitgebracht werden, sollte an allen Eingängen deutlich darauf hingewiesen werden. Ohne entsprechende Kontrollen ist ein einfacher Hinweis aber meist wirkungslos.

Es reicht als Schutz nicht aus, Mobiltelefone einfach auszuschalten bzw. in den Standby oder Flugmodus zu bringen. Sofern sie entsprechend manipuliert sind, können sie über Funk unbemerkt eingeschaltet werden.

Mobiltelefon-Detektoren

Mobiltelefon-Detektoren sind Geräte, die erkennen, wenn in einem abgegrenzten Bereich ein oder mehrere Mobiltelefone in den Sendebetrieb (Gesprächsverbindungsaufbau) gehen.

Es gibt aktive und passive Detektoren. Passive Warngeräte melden Mobiltelefone, die sich im Sendebetrieb befinden. Der Wirkungsbereich der Geräte kann so eingestellt werden, dass er auf den zu überwachenden Bereich beschränkt ist. Es wird empfohlen, bei einem entsprechenden Schutzbedarf solche Warngeräte zu installieren und diese bei Gesprächen mit vertraulichem Inhalt zu aktivieren. Moderne Mobiltelefone benötigen allerdings zum Abhören keine stehende Funkverbindung, sondern können das Gespräch aufzeichnen und die Sounddatei mit Verzögerung über das Mobilfunknetz übertragen. Daher schützen passive Mobiltelefon-Detektoren nur bedingt davor, dass Raumgespräche abgehört werden.

Um auch Mobiltelefone zu erkennen, die im Ruhebetrieb (Standby) sind, wäre ein aktiver Sendeteil für den Detektor notwendig. Mithilfe dieses Sendeteils kann das Mobiltelefon dazu gebracht werden, in den Sendebetrieb zu gehen. Danach kann es dann mit einem Detektor erkannt werden. Mithilfe dieser aktiven Detektoren lassen sich so alle eingeschalteten Mobiltelefone detektieren. Später eingeschaltete Geräte sollten sich bei der Basisstation anmelden und können bei diesem Einbuchungsvorgang ebenfalls detektiert werden. Die Störsender können auch so eingesetzt werden, dass sie in einem räumlich abgegrenzten Bereich den Funkbetrieb derart stören, dass dort kein Mobilfunkempfang möglich ist.

Derzeit können aber nur passive Mobiltelefon-Detektoren empfohlen werden. Aktive Detektoren sind zwar ebenfalls sinnvoll, sie besitzen jedoch keine Betriebsgenehmigung für Deutschland. Auch Sender, die den Mobilfunkbetrieb stören, sind in Deutschland nicht zugelassen. Mobiltelefone können auch als Diktiergeräte genutzt werden. Lautlos und in den Flugmodus geschaltete Geräte können problemlos Besprechungen aufzeichnen, selbst aktive Mobiltelefon-Detektoren sind dann keine geeignete Gegenmaßnahme.

3 Weiterführende Informationen

3.1 Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz gerne unter entgegen.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Mobiltelefon" finden sich unter anderem in folgenden Veröffentlichungen:

[TDSV] Telekommunikationsdienstunternehmen-Datenschutzverordnung - Verordnung über den Datenschutz für Institutionen

https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/Meldepflicht/Meldeformular_pdf.pdf

und https://dsgvo-gesetz.de , beide zuletzt abgerufen am 20.04.2018

SYS.3: Mobile Devices

Umsetzungshinweise zum Baustein SYS.3.4 Mobile Datenträger

1 Beschreibung

1.1 Einleitung

Mobile Datenträger werden für viele unterschiedliche Zwecke eingesetzt, beispielsweise für den Datentransport, die Speicherung von Daten oder die Datennutzung unterwegs. Es gibt zahlreiche verschiedene Varianten von mobilen Datenträgern, hierzu gehören unter anderem Wechselplatten, CD-ROMs, DVDs, Magnetbänder, USB-Festplatten und USB-Sticks. Durch diese vielfältigen Formen und Einsatzgebiete werden nicht immer alle erforderlichen Sicherheitsbetrachtungen vorgenommen.

Datenträger können danach klassifiziert werden, ob sie nur lesbar, einmalig beschreibbar oder wiederbeschreibbar sind. Sie können auch nach weiteren Kriterien unterteilt werden, beispielsweise

- nach der Art der Datenspeicherung: analoge oder digitale Datenträger,wie sie bearbeitet werden können: ohne technische Hilfsmittel, wie z. B. Papier, oder nur mit technischen Hilfsmitteln, wie z. B. DVDs, nach ihrer Bauform: auswechselbare Datenträger, externe Datenspeicher oder Datenträger, die in andere Geräte integriert sind.
- wie sie bearbeitet werden können: ohne technische Hilfsmittel, wie z. B. Papier, oder nur mit technischen Hilfsmitteln, wie z. B. DVDs, nach ihrer Bauform: auswechselbare Datenträger, externe Datenspeicher oder Datenträger, die in andere Geräte integriert sind.
- nach ihrer Bauform: auswechselbare Datenträger, externe Datenspeicher oder Datenträger, die in andere Geräte integriert sind.

Auswechselbare Datenträger, teilweise auch als Wechselmedien bezeichnet, werden in ein Laufwerk eingelegt. Beispiele hierfür sind CD-ROMs, DVDs, Blu-ray Discs, Magnetbänder und Speicherkarten. Externe Datenspeicher, wie beispielsweise USB-Sticks und externe Festplatten, können hingegen direkt an ein IT-System angeschlossen werden. Beispiele für Datenträger, die in anderen Geräten integriert sind, sind die Speicherkomponenten in Smartphones, Tablets und Digitalkameras.

Neben den digitalen Datenträgern sind auch Informationen auf Papier oder anderen analogen Datenträgern bei der Sicherheitskonzeption zu berücksichtigen. Dies betrifft beispielsweise Ausdrucke und Kopien sowie die Nutzung von Fax-Diensten. Weitere Hinweise hierzu finden sich in den Bausteinen SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte und NET.4.3 Faxgerät.

In diesen Umsetzungshinweisen wird einerseits aufgezeigt, wie die auf mobilen Datenträgern gespeicherten Informationen sicher genutzt werden können und andererseits wie einer unbefugten Weitergabe von Informationen über mobile Datenträger vorgebeugt werden sollte.

1.2 Lebenszyklus

Für den sicheren Umgang mit mobilen Datenträgern sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung und Konzeption über die Beschaffung bis hin zur Notfallvorsorge. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Planung und Konzeption

Es sollte ein Konzept für den sicheren Umgang mit mobilen Datenträgern erstellt werden, in dem für die verschiedenen Arten von mobilen Datenträgern Risiken und Sicherheitsmaßnahmen aufgezeigt werden (siehe SYS.3.4.M4 Erstellung einer Richtlinie zum sicheren Umgang mit mobilen Datenträgern).

Beschaffung

Die Auswahl geeigneter Datenträger ist abzustimmen. Für die Entscheidung, welche Arten von Datenträgern eingesetzt werden, kann zudem OPS.1.2.2 Archivierung berücksichtigt werden.

Betrieb

Basierend auf den jeweiligen Sicherheitsanforderungen sollten anhand von Einsatzszenarien Sicherheitshinweise für alle Mitarbeiter erstellt werden (siehe SYS.3.4.M1 Sensibilisierung der Mitarbeiter zum sicheren Umgang mit mobilen Datenträgern). Außerdem müssen die Laufwerke und Schnittstellen der IT-Systeme gemäß den Sicherheitsvorgaben geschützt werden (siehe SYS.3.4.M8 Absicherung von Laufwerken und Schnittstellen für Wechselmedien und externe Datenspeicher).

Aussonderung

Wenn Datenträger weitergegeben werden, sollten sie vor ihrer erneuten Verwendung oder Aussonderung physikalisch gelöscht werden, damit keine schützenswerten Informationen in die falschen Hände geraten (siehe SYS.3.4.M7 Physikalisches Löschen der Datenträger vor und nach Verwendung).

Notfallvorsorge

Wichtige Informationen, die auf mobilen Datenträgern gespeichert sind, sollten noch an einer anderen Stelle gespeichert sein, um einem Verlust vorzubeugen (siehe SYS.3.4.M3 Sicherungskopie der übermittelten Daten).

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Mobile Datenträger" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

SYS.3.4.M1 Sensibilisierung der Mitarbeiter zum sicheren Umgang mit mobilen Datenträgern

In Behörden und Unternehmen werden heute die verschiedensten Arten von mobilen Datenträgern eingesetzt. Ebenso nimmt die Zahl von Geräten zu, die neben ihrer eigentlichen Funktion zusätzlich als mobile Datenträger einsetzbar sind. Damit steigt sowohl die Zahl möglicher Verbreitungswege für Informationen als auch die Zahl möglicher Sicherheitslücken. Einige dieser Sicherheitsrisiken lassen sich zwar technisch minimieren, aber ohne eine Einbeziehung der Mitarbeiter in den sicheren und sachgerechten Umgang mit mobilen Datenträgern werden Behörden oder Unternehmen immer wieder von technischen Neuerungen überrollt.

Alle Mitarbeiter müssen über die Arten und Einsatzmöglichkeiten von mobilen Datenträgern aufgeklärt werden. Dazu gehört auch, sie über die verschiedenen Bauformen und Varianten zu informieren, also dass beispielsweise auch ein Smartphone ein mobiler Datenträger ist. Außerdem sollten die Mitarbeiter über potenzielle Risiken und Probleme bei der Nutzung informiert sowie über den Nutzen, aber auch die Grenzen der eingesetzten Sicherheitsmaßnahmen aufgeklärt werden. Die Mitarbeiter sind zudem regelmäßig über neue Gefahren und Aspekte von mobilen Datenträgern zu unterrichten, z. B. über entsprechende Artikel im Intranet oder in der Mitarbeiterzeitschrift.

Die Benutzer müssen darauf hingewiesen werden, wie sie sorgfältig mit den mobilen Datenträgern umgehen sollten, um einem Verlust oder Diebstahl vorzubeugen bzw. um eine lange Lebensdauer zu gewährleisten. Dabei sollten beispielsweise Fragen zur Aufbewahrung außerhalb von Büro- oder Wohnräumen sowie zur Empfindlichkeit gegenüber zu hohen oder zu niedrigen Temperaturen behandelt werden. Beschädigungen oder Verluste sind zeitnah zu melden (siehe SYS.3.4.M2 Verlustmeldung mobiler Datenträger).

Weitere Aspekte, auf die die Benutzer hingewiesen werden sollten, sind:

- welche Daten auf mobilen Datenträgern gespeichert werden dürfen und welche nicht,
- wie die auf diesen mobilen Datenträgern gespeicherten Daten vor unbefugtem Zugriff, Manipulation und Verlust geschützt werden,
- wie Daten auf mobilen Datenträgern sicher gelöscht werden können und wie Datenträger zu entsorgen sind.

SYS.3.4.M2 Verlustmeldung mobiler Datenträger [Benutzer]

Verlust oder Diebstahl eines dienstlich genutzten mobilen Datenträgers muss umgehend gemeldet werden. Das gilt auch für private Datenträger, die dienstlich genutzt werden. Hierfür muss es in jeder Institution klare Meldewege und Ansprechpartner geben.

Ausfälle oder Defekte sollten ebenfalls gemeldet werden, auch bei geringpreisigen mobilen Datenträgern, damit das IT-Management erkennen kann, ob hiervon größere Lieferungen betroffen sind. Insbesondere bei Datenträgern, die für Datensicherungen und Archivierung eingesetzt werden, ist eine hohe Verlässlichkeit und eine lange Lebensdauer wichtig. Verliert ein Mitarbeiter einen mobilen Datenträger oder wird er gestohlen, muss wiederum schnell gehandelt werden, da es hier nicht nur darum geht, das Gerät wiederzubeschaffen, sondern auch darum, potenziellen Missbrauch der betroffenen Informationen zu verhindern.

Wenn verlorene Datenträger wieder auftauchen, wird dringend empfohlen, sie auf eventuelle Manipulationen zu untersuchen, z. B. ob Schrauben geöffnet, Siegel entfernt wurden oder sich das Gewicht gegenüber dem Auslieferungszustand geändert hat. Besteht ein Verdacht, sollte das Gerät entweder gleich entsorgt oder von einem Spezialisten weiter untersucht werden. Um sicherzustellen, dass sich keine manipulierten Programme oder Schadsoftware auf den wiedererlangten Datenträgern befinden, sollte die Anforderung SYS.3.4.M7 Physikalisches Löschen der Datenträger vor und nach der Verwendung umgesetzt werden.

Sollen Datenträger entsorgt werden, sollte vorher sichergestellt werden, dass die auf den Datenträgern abgespeicherten Restinformationen nicht in falsche Hände gelangen können. Hierzu sollte er sicher gelöscht werden (SYS.3.4.M7 Physikalisches Löschen der Datenträger vor und nach der Verwendung), generell sollten die Anforderungen des Bausteins OPS.1.2.7 Verkauf/Aussonderung von IT umgesetzt werden.

SYS.3.4.M3 Sicherungskopie der übermittelten Daten [Benutzer]

Sind die zu übertragenden Daten nur zum Zweck der Datenübertragung erstellt bzw. zusammengestellt worden und nicht auf einem weiteren Medium gespeichert, muss eine Sicherungskopie dieser Daten vorgehalten werden. Kommt der mobile Datenträger abhanden oder wird beschädigt, gehen die Daten somit nicht verloren.

Gemeinsam mit den Basismaßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Mobile Datenträger".

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Mobile Datenträger".

SYS.3.4.M4 Erstellung einer Richtlinie zum sicheren Umgang mit mobilen Datenträgern [Benutzer]

Über mobile Datenträger können je nach technischer Auslegung eine große Menge an Daten bei hohen Durchsatzraten ausgetauscht werden. Die Varianten von mobilen Datenträgern sind mittlerweile vielfältig. Auch sind sie nicht immer auf den ersten Blick als solche zu erkennen. So gibt es beispielsweise Armbanduhren oder Schlüsselanhänger mit integriertem Datenspeicher. Die gängige Größe dieser Datenträger beginnt hier bei einigen hundert Megabyte und kann durchaus bis zu mehreren Terabyte reichen.

Daher sollten für den Umgang mit mobilen Datenträgern einige grundlegende Aspekte berücksichtigt werden. Es ist zu klären,

- welche mobilen Datenträger in der Institution genutzt werden sollen,
- welche tatsächlich genutzt werden und wer diese einsetzt,
- welche Daten auf mobilen Datenträgern gespeichert werden dürfen und welche nicht,
- wie die auf diesen mobilen Datenträgern gespeicherten Daten vor unbefugtem Zugriff, Manipulation und Verlust geschützt werden,
- mit welchen externen Mitarbeitern oder Dienstleistern mobile Datenträger ausgetauscht werden dürfen und welche Sicherheitsregelungen dabei zu beachten sind (siehe hierzu OPS.1.2.3 Datenträgeraustausch),
- wie verhindert wird, dass mobile Datenträger dazu benutzt werden, unbefugt Informationen weiterzugeben,
- wie gegen die Verbreitung von Schadsoftware über die mobilen Datenträger vorgebeugt wird.

Es sollte außerdem geklärt werden, ob Mitarbeiter ihre privaten mobilen Datenträger innerhalb der Institution nutzen dürfen, und auch umgekehrt, ob Mitarbeiter private Daten auf dienstlichen mobilen Datenträgern speichern oder nutzen dürfen. Ebenso ist zu klären, ob die von Externen mitgebrachten mobilen Datenträger innerhalb der Institution eingesetzt werden dürfen, beispielsweise um Dateien auszutauschen.

Je restriktiver die Sicherheitsvorgaben für den Umgang mit mobilen Datenträgern sind, desto höher sind auch die Einschränkungen im Arbeitsalltag. Daher sollten alle Sicherheitsvorgaben daraufhin abgewogen werden, ob sie angemessen sind.

Die Vielzahl und Varianten von Datenträgern werden weiter zunehmen. Mobile Datenträger werden zunehmend "unsichtbar", da sie in anderen Geräten integriert werden. Es sollte regelmäßig überprüft werden, ob die Sicherheitsvorgaben für den Umgang mit mobilen Datenträgern noch aktuell sind, angefangen damit, ob alle Varianten von derzeit gebräuchlichen Datenträgern noch erfasst sind.

Mobile Datenträger können leicht unterwegs verloren oder gestohlen werden. Deswegen ist je nach Schutzbedarf zu überlegen, ob die darauf gespeicherten Informationen verschlüsselt werden sollten. Hierfür sollten Produkte eingesetzt werden, die automatisch alle Daten verschlüsseln, die Benutzer auf mobilen Datenträgern speichern. Weitere Hinweise hierzu finden sich in SYS.3.4.M10 Datenträgerverschlüsselung.

Die von der Institution festgelegte Vorgehensweise sollte dokumentiert und in einer Sicherheitsrichtlinie für die Mitarbeiter aufbereitet werden.

SYS.3.4.M5 Regelung der Mitnahme von mobilen Datenträgern

Die IT-Komponenten, die innerhalb einer hauseigenen Liegenschaft eingesetzt werden, sind im Allgemeinen durch infrastrukturelle Sicherheitsmaßnahmen ausreichend vor Missbrauch und Diebstahl geschützt. Mobile Datenträger werden jedoch oft außer Haus eingesetzt, z. B. bei Dienstreisen. Um diese ausreichend schützen zu können, muss die Mitnahme solcher Datenträger klar geregelt werden.

Dabei sollte festgelegt werden,

- welche mobilen Datenträger außer Haus mitgenommen werden dürfen,
- wer mobile Datenträger außer Haus mitnehmen darf und
- welche grundlegenden Sicherheitsmaßnahmen dabei beachtet werden müssen (Virenschutz, Verschlüsselung schützenswerter Daten, Aufbewahrung etc.).

Die Art und der Umfang der anzuwendenden Sicherheitsmaßnahmen für extern eingesetzte Datenträger hängen einerseits vom Schutzbedarf der darauf gespeicherten IT-Anwendungen und Daten und andererseits von der Sicherheit der Einsatz- bzw. Aufbewahrungsorte ab.

Grundsätzlich sollten Mitarbeiter für alle mobilen Datenträger, die sie extern einsetzen wollen, eine entsprechende Genehmigung einholen. Insbesondere außerhalb der institutionseigenen Liegenschaften sollten die Benutzer für den Schutz der ihnen anvertrauten Datenträger sorgen. Darauf und auf die zu ergreifenden Vorsichtsmaßnahmen sind sie hinzuweisen. Dazu gehören folgende Regeln:

- Mobile Datenträger müssen stets sicher aufbewahrt werden. Bei Dienstreisen sollten sie nicht unbeaufsichtigt gelassen werden.
- Mobile Datenträger, die schützenswerte Daten enthalten, sollten möglichst komplett verschlüsselt werden (SYS.3.4.M10 Datenträgerverschlüsselung). Wenn solche Datenträger eine Verschlüsselungsfunktion ohne weitere Hilfsmittel ermöglichen, ist es empfehlenswert, diese Funktionen auch dann zu nutzen, wenn weniger schützenswerte Daten auf dem Datenträger enthalten sind.
- Die Verwaltung, Wartung und Weitergabe von extern eingesetzten mobilen Datenträgern sollte geregelt werden. Hierzu können beispielsweise Pools eingerichtet werden.
- Es sollte notiert werden, wann und von wem welche Datenträger außer Haus eingesetzt wurden.

SYS.3.4.M6 Datenträgerverwaltung [Fachverantwortliche]

Aufgabe der Datenträgerverwaltung als Teil der Betriebsmittelverwaltung ist es, den Zugriff auf mobile Datenträger im erforderlichen Umfang und in angemessener Zeit gewährleisten zu können. Dies erfordert eine geregelte Verwaltung der Datenträger, die eine einheitliche Kennzeichnung sowie eine Führung von Bestandsverzeichnissen erforderlich macht. Weiterhin ist im Rahmen der Datenträgerverwaltung die sachgerechte Behandlung und Aufbewahrung der Datenträger, deren ordnungsgemäßer Einsatz und Transport und schließlich auch noch die Löschung bzw. Vernichtung der Datenträger zu gewährleisten.

Bestandsverzeichnisse ermöglichen einen schnellen und zielgerichteten Zugriff auf mobile Datenträger. Sie geben beispielsweise Auskunft über Aufbewahrungsort, Aufbewahrungsdauer und berechtigte Empfänger.

Die äußerliche **Kennzeichnung** von mobilen Datenträgern ermöglicht deren schnelle Identifizierung. Die Kennzeichnung sollte jedoch für Unbefugte keinen Rückschluss auf den Inhalt erlauben (z. B. die Beschriftung eines USB-Sticks mit dem Stichwort "vertraulich"), um einen Missbrauch zu erschweren. Es sollte aber beachtet werden, dass flankierende Regelungen und Vorgaben, die für die Institution gelten, eine entsprechende Kennzeichnung fordern. In diesem Fall müssen in der Regel ergänzende Anforderungen aus diesen Regelungen und Vorgaben umgesetzt werden. Eine festgelegte Struktur von Kennzeichnungsmerkmalen (z. B. Datum, Ablagestruktur, lfd. Nummer) erleichtert die Zuordnung in Bestandsverzeichnissen.

Für eine **sachgerechte Behandlung** von mobilen Datenträgern sind die Herstellerangaben, die üblicherweise auf der Verpackung zu finden sind, heranzuziehen. Hinsichtlich der Aufbewahrung von Datenträgern sind einerseits Maßnahmen zur Lagerung (magnetfeld- und staubgeschützt, klimagerecht) und andererseits Maßnahmen zur Verhinderung des unbefugten Zugriffs (geeignete Behältnisse, Schränke, Räume) zu treffen.

Der **Versand oder Transport** von mobilen Datenträgern muss so erfolgen, dass sie möglichst nicht beschädigt werden können (z. B. Magnetbandversandtasche, luftgepolsterte Umschläge). Die Verpackung des Datenträgers ist an seiner Schutzbedürftigkeit auszurichten (z. B. mittels verschließbaren Transportbehältnissen). Versand- oder Transportarten (z. B. Kuriertransport) müssen ebenso festgelegt werden wie das Nachweisverfahren über den Versand (z. B. Begleitzettel, Versandscheine) und den Eingang beim Empfänger (z. B. Empfangsbestätigung). Der Datenträger darf über die zu versendenden Daten hinaus, keine "Restdaten" enthalten. Dies kann durch physikalisches Löschen erreicht werden.

Weiterhin ist zu beachten, dass bevor wichtige Datenträger abgegeben werden, eine Sicherungskopie erstellt wird. Weitere Ausführungen zum Versand und Transport von Datenträgern enthält der Baustein OPS.1.2.3 Datenträgeraustausch.

Für die interne Weitergabe von Datenträger können Regelungen getroffen werden wie Quittungsverfahren, Abhol-/Mitnahmeberechtigungen sowie das Führen von Bestandsverzeichnissen über den Verbleib der Datenträger.

Für den Fall, dass **von Dritten erhaltene Datenträger** eingesetzt werden, sind Regelungen über deren Behandlung vor dem Einsatz zu treffen. Werden zum Beispiel digitale Daten übermittelt, sollte generell ein Computer-Viren-Check des mobilen Datenträgers bzw. der Datensätze erfolgen. Dies gilt entsprechend auch vor dem erstmaligen Einsatz neuer digitaler Datenträger. Es ist empfehlenswert, nicht nur beim Empfang, sondern auch vor dem Versenden von digitalen Datenträgern diese auf Computer-Viren zu überprüfen.

Eine geregelte Vorgehensweise für die Löschung oder Vernichtung von Datenträgern verhindert den Missbrauch der gespeicherten Daten. Bevor mobile Datenträger wiederverwendet werden, sind die darauf gespeicherten Daten sicher zu löschen (siehe hierzu OPS.1.1.8 Löschen und Vernichten von Daten).

SYS.3.4.M7 Sicheres Löschen der Datenträger vor und nach der Verwendung [Fachverantwortliche]

Neben den im Baustein OPS.1.1.8 Löschen und Vernichten von Daten enthaltenen Hinweisen zur Löschung oder Vernichtung von Datenträgern, sind für den Datenträgeraustausch folgende Punkte zu beachten:

- Eine für den normalen Schutzbedarf ausreichende physikalische Löschung lässt sich erreichen, indem der komplette Datenträger oder zumindest die genutzten Bereiche mit einem bestimmten Muster überschrieben werden. Möglich ist auch eine Formatierung des Datenträgers, wenn diese nicht wieder rückgängig gemacht werden kann. Es sollte vermieden werden, nur einzelne Dateien zu löschen, hierbei bleiben häufig Restinformationen erhalten, die die Rekonstruktion der gelöschten Dateien ermöglichen.
- Magnetische Datenträger, die für den Austausch bestimmt sind, sollten vor dem Beschreiben mit den zu übermittelnden Informationen physikalisch gelöscht werden. Es soll damit sichergestellt werden, dass keine Restdaten an unberechtigte Empfänger weitergegeben werden.
- In der Regel sind die übertragenen Daten auch für den Empfänger schützenswert. Analog ist auch hier nach dem Wiedereinspielen der Daten eine physikalische Löschung des Datenträgers vorzusehen.
- Auf den Einsatz von nicht-löschbaren Datenträgern ist zum Zwecke des Datenaustausches dann zu verzichten, wenn sich darauf weitere, nicht für den Empfänger bestimmte Informationen befinden, die nicht gelöscht werden können.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

SYS.3.4.M10 Datenträgerverschlüsselung (C)

Vertrauliche Informationen können auf verschiedene Weise verschlüsselt und damit vor unbefugter Kenntnisnahme geschützt werden. So kann beispielsweise der komplette Datenträger, eine einzelne Partition oder nur eine einzelne Datei verschlüsselt werden. Aus Sicherheitssicht ist es besser, den kompletten Datenträger zu verschlüsseln, da dann weniger Benutzereingriffe erforderlich sind und alle Daten vor unbefugtem Zugriff geschützt sind. Werden nur einzelne Dateien oder Dateicontainer verschlüsselt, besteht die Gefahr, dass versehentlich schützenswerte Daten in unverschlüsselten Bereichen der Festplatte abgelegen werden. Zudem muss der Benutzer hierfür explizit ein Verschlüsselungsprogramm starten.

Datenträgerverschlüsselung lässt sich mit Software, aber auch mit Hardware-Unterstützung umsetzen. Software-Lösungen sind z. B. BitLocker von Microsoft oder das Open-Source-Programm VeraCrypt. Mobile Datenträger, wie USB-Sticks, sollten möglichst immer vollständig verschlüsselt werden, auch wenn sie nur gelegentlich für vertrauliche Informationen eingesetzt werden.

Das entscheidende Merkmal eines Verschlüsselungsverfahrens ist die Güte des Algorithmus sowie die Schlüsselauswahl. Ein anerkannter Algorithmus, der für den normalen Schutzbedarf ausreicht, ist der Tripel-DES, der auf dem Data Encryption Standard (DES) basiert. Dieser ist leicht zu programmieren, zumal der Quell-Code in vielen Fachbüchern in der Programmiersprache C abgedruckt ist. Ein anderer anerkannter Algorithmus ist der Advanced Encryption Standard (AES).

Die kryptographischen Schlüssel sollten sicher erzeugt und getrennt vom verschlüsselten mobilen Datenträger aufbewahrt werden (siehe CON.1 Kryptokonzept). Hierfür können beispielsweise Chipkarten oder USB-Token eingesetzt werden. Eine solche Trennung ist bei der Verschlüsselung von USB-Sticks in der Regel nicht möglich, was bei der Sicherheitsanalyse berücksichtigt werden sollte.

Um den Anforderungen der Vertraulichkeit der zu übertragenden Informationen zu entsprechen, sollten die IT-Systeme der Absender und der Empfänger den Zugriffsschutz auf das Verschlüsselungsprogramm ausreichend gewährleisten. Gegebenenfalls sollte dieses Programm auf einem auswechselbaren Datenträger gespeichert, verschlossen aufbewahrt und nur bei Bedarf eingespielt und genutzt werden.

Genutzte Passwörter müssen den Anforderungen hinsichtlich Länge und zu verwendender Zeichen genügen.

SYS.3.4.M11 Integritätsschutz durch Checksummen oder digitale Signaturen (I)

Ist für den Datenaustausch lediglich die Integrität der zu übermittelnden Daten sicherzustellen, muss unterschieden werden, ob ein Schutz nur gegen zufällige Veränderungen, z. B. durch Übertragungsfehler, oder auch gegen Manipulationen geleistet werden soll. Sollen ausschließlich zufällige Veränderungen erkannt werden, können Checksummen-Verfahren (z. B. Cyclic Redundancy Checks) oder fehlerkorrigierende Codes eingesetzt werden. Schutz gegenüber Manipulationen bieten darüber hinaus Verfahren, die mithilfe eines symmetrischen Verschlüsselungsalgorithmus (z. B. Tripel-DES) aus der zu übermittelnden Information einen so genannten Message Authentication Code (MAC) erzeugen. Andere Verfahren bedienen sich eines asymmetrischen Verschlüsselungsalgorithmus (z. B. RSA) in Kombination mit einer Hashfunktion und erzeugen eine "Digitale Signatur". Die jeweiligen erzeugten "Fingerabdrücke" (Checksumme, fehlerkorrigierende Codes, MAC, Digitale Signatur) werden über einen unabhängigen Transportweg mit der Information an den Empfänger übertragen und können von diesem überprüft werden.

3 Weiterführende Informationen

3.1 Wissenswertes

Viele mobile Datenträger haben direkt integrierte Schutzmechanismen. Diese sollten grundsätzlich immer Verwendung finden, um Daten vor unbefugtem Zugriff zu schützen. Mobile Datenträger, wie USB-Sticks mit integrierter Hardware-Verschlüsselung, bieten in der Regel ein deutlich höheres Schutzniveau, als jene, die nur einen Zugriffsschutz verwirklichen, ohne die Daten selbst zu verschlüsseln. Bei allen Verfahren sollte darauf geachtet werden, dass ein Fehlbedienungszähler ein systematisches Durchtesten des Passwortes, der PIN oder eines Fingers verhindert. Bei einem mobilen Datenträger mit Fingerabdruck-Sensor sollte zusätzlich darauf geachtet werden, statt der Fingerkuppen möglichst andere Teile des Fingers zu verwenden, um Angriffe durch Klonen von Fingerabdrücken zu erschweren.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Mobile Datenträger" finden sich unter anderem in folgenden Veröffentlichungen:

[CS008] Schutz von Daten auf USB-Sticks

BSI-Veröffentlichungen zur Cyber-Sicherheit (BSI-CS 008), Version 1.0, Mai 2012, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_008.html, zuletzt abgerufen am 05.10.2018

Umsetzungshinweise zum Baustein SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte

1 Beschreibung

1.1 Einleitung

Zur Grundausstattung in Büros gehören typischerweise Kopierer, Drucker undMultifunktionsgeräte. Sehr häufig ist es aber nicht effizient, jeden einzelnen Arbeitsplatz mit einem Drucker auszustatten. Daher werden oft zentrale Netzdrucker, Kopierer oder Multifunktionsgeräte eingesetzt, auf denen die Mitarbeiter ihre Dokumente ausdrucken oder vervielfältigen können.

Da es einige Nachteile hat, wenn Aufträge vom Arbeitsplatz-PC direkt an einen Netzdrucker verschickt werden, setzen die meisten Institutionen einen zentralen Druckserver ein, der die Aufträge annimmt und auf die verfügbaren Drucker verteilt.

Die Integration der papierverarbeitenden Geräte in ein Netz ist in vielen Fällen nicht nur auf Drucker beschränkt. Netzfähige Dokumentenscanner können beispielsweise für eine Vielzahl von Benutzern bereitgestellt werden, damit diese Papierdokumente digitalisieren können. In Verbindung mit einem Drucker kann ein Scanner beispielsweise wie ein Kopierer betrieben werden.

Als Multifunktionsgeräte werden in diesem Baustein Geräte bezeichnet, die mehrere verschiedene papierverarbeitende Funktionen bieten, etwa Drucken, Kopieren und Scannen oder auch Fax-Dienste. Aus Gründen der Lesbarkeit werden nicht alle Gerätetypen überall einzeln benannt. Da aber beispielsweise für digitale Kopierer ähnliche Sicherheitsempfehlungen wie für Netzdrucker zu beachten sind, gelten für sie die Anforderungen analog.

1.2 Lebenszyklus

Planung und Konzeption

Der Einsatz von Netzdruckern, Kopierern und Multifunktionsgeräten muss sorgfältig geplant werden (siehe SYS.4.1.M1 *Erstellung eines Basis-Konzepts für den Einsatz von Druckern, Kopierern und Multifunktionsgeräten* sowie SYS.4.1.M5 Erstellung eines Sicherheitskonzeptes für den *Einsatz von Druckern und Multifunktionsgeräten*). Im Kapitel 3.1.2 *Verwaltung von Druckern* dieser Umsetzungshinweise sind vertiefende Informationen dazu beschrieben, woraus typische Druckerlandschaften bestehen und wie sie gestaltet sind. Die Sicherheitsanforderungen an Netzdrucker müssen in die allgemeine Sicherheitsstrategie der Institution integriert sein.

Viele Probleme mit Druckern, Kopierern und Multifunktionsgeräten können nicht immer mit technischen Maßnahmen gelöst werden. Die Benutzer müssen über eine sicherheitsbewusste Bedienung der Geräte informiert und hierauf verpflichtet werden (siehe SYS.4.1.M10 *Erstellung von Benutzer- und Administratorenrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten*).

Es sollten auch die speziellen Anforderungen bestimmter Gerätearten berücksichtigt werden. Hierzu gehören beispielsweise Multifunktionsgeräte (siehe SYS.4.1.M9 *Netztrennung beim Einsatz von Druckern und Multifunktionsgeräten*) und Dokumentenscanner (siehe Kapitel 3.1.3 *Einsatz von netzfähigen Dokumentenscannern*).

Beschaffung

Anhand der Einsatzszenarien sind die Anforderungen an die zu beschaffenden Produkte zu formulieren und basierend darauf geeignete Produkte auszuwählen. Wissenswertes dazu ist im Kapitel 3.1.1 *Kriterien für die Beschaffung und geeignete Auswahl von Druckern, Kopierern und Multifunktionsgeräten* zu finden.

Umsetzung

Sind alle Planungsschritte durchlaufen, geht es um die Inbetriebnahme der Geräte. Dabei kommt es auch darauf an, wo die Geräte positioniert werden (siehe SYS.4.1.M3 *Geeignete Aufstellung von Druckern, Kopierern und Multifunktionsgeräten*).

Wie jedes IT-System sollten auch netzfähige Drucker, Kopierer und Multifunktionsgeräte vor unberechtigter Nutzung geschützt werden (siehe SYS.4.1.M13 *Authentisierung und Autorisierung bei Druckern, Kopierern und Multifunktionsgeräten*). Aber auch die Medien, auf denen die (digitalen) Informationen übertragen und abgelegt werden, müssen angemessen abgesichert werden (siehe SYS.4.1.M11 *Verschlüsselung von Informationen Druckern, Kopierern und Multifunktionsgeräten*).

Neben der Druckhardware sind die Softwarekomponenten, wie Druckserver oder -clients, für einen sicheren Betrieb wichtig. In Abhängigkeit vom eingesetzten Betriebssystem und Drucksystem sind entsprechende Anforderungen und Bausteine umzusetzen.

Aussonderung

Sehr oft sind im Speicher der Drucker, Kopierer und Multifunktionsgeräte schutzbedürftige Informationen abgelegt, die geschützt werden müssen (siehe SYS.4.1.M6 *Schutz von Nutz- und Metadaten* berücksichtigt werden.

Notfallvorsorge

Aspekte der Notfallplanung für vernetzte Drucker, Kopierer und Multifunktionsgeräte werden in SYS.4.1.M16 *Notfallvorsorge bei Druckern, Kopierern und Multifunktionsgeräten* thematisiert.

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Drucker, Kopierer und Multifunktionsgeräte" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

SYS.4.1.M1 Erstellung eines Basis-Konzepts für den Einsatz von Druckern, Kopierern und Multifunktionsgeräten [Leiter IT]

Eine grundlegende Voraussetzung für den sicheren Einsatz von Druckern, Kopierern und Multifunktionsgeräten ist eine angemessene Planung im Vorfeld. Der Einsatz der Geräte kann in mehreren Schritten nach dem Prinzip des Top-Down-Entwurfs geplant werden: Ausgehend von einem Grobkonzept für das Gesamtsystem werden konkrete Planungen für Teilkomponenten in spezifischen Teilkonzepten festgelegt (siehe dazu auch *SYS.4.1.M3 Planung des Einsatzes von Druckern, Kopierern und Multifunktionsgeräten*). Im Grobkonzept sollten beispielsweise folgende Schwerpunkte behandelt werden:

- Zunächst muss geregelt werden, wo Drucker, Kopierer und Multifunktionsgeräte aufgestellt werden sollen und wer diese Räume betreten bzw. auf die Geräte zugreifen darf.
- Weiterhin muss geregelt werden, wer welche Zugriffsberechtigungen auf welche Netzgeräte für welche Aufgaben erhält.
- Die Drucker, Kopierer und Multifunktionsgeräte müssen vor Angriffen geschützt werden.
    - Durch entsprechende Maßnahmen sollte physischen Manipulationen entgegengewirkt werden. Werden beispielsweise Schlösser oder Siegel an Wartungszugängen, wie Zugangsklappen angebracht, können unautorisierte Veränderungen erschwert oder zumindest erkannt werden.
    - Ebenso sollten Angriffe über Netze erschwert werden. Hierzu gehören beispielsweise unberechtigte Zugriffe auf Schnittstellen zur Fernadministration über das LAN.
    - Außerdem müssen die elektronischen Informationen geschützt werden, sowohl bei der Übertragung zu den Geräten als auch bei der weiteren Verarbeitung. Beispielsweise sollte überlegt werden, alle Dokumente, die auf den Festplatten der Geräte (eventuell nur temporär) abgespeichert werden, zu verschlüsseln. Alle Entscheidungen, die in der Planungsphase getroffen wurden, müssen so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können. Dabei ist darauf zu achten, dass sie passend strukturiert und verständlich sind.

SYS.4.1.M2 Geeignete Aufstellung und Zugriff auf Drucker, Kopierer und Multifunktionsgeräte

Um zu verhindern, dass Drucker, Kopierern oder Multifunktionsgeräte manipuliert werden oder die Druckausgaben von Unbefugten kopiert oder mitgelesen werden können, müssen die Geräte so aufgestellt werden, dass nur berechtigte Mitarbeiter Zugang zu ihnen haben. Zumindest sollten die Geräte nicht in Bereichen aufgestellt werden, in denen sich häufig externe Personen aufhalten, insbesondere also nicht in der Nähe von Besprechungs-, Veranstaltungs- oder Schulungsräumen. Hiervon ausgenommen sind lediglich solche Geräte, die speziell für diese Bereiche vorgesehen sind, beispielsweise in Schulungsräumen.

Häufig stehen in Druckerräumen auch Kopierer. Aus Sicherheitssicht ist zu hinterfragen, ob hierdurch die Gefahr steigt, dass herumliegende Ausdrucke kopiert werden können. Um solche Probleme zu vermeiden, ist es sinnvoll, Drucker und Kopierer so aufzustellen, dass sie vom eigenen Personal gut eingesehen werden können. Besser ist es jedoch, die Geräte in einem geschlossenen Raum aufzustellen, zu dem nur Berechtigte Zutritt haben. Das ist besonders bei höherem Schutzbedarf zu empfehlen.

Noch besser kann es bei großen Druckern sein, wenn die Ausdrucke durch eine vertrauenswürdige Person in nur für den jeweiligen Empfänger zugängliche Fächer verteilt werden. Druckerausgaben müssen daher mit dem Namen des Empfängers gekennzeichnet sein. Das kann automatisch durch die Druckprogramme erfolgen. Bei hohem Schutzbedarf sollte geprüft werden, ob diese Lösung geeignet ist.

Benutzer stellen häufig erst am Drucker fest, dass sie das falsche Dokument ausgedruckt haben oder dass noch eine Kleinigkeit geändert werden muss. Solche Ausdrucke werden dann häufig direkt beim Drucker in einen offenen Papierkorb geworfen. Da damit auch vertrauliche Dokumente in falsche Hände geraten können, empfiehlt es sich, einen Vernichter direkt neben Netzdruckern aufzustellen. Ersatzweise müssen die Benutzer darauf hingewiesen werden, dass solche Dokumente nicht liegengelassen werden dürfen und anderweitig zu vernichten sind.

SYS.4.1.M3 Regelmäßige Aktualisierung von Druckern, Kopieren und Multifunktionsgeräten

Es muss regelmäßig überprüft werden, ob die Drucker, Kopierer und Multifunktionsgeräte auf dem aktuellen Stand sind. Wenn Sicherheitslücken identifiziert werden, müssen diese so schnell wie möglich behoben werden. Vorhandene Patches und Updates müssen sofort eingespielt werden oder anderweitige Sicherheitsmaßnahmen ergriffen werden, wenn keine Patches zur Verfügung stehen. Generell muss darauf geachtet werden, dass Patches und Updates nur aus vertrauenswürdigen Quellen bezogen werden.

Vertiefende Informationen sind in OPS.1.2.1 Patch- und Änderungsmanagement zu finden.

SYS.4.1.M12 Ordnungsgemäße Entsorgung von Geräten und schützenswerten Betriebsmitteln

Betriebsmittel (z. B. Papier, Festplatten, Flash-Speicher oder -karten, aber auch spezielle Tonerkassetten) werden irgendwann nicht mehr benötigt oder müssen aufgrund von Defekten ausgesondert werden. Wenn sie schützenswerte Daten enthalten, müssen sie so entsorgt werden, dass keine Rückschlüsse auf vorher gespeicherte Daten möglich sind. Bei funktionstüchtigen Datenträgern, die sich in Druckern, Kopierern und Multifunktionsgeräten befinden, sollten die Daten physisch gelöscht werden. Nicht funktionierende Datenträger müssen mechanisch zerstört werden (siehe OPS.1.18 *Löschen und Vernichten*).

Die Art der Entsorgung schutzbedürftigen Materials sollte in einer speziellen Sicherheitsrichtlinie geregelt werden. In der Institution müssen die dafür benötigten Entsorgungseinrichtungen vorhanden sein, z. B. Aktenvernichter.

Wird schutzbedürftiges Material erst gesammelt und dann entsorgt, so ist die Sammlung unter Verschluss zu halten und vor unberechtigtem Zugriff zu schützen.

Soweit sich in der Institution keine umweltgerechte und sichere Entsorgung durchführen lässt, müssen dafür geeignete Dienstleister ausgewählt werden. Damit beauftragte Unternehmen sind darauf zu verpflichten, die erforderlichen Sicherheitsmaßnahmen einzuhalten. Ein Mustervertrag findet sich unter den Hilfsmitteln zum IT-Grundschutz auf den BSI-Webseiten. Es sollte regelmäßig geprüft werden, ob der Entsorgungsvorgang verlässlich ist.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Drucker, Kopierer und Multifunktionsgeräte".

SYS.4.1.M4 Erstellung eines Sicherheitskonzeptes für den Einsatz von Druckern, Kopieren und Multifunktionsgeräten [Leiter IT]

tbd: Anpassung an die Anforderung SYS.4.1.A5 des Bausteins SYS.4.1. Drucker und Multifunktionsgeräte notwendig, Anmerkungen und Vorschläge gerne an die E-Mail-Adresse grundschutz@bsi.bund.de

Die Verantwortlichen sollten ein Sicherheitskonzept für Drucker, Kopierer und Multifunktionsgeräte entwickeln. Darin sollten generell geregelt werden,

- welche Anforderungen an die Informationssicherheit der Geräte zu stellen sind,
- welche Vorgaben schon bei der Beschaffung der Geräte zu erfüllen sind,
- wie auf den Geräten gespeicherte oder damit verarbeitete Informationen technisch geschützt werden,
- wie die Geräte und Druckserver vor unbefugten Änderungen und Angriffen geschützt werden,
- wer damit arbeiten darf,
- welche Funktionen genutzt werden,
- wo Geräte aufgestellt werden dürfen,
- wer Geräte administrieren darf,
- wie der vorgegebene Sicherheitsstandard eingehalten wird und
- wie Benutzer über die Sicherheitsvorgaben informiert, eingewiesen und dazu verpflichtet werden, diese einzuhalten.

Die folgenden Teilkonzepte sollten hierbei bei der Planung des Einsatzes von Druckern, Kopierern und Multifunktionsgeräten berücksichtigt werden:

- Allgemeine Aspekte:
  - **Kauf oder Mieten:** In einigen Fällen kann es sinnvoll sein, die benötigten Geräte nicht zu kaufen, sondern zu mieten. Werden sie gemietet, muss sichergestellt werden, dass eventuell im Speicher abgelegte Dokumente sicher gelöscht werden, damit diese nicht vom nächsten Kunden, der das Gerät mietet, wieder hergestellt werden können. Hierbei muss vorab überprüft werden, ob die Geräte ohne Speicher zurückgegeben werden können oder ob die Speicherbereiche zuverlässig gelöscht werden können, ohne diese physisch zu zerstören.
  - **Lokale oder netzfähige Drucker:** Es ist zu entscheiden, wo lokale und wo netzfähige Drucker eingesetzt werden sollen. Häufig bietet auch eine Zwischenlösung Vorteile: Benutzer, die oft sensible Informationen ausdrucken müssen, erhalten für diese Ausdrucke einen lokalen Drucker. Für die Ausdrucke der restlichen Benutzer oder für Ausdrucke von Informationen mit einem geringeren Schutzbedarf sind bei der Zwischenlösung leistungsfähigere, zentrale Drucker verfügbar.
  - **Druckserver:** Netzdrucker können direkt von den Arbeitsplatzrechnern oder über einen (oder mehrere) Druckserver angesteuert werden. Ein Druckserver nimmt die Druckaufträge von den IT-Systemen an und leitet sie an die gewünschten Drucker weiter. Neben einer zentralen Verwaltung und Protokollierung können die Drucker so effizienter gegen Angriffe geschützt werden, wenn nur noch die Druckserver auf die Netzdrucker zugreifen dürfen. Es ist eine geeignete Lösung auszuwählen.
  - **Richtlinien für die Nutzung:** Um Drucker, Kopierer und Multifunktionsgeräte sicher und effektiv in Institutionen einsetzen zu können, müssen hierfür Sicherheitsvorgaben erstellt werden, die auf den vorhandenen Sicherheitszielen basieren sowie die Anforderungen aus den geplanten Einsatzszenarien einbeziehen. Diese spezifischen Sicherheitsvorgaben müssen mit dem übergreifenden Sicherheitskonzept der Institution abgestimmt sein.
    Darauf aufbauend ist die sichere Nutzung dieser Geräte zu regeln, und es müssen Sicherheitsrichtlinien dafür erarbeitet werden (siehe SYS.4.1.M5 Erstellung von *Benutzerrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten*). Es ist darauf zu achten, dass Drucker, Multifunktionsgeräte und ähnliche Geräte in Sicherheitsaudits einbezogen werden und dass auch bei diesen Geräten regelmäßig kontrolliert wird, ob die Sicherheitsvorgaben umgesetzt sind.
  - **Verteilung von Privilegien:** Es muss entschieden werden, ob bestimmte Funktionen eines Druckers, Kopierers oder Multifunktionsgerätes auf ausgewählte Benutzer beschränkt werden sollen.
  - **Nachfüllen von Verbrauchsgütern:** Bei Druckern, Kopierern und Multifunktionsgeräten müssen regelmäßig Verbrauchsgüter wie Tinte, Toner oder Papier nachgefüllt werden. Es sind Regelungen zu treffen, wer hierfür zuständig ist und welche Abläufe dabei eingehalten werden müssen (siehe SYS.4.1.M7 *Versorgung und Kontrolle der Verbrauchsgüter*).

- **Regelungen des Dokumentenzugriffs:** Es müssen Maßnahmen ergriffen werden, die den Zugriff auf fremde Dokumente erschweren:
  - **Sicherheitskritische Informationen:** Werden an Netzdruckern häufig sicherheitskritische Informationen ausgedruckt, muss sichergestellt werden, dass nur befugte Personen auf die Ausdrucke zugreifen können. Hierfür können beispielsweise Netzdrucker und Kopierer eingesetzt werden, bei denen sich die Benutzer für einen Ausdruck direkt am Gerät authentisieren müssen (siehe SYS.4.1.M13 *Authentisierung bei Druckern, Kopierern und Multifunktionsgeräten*). Alternativ könnte auch der Zutritt zum Drucker auf wenige vertrauenswürdige Personen beschränkt werden, die die Ausdrucke an die jeweiligen Empfänger verteilen.
  - **Weitere Restriktionen:** Es ist zu klären, ob und welche Restriktionen für Druckerzugriffe gelten sollen. Beispielsweise ist es normalerweise nicht sinnvoll, dass Mitarbeiter, die sich von außerhalb ins Netz einwählen, auf entfernte Drucker ausdrucken können, da sie ihre Ausdrucke nicht direkt abholen können. Auch für die Zeiten, in denen normalerweise nicht gedruckt wird, können entsprechende Restriktionen umgesetzt werden.
- **Schutz der Geräte:** Der Zugriff auf die Netzdrucker sollte beschränkt werden (siehe SYS.4.1.M6 *Beschränkung der Zugriffe auf Drucker, Kopierer und Multifunktionsgeräte*):
  - **Administration:** Damit unberechtigten Personen Druckereinstellungen nicht verändern können, sind entsprechende Schutzmaßnahmen für Netzdrucker umzusetzen.
  - **Physischer Schutz:** Es sollte überlegt werden, Maßnahmen gegen Manipulationen direkt am Gerät zu ergreifen. Hierzu gehören eine geeignete Aufstellung der Drucker sowie der Schutz der Schnittstellen.
  - **Netzspezifischer Schutz:** Bei netzfähigen Komponenten sind Mechanismen zum Schutz vor Angriffen aus dem Netz einzurichten. Wenn IEEE 802.1X oder ähnliche Verfahren zur netztechnischen Zugangskontrolle von den Netzdruckern und der Netzinfrastruktur unterstützt werden, sollten diese auch verwendet werden. Damit wird verhindert, dass IT-Systeme unberechtigt an das Netz angeschlossen werden. Weiterhin sollten Druckserver keine Verbindungen zu anderen IT-Systemen außer zu den voreingestellten Druckern aufbauen können.

- **Verfügbarkeit:** Es wird empfohlen, Vorkehrungen gegen einen Ausfall der Druckserver oder einzelner Geräte zu treffen. Durch entsprechende Wartungsverträge kann beispielsweise die Ausfallzeit reduziert werden, wenn technische Defekte auftreten (siehe SYS.4.1.M15 *Notfallvorsorge bei Druckern, Kopierern und Multifunktionsgeräten*).
- **Verschlüsselung:** In der Anforderung SYS.4.1.M14 *Informationsschutz bei Druckern, Kopierern und Multifunktionsgeräten* werden unter anderem folgende Fragestellungen betrachtet, die bei der Planung eine wichtige Rolle spielen:
  - **Festplattenverschlüsselung:** Viele Drucker und digitale Kopiergeräte besitzen eingebaute Speichermedien, auf denen Informationen abgelegt werden. Falls das Gerät hierfür eine Verschlüsselung unterstützt, sollte diese benutzt werden.
  - **Verschlüsselung der Kommunikation:** Es sollte überlegt werden, die Kommunikation zwischen den Arbeitsplatzrechnern und den Druckservern sowie zwischen den Druckservern und den Druckern zu verschlüsseln.
- **Löschen des Gerätespeichers:** Als Zwischenspeicher für die temporäre Ablage der zu druckenden Informationen werden bei größeren Geräten häufig Festplatten verwendet. Je nach Konfiguration werden die Informationen im Zwischenspeicher nicht nur temporär, sondern permanent gespeichert. Es sollte gewährleistet werden, dass die Informationen nach dem Ausdruck aus dem Zwischenspeicher gelöscht werden. Hierfür besitzen viele Kopierer eine Löschfunktion. Wenn sich die Dokumente nicht automatisch löschen lassen, sollten alle Benutzer darauf hingewiesen werden, diese Funktion konsequent zu benutzen (siehe SYS.4.1.M5 *Benutzerrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten*).

Alle Entscheidungen, die in der Planungsphase getroffen wurden, müssen so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können.

SYS.4.1.M5 Erstellung von Benutzer- und Administrationsrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten [Informationssicherheitsbeauftragter (ISB)]

Drucker, Kopierer und Multifunktionsgeräte lassen sich nicht allein mit technischen Maßnahmen absichern. Zusätzlich müssen entsprechende Sicherheitsrichtlinien für die Administratoren und die Benutzer festgelegt werden. In der Administrationsrichtlinie sollten alle umzusetzenden Sicherheitsmechanismen für Drucker, Kopierer und Multifunktionsgeräte beschrieben sein. Dieses Dokument richtet sich an das Fachpersonal der Institution.

Die Sicherheitsrichtlinien für die Benutzer sollten in einem übersichtlichen Merkblatt zusammengefasst werden. Dieses Merkblatt sollte an allen Aufstellungsorten der Geräte aufgehängt werden.

Es sind folgende Aspekte zu berücksichtigen:

- **Zutritt zu den Kopier- und Druckerräumen:** Wenn möglich, sollte der Zutritt zu Räumen mit Druckern, Kopierern und Multifunktionsgeräten beschränkt werden (siehe auch SYS.4.1.M2 *Geeignete Aufstellung von Druckern, Kopierern und Multifunktionsgeräten*). Es bietet sich an, den Zutritt beispielsweise auf die Mitarbeiter einer Abteilung oder auf die Benutzer einer Etage einzugrenzen. Die Benutzer sind über die Zutrittsbeschränkungen und die zugelassenen Personenkreise zu unterrichten.
- **Behandlung nicht abgeholter Dokumente:** Häufig werden ausgedruckte Dokumente nicht abgeholt, gedruckte Fax-Sendeberichte vergessen oder Fehldrucke nicht entsorgt. Alle Benutzer müssen darüber informiert sein, dass sie ihre Ausdrucke zeitnah abholen müssen. Dokumente, die keinem Benutzer zugeordnet werden können, sollten eingesammelt oder besser direkt mit einem Schredder vernichtet werden.
- **Umgang mit sensiblen Dokumenten:** Als "hoch vertraulich" klassifizierte Informationen sollten nicht an allgemein zugänglichen Druckern ausgedruckt bzw. Kopierern vervielfältigt werden. Amtlich geheim zu haltende Dokumente (Verschlusssachen) müssen gemäß der geltenden Vorschriften und Anweisungen geschützt werden.
- **Authentisierung am Gerät:** Soll eine Authentisierung direkt am Drucker, Kopierer oder Multifunktionsgerät erfolgen (siehe SYS.4.1.M13 *Authentisierung bei Druckern, Kopierern und Multifunktionsgeräten*), müssen die Benutzer in dieses Verfahren eingewiesen werden.

- **Verteilung von Ausdrucken:** Werden an Netzdruckern oft sicherheitskritische Informationen ausgedruckt, sollte überlegt werden, die Ausdrucke an die jeweiligen Empfänger durch vertrauenswürdige Personen verteilen zu lassen. Dieser Ansatz ist eine Alternative zur Authentisierung am Gerät und hat den Vorteil, dass nur diese Personen Zutritt zu den jeweiligen Druckern benötigen.
- **Auswahl eines Standarddruckers:** Bei mehreren verfügbaren Druckern oder Multifunktionsgeräten können die Benutzer auf ihrem Client meist für alle Applikationen einen Standarddrucker vorauswählen. Als Standarddrucker sollte ein logisches (virtuelles) Gerät wie ein Druckvorschau-Programm oder ein PDF-Generator gewählt werden. Das schützt davor, dass Informationen unbemerkt ausgedruckt werden, beispielsweise weil unbeabsichtigt die Drucken-Schaltfläche in einer Applikation betätigt wurde.
- **Löschen des Kopierspeichers durch den Benutzer:** Ein Vorteil von digitalen Kopierern ist, dass ein einmal eingescanntes Dokument beliebig oft ausgedruckt werden kann. Damit Unbefugte nicht auf solche Informationen zugreifen können, muss der hierfür verwendete temporäre Speicher nach der Benutzung gelöscht werden. Bei vielen Kopierern können die Benutzer das nur manuell veranlassen, daher müssen entsprechende Hinweise und Anweisungen an den Geräten angebracht werden.Jeder Benutzer sollte sich mit dem Merkblatt zum sicheren Umgang mit Druckern, Kopierern und Multifunktionsgeräten vertraut machen.

SYS.4.1.M7 Beschränkung der administrativen Fernzugriffe auf Drucker, Kopierer und Multifunktionsgeräte

Um Angriffe auf Drucker, Kopierer und Multifunktionsgeräte zu erschweren, muss der Zugriff auf diese Geräte beschränkt werden. Im Folgenden werden einige Aspekte beschrieben, die für den sicheren Betrieb von Druckern und Kopierern berücksichtigt werden sollten:

- Beschränkung auf notwendige Zugriffsrechte:
  Wenn möglich, sollten nur so wenig Administratoren wie nötig den vollständigen Zugriff erhalten. Dabei sollten immer nur die Zugriffsrechte vergeben werden, die für die Aufgabenwahrnehmung notwendig sind.

- Absicherung der Administrationszugriffe:
  Auf administrative Bereiche und die Konfiguration sollten nur autorisierte Personen zugreifen dürfen. Der Zugriff sollte erst nach einer Authentisierung, beispielsweise durch ein Passwort oder eine PIN, möglich sein. Falls Drucker, Kopierer oder Multifunktionsgeräte über ein Netz administriert werden, muss sichergestellt sein, dass sich die Administratoren hierfür ebenfalls authentisieren müssen. Wenn systemseitig keine Authentisierung unterstützt wird, müssen geeignete Ersatzmaßnahmen ergriffen werden.
- Absicherung der Administration bei Fernzugriff:
  Alle Administrationszugriffe sollten möglichst nur über einen verschlüsselten Kanal stattfinden, damit keine Passwörter oder andere schutzbedürftige Informationen mitgehört werden können. Beispielsweise kann bei einigen Gerätetypen die Übertragung der Konfigurationsdaten über HTTPS oder SNMPv3 verschlüsselt werden. In diesem Fall sollte die unverschlüsselte Kommunikation unterbunden werden, indem beispielsweise die HTTP-Schnittstelle für die Konfiguration deaktiviert wird.
- Schutz der Anzeige des BedienfeldsIn der Regel verfügen Drucker, Kopierer und Multifunktionsgeräte über Anzeigefelder, auf denen zahlreiche Informationen angezeigt werden. Hierzu können auch Informationen gehören, die Rückschlüsse auf die ausgedruckten Dokumente schließen lassen, wie beispielsweise Datei- und Benutzernamen (z. B. "Bewerbung_bei_Recplast.doc" von Benutzer XYZ). Bei einigen Geräten werden diese Anzeigen nicht nur lokal am Gerät dargestellt, sondern können über ein Datennetz übermittelt werden. Damit die dargestellten Informationen nicht missbraucht werden können, sollte festgelegt werden, ob die Anzeige des Bedienfelds über ein Datennetz überhaupt eingesehen werden soll. Wenn dies dennoch gewünscht wird, sollte die Anzeige des Bedienfelds nur an die Mitarbeiter des IT-Betriebs übertragen werden können. Den betroffenen Benutzern sollte im Vorfeld mitgeteilt werden, dass die Anzeige des Bedienfelds von weiteren Personen eingesehen werden kann.
- Verzicht auf nicht benötigte Funktionen:

Drucker, Kopierer und Multifunktionsgeräte bieten oft mehr Funktionen, als im normalen Betrieb benötigt werden. Dadurch können sich unnötige Risiken ergeben. Daher sollten alle nicht benötigten Funktionen deaktiviert bzw. deren Nutzung so weit wie möglich eingeschränkt werden.

- Paketfilter:
  In einigen Druckern sind Paketfilter integriert, über die Verbindungen anhand von IP-Adressen oder Portnummern gefiltert werden können. Alle Ports, die nicht für den Druckbetrieb und zur Konfiguration des Druckers benötigt werden, sind möglichst zu blockieren. Unterstützt das Gerät eine verschlüsselte Kommunikation, sollte die unverschlüsselte Kommunikation mit dem Gerät so weit wie möglich unterbunden werden, beispielsweise über die entsprechenden Portnummern. Werden Druckserver eingesetzt, ist darauf zu achten, dass nur von diesen Servern eine Verbindung zu den Druckern aufgebaut werden darf. Hierdurch wird der Verbindungsaufbau von unautorisierten IT-Systemen zu den Druckern erschwert. Eine Ausnahme bilden allerdings Systeme, von denen aus Drucker konfiguriert werden sollen. Diese Systeme müssen natürlich ebenfalls auf den Drucker zugreifen können.
  Die Paketfilter sind generell so restriktiv wie möglich zu konfigurieren. Das gilt auch für den Verbindungsaufbau von den Netzdruckern zu anderen IT-Systemen. Beispielsweise sollten die Paketfilter so konfiguriert werden, dass Netzdrucker keine Verbindungen zu einem IT-System außerhalb des LANs aufbauen können. Das erschwert den ungewollten Datenaustausch mit externen IT-Systemen, beispielsweise mit Computern im Internet. Unabhängig von lokalen Paketfiltern muss am zentralen Sicherheitsgateway die Kommunikation zwischen den Druckern und externen Netzen blockiert werden.
- Netzsegmentierung:
  Oft ist es empfehlenswert, alle Drucker, Kopierer und Multifunktionsgeräte in einem logischen Netz zusammenzufassen. Das erleichtert es in vielen Fällen, sie zu konfigurieren und zu administrieren. Wird das konsequent umgesetzt, kann auf den zuständigen Routern und Gateways die Kommunikation zwischen den Druckern und anderen Netzsegmenten gezielt kontrolliert werden (sowohl Empfang als auch Versand von IP-Paketen).

SYS.4.1.M11 Einschränkung der Anbindung von Druckern, Kopierern und Multifunktionsgeräten

Häufig ist es unter wirtschaftlichen oder praktischen Gesichtspunkten nicht zweckmäßig, separate Geräte zum Drucken, Scannen, Kopieren und Fax-Versand/Empfang einzusetzen. Als Alternative sind Multifunktionsgeräte, die auch als All-in-One-Geräte bezeichnet werden, erhältlich, die mehrere oder sogar alle diese Funktionen in einem Gerät unterstützen. Teilweise bieten diese Geräte auch zusätzliche Kommunikationsschnittstellen, beispielsweise für Webzugriffe.

Multifunktionsgeräte haben meist gegenüber Einzelgeräten einen geringeren Administrationsaufwand und benötigen weniger Anschlussleitungen (Energie- und eventuell auch Datenleitungen). Multifunktionsgeräte können in der Regel direkt oder über ein LAN an Arbeitsplatzrechner angeschlossen werden.

Einige Geräte bieten eine Fax- und Modem-Funktionalität, die den Anschluss an ein Telefonnetz voraussetzt, sodass über die Kopplung mit anderen IT-Systemen eine physische Verbindung zwischen dem LAN und dem Telefonnetz entstehen kann. Falls diese Verbindung nicht von einem Sicherheitsgateway kontrolliert wird, sind hierüber unter Umständen unkontrollierte Internet-Zugriffe möglich, sodass beispielsweise Angreifer von außen auf das LAN zugreifen könnten. Der unberechtigte Aufbau von Datenverbindungen sowie ungewollten Fernwartungen muss in jedem Fall unterbunden werden.

Eine Ausnahme sind Multifunktionsgeräte mit Fax-Funktionalität, die nicht an ein Telefonnetz angeschlossen werden müssen. Diese Geräte scannen Dokumente ein und senden sie über eine Datenverbindung an einen zentralen Fax-Server, der sich typischerweise ebenfalls im LAN befindet. Erst der Fax-Server, der an das Telefonnetz angeschlossen ist, versendet das Fax an den eigentlichen Empfänger. Wird ein Fax-Server verwendet, sind die im Baustein NET.4.3 *Fax* empfohlenen Maßnahmen umzusetzen.

Wenn Multifunktionsgeräte an ein Telefonnetz angeschlossen werden können, muss zunächst entschieden werden, ob dieser Anschluss tatsächlich erforderlich ist, das heißt, ob die entsprechende Fax- oder Modem-Funktionalität benötigt wird. Falls auf den Anschluss an das Telefonnetz verzichtet werden kann, sind möglichst folgende Schutzmaßnahmen zu ergreifen:

- Die Fax- bzw. Modem-Funktionalität ist auf dem Gerät zu deaktivieren.
- Das Kabel für den Anschluss an das Telefonnetz ist zu entfernen. Keinesfalls darf das Kabel in die Telefondose eingesteckt werden.
- Wenn sich das Gerät an einem frei zugänglichen Ort befindet, sollten möglichst die Telefondosen in dem jeweiligen Raum deaktiviert oder die Schnittstelle zum Telefonnetz aus dem Gerät ausgebaut werden. Ist beides nicht möglich, sollte regelmäßig kontrolliert werden, ob nicht unbefugt die Verbindung zum Telefonnetz hergestellt worden ist.

Wenn die Fax- oder Modem-Funktionalität des Multifunktionsgerätes genutzt werden soll, muss sichergestellt sein, dass der hierfür erforderliche Anschluss an das Telefonnetz nicht zu unkontrollierten Datenverbindungen zwischen dem LAN und Fremdnetzen führen kann. Folgende Ansätze sind möglich:

- Das Multifunktionsgerät wird an einen Stand-Alone-PC angeschlossen, das heißt an einen Rechner, der nicht mit dem LAN verbunden ist. Nachteilig bei diesem Ansatz ist, dass Daten in vielen Fällen mithilfe von Datenträgern zwischen dem Stand-Alone-PC und dem LAN transportiert werden müssen (siehe auch SYS.3.4 Mobile Datenträger).
- Eine Alternative ist, das Multifunktionsgerät oder den Rechner, an dem das Gerät angeschlossen ist, mithilfe eines zusätzlichen Sicherheitsgateways vom LAN zu trennen.
- Eine weitere Alternative ist, das Multifunktionsgerät oder den Rechner, an dem das Multifunktionsgerät angeschlossen ist, in einer demilitarisierten Zone (DMZ) eines bestehenden Sicherheitsgateways zu platzieren.

Alle genannten Lösungsansätze müssen systematisch im Sicherheitskonzept berücksichtigt werden und erfordern zusätzliche Sicherheitsmaßnahmen, beispielsweise zum Schutz vor schädlichem Code.

SYS.4.1.M15 Verschlüsselung von Informationen bei Druckern, Kopierern und Multifunktionsgeräten

Damit ein Ausdruck erstellt werden kann, müssen die erforderlichen Informationen vom Arbeitsplatzrechner zum Drucker übertragen werden. Bei Kopierern findet das meist intern zwischen Scannereinheit und Speicher statt. Ein Angreifer könnte versuchen, auf den Speicher zuzugreifen oder die Informationen bei der Übertragung zum Drucker abzuhören.

Es sollte gewährleistet werden, dass die Informationen nach dem Ausdruck aus dem Zwischenspeicher gelöscht werden (siehe SYS.4.1.M5 *Benutzerrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten* und *SYS.4.1.M3 Planung des Einsatzes von Druckern, Kopierern und Multifunktionsgeräten*). Falls häufig Informationen mit einem höheren Schutzbedarf ausgedruckt oder kopiert werden, ist zu beachten, dass einfaches Löschen nicht ausreicht, um zu verhindern, dass gelöschte Daten wiederhergestellt werden können (siehe OPS.1.18 Löschen und Vernichten). Einige Geräte besitzen hierfür Mechanismen zum *sicheren Löschen*. Hierbei handelt es sich um eine Löschfunktion, welche die Daten zusätzlich überschreibt. Falls eine solche Funktion vorhanden ist, muss sie aktiviert werden. Andernfalls müssen adäquate Alternativlösungen gefunden werden.

Wenn möglich, sollten auch Maßnahmen ergriffen werden, die es einem Angreifer erschweren, auf den Speicher physisch zuzugreifen bzw. die Festplatten auszubauen. Um erkennen zu können, ob versucht wurde, den internen Speicher auszubauen oder zu manipulieren, sollten die Geräte versiegelt werden. Generell sollten Drucker, Kopierer und Multifunktionsgeräte so aufgestellt werden, dass sich niemand unbeobachtet an ihnen zu schaffen machen kann.

Als zusätzlicher Schutz wird empfohlen, die Informationen in den internen Speichern verschlüsselt zu speichern. Zahlreiche Drucker, Kopierer und Multifunktionsgeräte bieten diese Funktion an. Wenn das eingesetzte Gerät eine verschlüsselte Speicherung unterstützt, sollte diese Funktion aktiviert werden.

Die Kommunikation zwischen Arbeitsplatzrechnern, Druckservern und Netzdruckern erfolgt meist über ein Datennetz, für das die gleichen Gefährdungen wie bei anderen Datenverbindungen zu beachten sind. Damit diese Kommunikation nicht abgehört werden kann, sollten daher die Druckaufträge möglichst verschlüsselt übertragen werden.

Einige Druckprotokolle, wie das besonders bei Unix-Systemen weit verbreitete LPR/LPD-Protokoll (Line Printer Remote / Line Printer Daemon), unterstützen keine Verschlüsselung. Ähnlich ist die Situation bei SMB/CIFS (Server Message Block / Common Internet File System) unter Windows.

Daher sollte ein Protokoll wie IPP (Internet Printing Protocol) gewählt werden, das eine Verschlüsselung unterstützt, beispielsweise TLS/SSL (Transport Layer Security / Secure Sockets Layer) in Verbindung mit IPP.

Unter Unix-Systemen sollte beispielsweise das Common Unix Printing System (CUPS) eingesetzt werden, das bei neueren Versionen in der Voreinstellung zur Kommunikation zwischen Client und Druckserver das Protokoll IPP verwendet. Durch eine entsprechende Konfiguration kann dabei TLS/SSL aktiviert werden.

SYS.4.1.M17 Schutz von Nutz- und Metadaten

tbd: Anpassung an die Anforderung SYS.4.1.A6 des Bausteins SYS.4.1. Drucker und Multifunktionsgeräte notwendig, Anmerkungen und Vorschläge gerne an die E-Mail-Adresse grundschutz@bsi.bund.de

SYS.4.1.M18 Konfiguration von Druckern, Kopierern und Multifunktionsgeräten

tbd: Anpassung an die Anforderung SYS.4.1.A7 des Bausteins SYS.4.1. Drucker und Multifunktionsgeräte notwendig, Anmerkungen und Vorschläge gerne an die E-Mail-Adresse grundschutz@bsi.bund.de

SYS.4.1.M19 Sicheres Löschen von Informationen bei Druckern, Kopierern und Multifunktionsgeräten

SYS.4.1.A12 Sicheres Löschen von Informationen bei Druckern, Kopierern und Multifunktionsgeräten notwendig, Anmerkungen und Vorschläge gerne an die E-Mail-Adresse grundschutz@bsi.bund.de

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

SYS.4.1.M14 Authentisierung und Autorisierung bei Druckern und Multifunktionsgeräten (CI)

Im normalen Büroalltag ist es oft einfach, Ausdrucke vertraulicher Dokumente direkt am Drucker einzusehen, solange diese noch nicht abgeholt wurden. Daher müssen Maßnahmen ergriffen werden, die den Zugriff auf fremde Dokumente erschweren.

Generell sollten nur berechtigte Personen auf die ausgedruckten oder kopierten Dokumente zugreifen können. Der Kreis der berechtigten Personen ist so klein wie möglich zu halten.

Kann der Zugang zu einem Netzdrucker nicht beschränkt werden, sollte überlegt werden, Geräte einzusetzen, die eine Authentisierungsfunktion für Benutzer bieten. Ist diese Funktion aktiviert, wird das Dokument erst ausgedruckt, nachdem sich der Benutzer, der den entsprechenden Druckauftrag abgesendet hat, am Gerät identifiziert und authentisiert hat. In der Praxis werden zur Authentisierung häufig Chipkarten oder PINs verwendet. Dabei können PINs je nach Gerätetyp benutzer- oder dokumentenspezifisch festgelegt werden. Bei letzterer Variante wird eine PIN festgelegt, wenn der Druckauftrag abgesendet wird. Erst nachdem diese PIN am Gerät eingegeben wurde, wird das Dokument, das der PIN zugeordnet ist, ausgedruckt. Druckaufträge, die zwar abgesendet, aber nicht abgeholt wurden, müssen regelmäßig gelöscht werden. Die Drucker sollten möglichst so konfiguriert werden, dass bei mehrmaliger Eingabe einer falschen PIN der Druckauftrag automatisch gelöscht wird.

Ein weiterer Sicherheitsgewinn kann erzielt werden, wenn das zu druckende Dokument vom Arbeitsplatz-PC verschlüsselt zum Drucker übertragen und verschlüsselt zwischengespeichert wird. Erst nach einer erfolgreichen Authentisierung direkt am Drucker wird das Dokument entschlüsselt und ausgedruckt.

Es gibt auch Kopierer, die eine ähnliche Authentisierungsfunktion bieten, meist als optionale Erweiterung. Erst nachdem eine Chipkarte eingelesen oder eine PIN eingegeben wurde, können die Benutzer kopieren. Obwohl diese Authentisierungsfunktionen hauptsächlich für Kostenabrechnungen angeboten werden, können Angreifer durch diese Erweiterungen schwerer unberechtigt Kopien erstellen.

Wenn an Netzdruckern oder Kopierern häufig hochvertrauliche Dokumente gedruckt beziehungsweise vervielfältigt werden müssen, sollte überlegt werden, hierfür Geräte mit Authentisierungsmöglichkeit einzusetzen.

SYS.4.1.M16 Notfallvorsorge bei Druckern, Kopierern und Multifunktionsgeräten (A)

Fallen Drucker, Kopierer und Multifunktionsgeräte länger aus, ist das für die meisten Institutionen nicht tolerierbar. Besonders durch einen Ausfall zentraler Komponenten, die für die gesamte Drucker-Infrastruktur erforderlich sind, werden Geschäftsprozesse erheblich beeinträchtigt. Je nach Verfügbarkeitsanforderungen sind daher geeignete Maßnahmen zu ergreifen, um die Ausfallzeit beziehungsweise deren Auswirkungen zu verringern.

Es ist darauf zu achten, dass immer genügend Verbrauchsmaterial verfügbar ist, z. B. Toner und Papier. Ab einer bestimmten Restmenge, die vom Verbrauch abhängig ist, muss neues Verbrauchsmaterial beschafft und bereitgestellt werden.

An jedem Kopierer, Drucker und Multifunktionsgerät sowie auch an anderen Komponenten des Drucksystems müssen diverse Konfigurationseinstellungen vorgenommen werden. Um diese Einstellungen nach einem Ausfall oder Austausch schnell wieder korrekt einrichten zu können, müssen die Konfigurationen systematisch dokumentiert werden.

Je weniger Geräte verfügbar sind, desto gravierender ist es, wenn ein einzelnes ausfällt. Der Ausfall eines Druckservers ist besonders problematisch, da diese Geräte oft nur einmal oder wenige Male vorhanden sind.

Um auf Notfälle reagieren zu können, sollte zwischen zentralen Komponenten einerseits und Druckern, Kopierern und Multifunktionsgeräten andererseits unterschieden werden. Bei einem höheren Schutzbedarf bezüglich der Verfügbarkeit sollte überlegt werden, zentrale Komponenten, wie Druckserver, redundant auszulegen. Wenn der einzige zentrale Server ausfällt, könnte sonst eventuell im gesamten LAN nicht mehr gedruckt werden.

Dezentrale Komponenten, wie Drucker, sind häufig auf mehreren Etagen oder in verschiedenen Büros eines Gebäudes zu finden. Generell sollte die Druckerlandschaft so gestaltet werden, dass die Benutzer beim Ausfall eines Druckers problemlos einen anderen Drucker verwenden können.

- Es sollte überlegt werden, für lokale Drucker, die einen höheren Schutzbedarf bezüglich der Verfügbarkeit haben und direkt an einen Arbeitsplatz angeschlossen werden, Ersatzgeräte bereitzustellen (*Cold Standby*). Bei einem Ausfall könnte der defekte Drucker zeitnah gegen das Ersatzgerät ausgetauscht werden.
- Für große Kopierer, Drucker und Multifunktionsgeräte die von mehreren Personen benutzt werden, sollten Wartungsverträge mit einer dem Schutzbedarf angemessenen Reaktionszeit abgeschlossen werden.
- Es sollte eine Liste von Fachhändlern geführt werden, bei denen unproblematisch neue Geräte beschafft werden können.
- Bei Bedarf können Ersatzteile gelagert werden, die häufig benötigt werden. Das ist allerdings nur sinnvoll, wenn entsprechendes Fachwissen vorhanden ist, um die Ersatzteile selbstständig austauschen zu können.

SYS.4.1.M20 Erweiterter Schutz von Informationen bei Druckern und Multifunktionsgeräten (C)

tbd: Anpassung an die Anforderung SYS.4.1.A13 des Bausteins SYS.4.1. Drucker und Multifunktionsgeräte notwendig, Anmerkungen und Vorschläge gerne an die E-Mail-Adresse grundschutz@bsi.bund.de

SYS.4.1.M21 Erweiterte Absicherung von Druckern und Multifunktionsgeräten (IA)

tbd: Anpassung an die Anforderung SYS.4.1.A14 des Bausteins SYS.4.1. Drucker und Multifunktionsgeräte notwendig, Anmerkungen und Vorschläge gerne an die E-Mail-Adresse grundschutz@bsi.bund.de

3 Weiterführende Informationen

3.1 Wissenswertes

3.1.1Kriterien für die Beschaffung und geeignete Auswahl von Druckern, Kopierern und Multifunktionsgeräten

Wenn neue Drucker, Kopierer oder Multifunktionsgeräte beschafft werden, sollten diese von vornherein so ausgewählt werden, dass im späteren Betrieb mit geringem personellen und organisatorischen Zusatzaufwand ein hohes Maß an Sicherheit erreicht werden kann.

Viele Drucker und Kopierer sind modular aufgebaut. Das Grundgerät kann um zusätzliche Funktionen erweitert werden. Hierzu gehören beispielsweise auch zusätzliche Sicherheitsmechanismen, wie die Unterstützung einer Authentisierung über PINs oder Chipkarten. Bevor Drucker, Kopierer und ähnliche Geräte beschafft werden, sind daher neben den allgemeinen Anforderungen auch die Sicherheitsanforderungen festzulegen. Die Anforderungen und die auf dieser Basis getroffenen Entscheidungen sind zu dokumentieren. Nachfolgend werden einige grundsätzliche Anforderungen bei der Beschaffung von Druckern aufgelistet:

- Grundlegende funktionale Anforderungen
  - Sollen netzfähige Geräte beschafft werden?
  - Ist die Leistungsfähigkeit des Geräts der Größe des Benutzerkreises angemessen?
  - Was für ein Druckertyp mit welchem Druckverfahren soll angeschafft werden?
  - Kann das Gerät nachträglich durch zusätzliche Funktionen erweitert werden?
    Viele Geräte können durch entsprechendes Zubehör beispielsweise Netzfähigkeit, Duplexdruck, zusätzliche Papierschächte und eine Authentisierung nachgerüstet werden.
  - Kann akzeptiert werden, dass auf den Ausdrucken Wasserzeichen hinterlassen werden, die eine Zuordnung eines Ausdrucks zu einem konkreten Drucker zulassen ("Yellow Dots")?
- Allgemeine Sicherheit
  - Unterstützt das System sichere Protokolle zur Administration?
    Damit die Geräte von zentraler Stelle aus administriert werden können, müssen netzfähige Geräte sichere Protokolle zur Administration unterstützen, bei einer Browser-basierten Konfiguration beispielsweise SSL/TLS.
  - Können Informationen verschlüsselt gespeichert werden?
    Um nach einem (unberechtigten) Ausbau der Festplatte den Zugriff auf die Daten zu verhindern, legen einige Geräte die Informationen verschlüsselt auf der Festplatte ab.
  - Ist eine Möglichkeit der Authentisierung direkt am Gerät vorgesehen (z. B. über Passwort- oder PIN-Eingaben oder Chipkarten) oder kann diese Funktion nachträglich eingebaut werden?
    Bei vielen Geräten ist eine Authentisierung vorgesehen, bei einigen allerdings nur für die Administration, um Zugriffe auf die Konfiguration abzusichern. Es gibt jedoch auch Geräte, bei denen sich alle Benutzerzugriffe absichern lassen, sodass Informationen erst ausgedruckt werden, wenn sich der Benutzer am Gerät authentisiert hat. Das dient als Schutz davor, dass an einen Netzdrucker übertragene oder an einem Kopierer eingescannte Informationen von Unberechtigten ausgedruckt werden können. Eine solche Funktion kann auch für eine Kostenkontrolle verwendet werden.
  - Sind Ösen oder andere Möglichkeiten vorhanden, um die Geräte physisch vor Diebstahl zu schützen?
  - Können Manipulationen an der Hardware durch Gehäuseschlösser oder ähnliche Vorkehrungen erschwert werden?
    Häufig kommt es beispielsweise vor, dass Speichermodule aus Druckern, Kopierern oder Multifunktionsgeräten können beispielsweise gestohlen werden.

- Sicheres Löschen des Speichers
  - Kann nach jedem Kopiervorgang der Speicher durch die Benutzer gelöscht werden?
    In vielen Geräten sind Speicher, meist in der Form von Festplatten, eingebaut. Wenn Daten dort unverschlüsselt gespeichert werden, können diese eventuell von Unbefugten ausgelesen werden. Außerdem besteht die Gefahr, dass Angreifer die im Gerät gespeicherten Seiten erneut ausdrucken lassen. Einige Geräte bieten daher Funktionen zum Löschen des Speichers. Wenn möglich, sollten sie so eingestellt werden können, dass automatisch nach jedem Kopiervorgang gelöscht wird.
  - Ist es möglich, die gesamte Festplatte zu löschen?
    Für eine spätere Entsorgung sollte die gesamte Festplatte durch Überschreiben gelöscht werden können. Dies sollte nur nach Eingabe eines entsprechenden Löschbefehls durch einen Berechtigten möglich sein. Alternativ sollte der Speicher ausgebaut und separat gelöscht werden können.
  - Werden Informationen zum Löschen auf dem Display angezeigt?
    Auf dem Display des Geräts sollte es möglichst angezeigt werden, wenn die zuletzt gespeicherten Daten oder die gesamte Festplatte durch Überschreiben gelöscht wird.
- Netztechnische Sicherheit
  - Besitzt das Gerät netztechnische Schutzmechanismen, wie IP- und Portfilter?
  - Muss das Gerät WLAN- oder Bluetooth-fähig sein oder ist ein kabelgebundener Anschluss ausreichend?
    Der Einsatz von Funktechniken ist mit höheren Sicherheitsrisiken verbunden als der Anschluss über Kabel. Bei funkbasierten Lösungen müssen deshalb meist zusätzliche Sicherheitsmaßnahmen ergriffen werden.
  - Unterstützt das Gerät die Verschlüsselung der Druckerkommunikation?
    Werden die auszudruckenden Informationen über ein Netz übertragen, sollte verhindert werden, dass sie mitgelesen oder verändert werden können. Darum sollten Netzprotokolle eingesetzt werden, die eine Verschlüsselung der Informationen unterstützen. Ein Beispiel hierfür ist das Internet Printing Protokoll (IPP) in Verbindung mit SSL (Secure Sockets Layer) bzw. TLS (Transport Layer Security).
  - Kann das Gerät in eine vorhandene IEEE 802.1X-Umgebung integriert werden?
    IEEE 802.1X ermöglicht die Authentisierung der Endgeräte am Netz. Dies schützt davor, dass IT-Systeme unerlaubt am LAN betrieben werden.
- Wartbarkeit
  - Bietet der Hersteller regelmäßige Updates und schnell verfügbare Sicherheitspatches an?
    Es ist besonders wichtig, dass der Hersteller zeitnah auf bekannt gewordene Sicherheitsmängel reagiert.
  - Können für das Produkt Wartungsverträge abgeschlossen werden?
    Oft ist der Zugriff auf Updates und Unterstützungsleistungen des Herstellers nur in Verbindung mit einem gültigen Wartungsvertrag möglich. Können im Rahmen der Wartungsverträge maximale Reaktionszeiten für die Problembehebung festgelegt werden?
    Ein Wartungsvertrag ist nur dann geeignet, wenn mit den garantierten Reaktions- und Wiederinbetriebnahmezeiten die festgelegten Anforderungen an die Verfügbarkeit der Geräte abgedeckt werden können.
  - Bietet der Händler oder Hersteller einen technischen Kundendienst (Hotline) an, der in der Lage ist, sofort bei Problemen zu helfen?
    Dieser Aspekt sollte Bestandteil eines Wartungsvertrags sein. Beim Abschluss des Vertrags ist darauf zu achten, dass die Hotline- bzw. Support-Mitarbeiter auch die Sprache der Personen sprechen, die in der Regel dort anrufen werden.

- Kosten
  - Wie hoch sind die Anschaffungskosten der Geräte?
  - Wie hoch sind die voraussichtlichen laufenden Kosten, einschließlich Wartung, Betrieb und Support?Diese Kosten sollten bereits in der Beschaffungsphase mit berücksichtigt werden. Der Inhalt der Wartungs- und Supportverträge sollte geprüft werden, beispielsweise im Hinblick auf Reaktionszeiten, Hotline und Qualifikation des Personals.

3.1.2Verwaltung von Druckern

Institutionen benötigen oft sehr viele Drucker für ihre unterschiedlichen Einsatzzwecke. Hierfür müssen geeignete Geräte ausgewählt werden. Außerdem ist festzulegen, wo die Hardware-Komponenten aufgestellt werden.

Im Folgenden werden typische Drucksysteme, deren Bestandteile und Kommunikationsbeziehungen vorgestellt. Drucksysteme bestehen in der Regel aus Client- und Server-seitigen Software-Komponenten.

Drucksysteme

In den seltensten Fällen sendet eine Anwendung den Druckauftrag direkt an einen Drucker, sondern zwischen der Anwendung und dem Drucker wird ein Drucksystem betrieben. Hierbei ist es oft erforderlich, dass diese Drucksysteme netzfähig sind und mehrere Clients auf einen Drucker zugreifen können. Auch bei einer ausschließlich lokalen Installation wird ein Drucksystem benötigt. Hierbei sendet der Client intern den Druckauftrag an den Druckserver.

Ein Drucksystem kann unter anderem folgende Aufgaben erfüllen:

- Annahme des Druckauftrags von der Anwendung,
- Verwaltung der Druckaufträge in einer Warteliste (Spooling),
- Ergänzung um zusätzliche Informationen, wie Trennseiten, Papierformat oder andere Eigenschaften,
- Umwandlung in ein dem Drucker verständliches Datenformat, wie PostScript oder PCL,
- Verwaltung von logischen und physischen Druckern,
- Benutzerverwaltung und
- Protokollierung.

Unterschiedliche Betriebssysteme favorisieren unterschiedliche Drucksysteme. Besonders bei heterogenen IT-Landschaften ist es entscheidend, dass die Drucksysteme miteinander kompatibel sind. Viele Systeme bieten Schnittstellen zu anderen Drucksystemen. Dadurch kann beispielsweise ein Unix-System auf einen Drucker zugreifen, der von einem Windows-System verwaltet wird.

Abhängig vom Betriebssystem sind folgende Drucksysteme weit verbreitet:

- Berkeley Printing System,
- Common Unix Printing System (CUPS) und
- Druckerfreigaben auf der Basis von SMB unter Windows.

Bei heterogenen Netzlandschaften ist möglichst ein Drucksystem auszuwählen, das von allen Betriebssystemen unterstützt wird. Als Alternative kann es zweckmäßig sein, mehrere verschiedene Drucksysteme einzusetzen, die unter Umständen untereinander kommunizieren können. Die Entscheidung über die zu nutzenden Drucksysteme ist zu begründen und zu dokumentieren.

Bestandteile

Der Druckauftrag, der von einer Anwendung erstellt wurde und an einen Drucker ausgegeben werden soll, muss mehrere Zwischenschritte durchlaufen. Für diese Schritte sind jeweils einzelne Komponenten zuständig, die im folgenden vorgestellt werden.

- **Druckclient**
  Bei einem Druckclient handelt es sich um eine Softwarekomponente, die auf dem Arbeitsplatz-PC installiert ist. In der Regel empfängt der Druckclient eine entsprechende Anweisung von einer Anwendung und sendet den Druckauftrag an den Druckserver weiter.
  Mit der Auswahl eines Druckernamens kann in vielen Fällen der Zieldrucker ausgewählt werden. Eine Ausnahme ist der Ausdruck in Druckerpools, bei denen für jeden Druckauftrag ein anderer Drucker vom Druckserver bestimmt werden kann.
  Häufig können weitere Funktionen, wie Duplexdruck und Heften, durch den Druckclient festgelegt werden. Hierfür sendet der Druckclient die Druckdaten an den Druckserver. Wie der Drucker angesteuert werden kann und welche Formate er beherrscht, wird in der Regel bei der Installation des Druckers dem Drucksystem bekannt gemacht.
- **Druckserver**
  Der Druckserver empfängt die Druckaufträge der Clients und verwaltet sie. Die Aufträge werden in eine Warteliste eingefügt und anschließend an den Drucker übertragen. Je nach Konfiguration wird bei mehreren Druckaufträgen das zuerst empfangene Dokument als erstes an den Drucker weitergeleitet oder durch eine entsprechende Priorität bevorzugt behandelt. In einigen Fällen lassen sich auch spezielle Zeiträume festlegen, in denen Druckaufträge ausgeführt werden.

- Das Dokument wird meistens direkt auf dem Druckserver aufbereitet. Dafür benötigt das Drucksystem die gerätespezifischen Druckerinformationen und Filter. Beispielsweise können diese Druckerinformationen als PPD (PostScript Printer Description) definiert sein. Verallgemeinert handelt es sich dabei um eine Spezifikation, welche Formate und Funktionen vom Drucker beherrscht werden. Beispiele für die spezifizierten Parameter sind Papierformate, Rasterauflösungen, Schriftarten, Duplex, Heften, Lochen und Farbdruck. Anhand dieser Spezifikation kann die Druckanweisung, die an den Drucker übermittelt wird, generiert werden.
- Der Druckserver bereitet den Druckauftrag auf. Dazu konvertiert er ihn in ein Datenformat, das vom jeweiligen Drucker unterstützt wird. Ist das Eingangsformat beispielsweise PostScript, muss das Dokument in ein für diesen Drucker verständliches Ausgangsformat konvertiert werden, wenn der Drucker nicht PostScript-fähig ist. Beispiele für Ausgangsformate sind PDF, PCL und PostScript.

- **Drucker**
  Der Drucker empfängt das vorbereitete Dokument vom Druckserver und gibt es aus. Es kann zwischen logischen und physischen Druckern unterschieden werden. Folgende Anschlussarten werden in der Praxis für physische Drucker eingesetzt:
  - Lokale Drucker: Diese Drucker verfügen in der Regel über eine USB-Schnittstelle und werden direkt an ein Client-System angeschlossen.
  - Netzdrucker: Der Drucker wird über ein Netz angesprochen.
  - Druckserver mit lokalen Druckern: Der Drucker wird lokal an einen Druckserver, der über einen Netzanschluss verfügt, angeschlossen. Dabei kann der Druckserver in Form einer Appliance oder als klassischer Server realisiert sein. Bei diesem Ansatz muss der Druckserver häufig zwischen Netz und lokalem Anschluss konvertieren, beispielsweise als USB-Ethernet-Bridge.

- Logische Drucker können innerhalb des Drucksystems unterschiedliche Aufgaben haben. Die folgenden Szenarien sind in der Praxis häufig anzutreffen:
    -
        - Mehrere physische Drucker werden über einen logischen Drucker angesprochen. Neben dem Vorteil einer höheren Druckleistung (es kann parallel gedruckt werden), kann ohne größeren Konfigurationsaufwand auf einen anderen Drucker zugegriffen werden, wenn einer ausfällt. Es wird empfohlen, nur Geräte mit ähnlichen Eigenschaften in einer Klasse zusammenzufassen.
        - Ein physischer Drucker wird von mehreren logischen Druckern, die jeweils auf unterschiedlichen Druckservern installiert sind, angesprochen. Das bietet sich an, wenn mehrere Druckserver eingesetzt werden. Fällt ein Druckserver aus, kann einfach auf einen anderen Druckserver gewechselt werden, sodass der Druckbetrieb ohne größeren Konfigurationsaufwand fortgesetzt werden kann.
        - Des Weiteren können logische Drucker verwendet werden, um einem physischen Drucker mit mehreren verschiedenen Einstellungen jeweils einen eigenen Druckernamen zuzuordnen. Beispielsweise können für einen physischen Drucker zwei logische Drucker definiert werden: einer für Simplex- und einer für Duplex-Druck. Alle logischen Drucker sind zu dokumentieren.

Kommunikationsbeziehungen

Zwischen den einzelnen Komponenten eines Drucksystems entstehen unterschiedliche Kommunikationsverbindungen.

- **Kommunikation zwischen Druckclient und Druckserver**
  Die Kommunikationsverbindung kann zwischen einem Druckclient und dem Druckserver sowie zwischen verschiedenen Druckservern aufgebaut werden. Je nach Szenario werden die Druckinformationen über ein Netz oder lokal ausgetauscht.
  Je nach Drucksystem können folgende Protokolle eingesetzt werden:
    - HTTP (Hypertext Transfer Protocol),
    - IPP (Internet Printing Protocol),
    - LPR/LPD (Line Printer Remote / Line Printer Daemon),
    - SMB (Server Message Block) und
    - Appletalk beziehungsweise Bonjour.

  Abhängig von den eingesetzten Druckern und vom gewählten Drucksystem sind geeignete Protokolle auszuwählen. Innerhalb eines Netzes sollten möglichst wenig unterschiedliche Druck-Protokolle eingesetzt werden. Die Entscheidung ist zu dokumentieren.
  Auch für die Verwaltung müssen bei einigen Drucksystemen Informationen ausgetauscht werden. Die Clients müssen beispielsweise regelmäßig über die verfügbaren Drucker und deren Status informiert werden. Dabei können, je nach Drucksystem, folgende Strategien verfolgt werden:
    - Broadcasting: In regelmäßigen Abständen sendet der Server unaufgefordert eine Nachricht an alle Clients in der Broadcast-Domäne.
    - Polling: Der Druckclient fragt die Informationen vom Server ab.

  Broadcasting vereinfacht die Administration, ist aber mit weiteren Problemen verbunden. Befinden sich die Clients und Server in verschiedenen Broadcast-Domänen, erreichen die Pakete nicht alle Clients. In der Praxis können auch Probleme auftreten, wenn der Druckserver mehrere Netzschnittstellen hat und die Broadcast-Pakete an die falschen Schnittstellen sendet. Für die Konfiguration ist ein Verfahren auszuwählen und zu dokumentieren.

- **Kommunikation zwischen Druckserver und Drucker**
  Für die Kommunikation mit den Druckern werden ebenfalls entsprechende Protokolle benötigt. Diese hängen von den Druckerspezifikationen und von der Anschlussart ab. Beispielsweise gibt es Protokolle für
  - die Kommunikation über die parallele Schnittstelle,
  - den Anschluss über USB,
  - den Betrieb über die serielle Schnittstelle und
  - die netzbasierte Kommunikation mit den Druckern, beispielsweise über das HP JetDirect Protokoll oder über IPP (Internet Printing Protocol).

  Einige Druckersysteme ermöglichen auch die Konfiguration der Drucker über den Druckserver. Neben proprietären Protokollen wird hier oft das Simple Network Management Protocol (SNMP) eingesetzt.
  Es müssen Protokolle ausgewählt werden, die für die Anforderungen der Institution und für die einzusetzenden Komponenten geeignet sind. Die Entscheidungen sind zu dokumentieren.

Design der Druckerlandschaft

Neben der Auswahl des Drucksystems spielt die Anordnung der einzelnen Bestandteile, wie Clients, Server und Drucker, eine wichtige Rolle. Grob können folgende Ansätze für die Druckerarchitektur unterschieden werden:

- Lokale Drucker: Sowohl die Anwendung, die den Druckauftrag generiert, als auch der Druckserver und der Druckclient werden gemeinsam auf einem IT-System betrieben. Der Drucker ist über die USB-, parallele oder serielle Schnittstelle an das IT-System angeschlossen.
- Arbeitsplatz-PC mit Netz-Drucker: Auf einem oder mehreren IT-Systemen befinden sich neben der sendenden Anwendung auch der Druckclient und der Druckserver. Die Druckserver der einzelnen IT-Systeme senden die Druckaufträge an einen netzfähigen Drucker.
- Zentraler Druckserver: Auf den Arbeitsplatzsystemen sind nur die Druckclients installiert. Diese nehmen den Druckauftrag an und leiten ihn über ein Netz an einen zentralen Druckserver weiter. Auf diesem Druckserver werden die Druckaufträge verwaltet. Der Druckserver sendet die Aufträge an lokale oder netzbasierte Drucker weiter, wo sie ausgegeben werden.
- Kombinationen: Es sind zahlreiche Kombinationen aus den oben genannten Anordnungen möglich. Ein Beispiel ist der Anschluss eines lokalen Druckers am Arbeitsplatz-PC für kleinere Druckaufträge und der parallele Betrieb eines zentralen Druckservers für umfangreiche Ausdrucke.

Die getroffenen Entscheidungen zum Aufbau der Druckerlandschaft sind zu dokumentieren.

Über Dokumentenscanner können analoge Informationen digitalisiert werden, beispielsweise um ein Papierdokument auf IT-Systeme zu kopieren, zu archivieren oder weiter zu bearbeiten. Statt an jedem Arbeitsplatz-PC einen lokalen Scanner zu installieren, ist es meist wirtschaftlicher, einen oder mehrere zentrale Scanner zur Verfügung zu stellen. Um geeignete Sicherheitsmaßnahmen auszuwählen, muss zwischen Scan-PCs und netzfähigen Dokumentenscannern unterschieden werden.

Ein Scan-PC ist ein Standard-PC, der oft an ein LAN angebunden ist und an den ein lokaler Scanner angeschlossen ist. Scan-PCs werden häufig in ähnlichen Räumlichkeiten wie Netzdrucker betrieben und können von diversen Mitarbeitern benutzt werden. Außerdem ist auf Scan-PCs üblicherweise Software installiert, mit der die eingescannten Informationen nachbearbeitet werden können, also beispielsweise OCR- oder Bildbearbeitungsprogramme.

Netzfähige Dokumentenscanner (*Büroscanner*) sind Kompaktgeräte, an denen Papierdokumente und Ähnliches ohne größeren Aufwand eingelesen und zur weiteren Bearbeitung über ein LAN an den Benutzer übertragen werden können, beispielsweise per E-Mail. Diese Funktion ist häufig auch in Faxgeräten integriert. Der Funktionsumfang von netzfähigen Dokumentenscannern ist meist deutlich geringer als bei Scan-PCs.

Scan-PC

Wird ein Standard-PC zum Scannen verwendet, so sind die Empfehlungen aus den Baustein SYS.2.1. Allgemeiner Client und den zutreffenden betriebssystemspezifischen Client-Bausteinen des IT-Grundschutz-Kompendiums umzusetzen.

Scan-PCs können im Produktivnetz, in einem Testnetz oder auch als Stand-Alone-System ohne einen Netzanschluss betrieben werden. Sie sollten so konfiguriert sein, dass sich die Benutzer authentisieren müssen. Die eingescannten Daten können über das Netz oder über transportable Datenträger zu den Arbeitsplatz-PCs übertragen werden.

Die analogen Scan-Vorlagen sollten nicht unbeaufsichtigt beim Gerät verbleiben. Auch die digitalen Scan-Ergebnisse sollten nach der Übertragung auf das gewünschte Zielsystem, zum Beispiel auf den Arbeitsplatz-PC des jeweiligen Benutzers, aus allen allgemein zugreifbaren Verzeichnissen gelöscht werden.

Netzfähige Dokumentenscanner

Mit diesen Geräten können auch ohne einen angeschlossenen PC Dokumente gescannt werden. Dabei werden die Dokumente in Bild-Dateien mit gängigen Dateiformaten umgewandelt.

Zur weiteren Bearbeitung müssen die Geräte die eingescannten Dokumente an andere IT-Systeme im Netz versenden. Folgende Übertragungs- und Speicherverfahren werden in der Regel unterstützt:

- Ablage auf Netzlaufwerke.
  Die eingescannten Dokumente werden direkt über ein Netzprotokoll auf einen Datei-Server übertragen. Unterstützt werden in der Regel NFS- und SMB-Freigaben oder die Übertragung mittels FTP. Grundsätzlich muss sichergestellt werden, dass der Personenkreis, der Zugriff auf die Zielverzeichnisse mit den eingescannten Daten hat, so klein wie möglich ist. Bei erhöhtem Schutzbedarf ist es eventuell erforderlich, dass nur der Benutzer, der die Informationen eingescannt hat, auch auf die Scan-Ergebnisse zugreifen kann. Nicht alle Scanner ermöglichen es, die erzeugten Dateien in benutzerspezifischen Bereichen der Server zu speichern. Wenn hierfür nur ein allgemein zugreifbares Verzeichnis gewählt werden kann, müssen die Dokumente so schnell wie möglich aus diesen öffentlichen Verzeichnissen gelöscht werden. Die Benutzer müssen entsprechend angewiesen werden. Zusätzlich sollten diese Verzeichnisse einmal täglich automatisch gelöscht werden. Der Zeitpunkt muss den Benutzern bekannt gegeben werden und ist so zu wählen, dass zu diesen Zeiten keine Benutzer mit den Scannern arbeiten.
- Scan-to-Mail:
  Hierbei hat der Benutzer beim Scannen die Möglichkeit, eine E-Mail-Adresse oder eine Benutzer-Kennung, der eine E-Mail-Adresse zugeordnet ist, anzugeben. An diese E-Mail-Adresse wird die erzeugte Datei über einen voreingestellten SMTP-Server übermittelt. Da auf diese Weise vertrauliche Informationen anonym das Netz verlassen könnten, sollte darauf geachtet werden, dass keine externen E-Mail-Adressen eingegeben werden können. Besser ist es, auch den SMTP-Server so zu konfigurieren, dass von den netzfähigen Dokumentenscannern keine E-Mails an externe E-Mail-Adressen versendet werden können.

- Scan-to-Print:
  Hier wird das Dokument direkt an einen Drucker gesendet, also die Scanner-Drucker-Kombination als digitaler Kopierer eingesetzt. Sind beide Geräte räumlich voneinander getrennt, besteht die Gefahr, dass während des Scannens die Dokumente unbefugt vom Drucker entfernt werden. Daher sollten die Systeme in diesem Fall möglichst so konfiguriert werden, dass der Ausdruck erst erfolgt, wenn alle Seiten des jeweiligen Dokuments vollständig eingescannt sind. Anderenfalls vergeht zwischen dem Scannen der ersten Seite und dem Abholen am Drucker unter Umständen zu viel Zeit.
- Scan-to-Fax:
  Das Verfahren Scan-to-Fax erlaubt es, eingescannte Dokumente direkt per Fax zu versenden. Hierfür wird beim Scannen eine Fax-Nummer angegeben. Das erzeugte Dokument wird dann entweder über ein integriertes Modem versendet, oder der Scanner baut über das LAN eine Verbindung zu einem Fax-Server auf.
  Beim Einsatz von Scannern, die über eingebaute Fax- oder Modem-Schnittstellen verfügen, müssen besondere Sicherheitsvorkehrungen getroffen werden, damit über diese Schnittstellen keine unerwünschten Kommunikationsverbindungen mit externen Netzen aufgebaut werden. Entsprechende Empfehlungen sind in der Anforderung SYS.4.1.M9 *Netztrennung beim Einsatz von Multifunktionsgeräten* beschrieben.
  Wenn möglich, sollte ein zentraler Fax-Server als Schnittstelle zwischen Scanner und Telefonnetz agieren. In diesem Fall sind insbesondere die Maßnahmen-Empfehlungen, die im Baustein NET.4.3 *Fax* aufgeführt sind, anzuwenden.

Wenn die eingesetzten Komponenten dies unterstützen, sollten die Kommunikationsverbindungen möglichst verschlüsselt werden, um zu erschweren, dass Angreifer die übertragenen Informationen abhören.

Nach dem Scannen dürfen keine Restinformationen auf dem System verbleiben. Die Dokumentenspeicher des Geräts sollten möglichst automatisch gelöscht werden, wenn der Scan-Vorgang abgeschlossen ist. Ist das nicht realisierbar, müssen die Benutzer darauf hingewiesen werden, dass sie die Dokumentenspeicher des Geräts nach der Benutzung manuell löschen müssen, damit nachfolgende Benutzer die eingescannten Informationen nicht einsehen können. Entsprechende Sicherheitsvorkehrungen müssen auch für sonstige Speicherbereiche getroffen werden, die im Rahmen des Scan-Vorgangs verwendet werden, beispielsweise für die dabei benutzten Netzlaufwerke.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Drucker, Kopierer und Multifunktionsgeräte" finden sich unter anderem in folgenden Veröffentlichungen:

[ACSD] Whitepaper Datenschutz und Sicherheit in Druckinfrastrukturen

mc² management consulting GmbH, Mai 2018, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/partner/161219_mc2_drucker_sicherheit.pdf, zuletzt abgerufen am 05.07.2018

[CERT] Informationen zu Schwachstellen und Sicherheitslücken von Druckern und zugehörigen Diensten, Warn- und Informationsdienst

CERT-Bund, https://www.cert-bund.de/search, zuletzt abgerufen am 05.07.2018

[CSE015] Drucker und Multifunktionsgeräte im Netzwerk

BSI-Veröffentlichungen zur Cyber-Sicherheit (BSI-CS 015), Version 1.1., Februar 2017, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_015.html, zuletzt abgerufen am 05.07.2018

[CSE069] Sichere Passwörter in Embedded Devices

Verhinderung von Schwachstellen durch Standardpasswörter und festcodierten Zugangsdaten, BSI-Veröffentlichungen zur Cyber-Sicherheit (BSI-CS 069), Version 1.0, Dezember 2013, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_069.html, zuletzt abgerufen am 05.07.2018

[CUPS] Common Unix Printing System

https://www.cups.org/, zuletzt abgerufen am 05.10.2018

[NIST80053] Security and Privacy Controls for Federal Information Systems and Organizations

NIST Special Publication 800-53, Revision 4, April 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf , zuletzt abgerufen am 30.08.2018

[PP0058] IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std 2600-2008

Operational Environment B, IEEE Std 2600.2-2009, IEEE Computer Society, Information Assurance (C/IA) Committee, BSI-CC-PP-0058-2010, Juli 2010, https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0058.html, zuletzt abgerufen am 05.07.2018

Umsetzungshinweise zum Baustein SYS.4.3 Eingebettete Systeme

1 Beschreibung

1.1 Einleitung

Eingebettete Systeme sind informationsverarbeitende Systeme, die in ein größeres System oder Produkt integriert sind, dort Steuerungs-, Regelungs- und Datenverarbeitungsaufgaben übernehmen und dabei oft nicht direkt vom Benutzer wahrgenommen werden. Eingebettete Systeme finden sich sowohl im Bereich der Hochtechnologie, wie z. B. der Luft- und Raumfahrt, der Medizintechnik, der Telekommunikation und der Automobil-Technik als auch im Consumer- und Haushaltsgerätebereich.

Ein eingebettetes System ist dadurch charakterisiert, dass es aus Soft- und Hardware eine funktionale Einheit bildet, die nur eine definierte Aufgabe erfüllt. Die Software eingebetteter Systeme wird als Firmware bezeichnet und ist zumeist in einem Flash-Speicher, einem EPROM, EEPROM oder ROM gespeichert und durch den Anwender nicht oder nur mit speziellen Mitteln bzw. Funktionen austauschbar. Sie besteht im Wesentlichen aus dem Bootloader, dem Betriebssystem und der Anwendung, wobei spezialisierte Systeme auf ein Betriebssystem verzichten. Eingebettete Systeme sind zwar spezialisierte Geräte, aber im Gegensatz zur reinen Hardwareimplementierung (ASIC) universelle Rechner. Als Plattformen kommen unterschiedliche CPU-Architekturen oder flexible hochintegrierte Field-Programmable-Gate-Array-(FPGA)-Bausteine infrage.

Eingebettete Systeme haben entweder keine Bedienschnittstelle oder nutzen Spezialperipherie, wie z. B. funktionelle Tasten, Drehschalter und auf den jeweiligen Einsatzzweck hin konzipierte Anzeigen. Das Spektrum an Ausgabeeinheiten reicht von einer einfachen Signallampe über LCDs bis hin zu komplexen Cockpit-Anzeigen. Eingebettete Systeme kommunizieren häufig über Datenbusse, die in komplexen Systemen heterogen vernetzt sind. Zusätzlich können über mehrere unterschiedliche und mehrkanalige Ein-/Ausgabeports Peripheriekomponenten, wie Sensoren und Aktoren, angebunden sein. Einige Arten eingebetteter Systeme verfügen über ein Webinterface, über das per Browser Konfigurationseinstellungen vorgenommen werden können.

1.2 Lebenszyklus

Planung und Konzeption

Die Sicherheitseigenschaften bzw. der Rahmen für Sicherheitsfunktionen eines eingebetteten Systems werden bereits durch konzeptionelle Festlegungen eingegrenzt. Bei der grundsätzlichen Entscheidung zur Software-Hardware-Aufteilung sind die unterschiedlichen Sicherheitseigenschaften der Realisierungen in Software oder Hardware zu berücksichtigen (siehe SYS.4.3.M7 *Hardware-Realisierung von Funktionen eingebetteter Systeme*). Zur Erhöhung der Systemstabilität sollte, falls erforderlich, ein hardware- oder softwarebasierter Speicherschutz implementiert werden (siehe SYS.4.3.M15 *Speicherschutz bei eingebetteten Systemen*). Das verwendete Betriebssystem sollte dem aktuellen Stand der Technik entsprechend absturzsicher sein und wenig Angriffspunkte aufweisen (siehe SYS.4.3.M8 *Sicheres Betriebssystem für eingebettete Systeme*). Um die Integrität und Vertraulichkeit von Programmen und Nutzdaten zu sichern, sollten kryptografische Verfahren eingesetzt werden. In einem Hardware-Sicherheitsmodule (Trusted Platform Module) können Schlüssel sicher erzeugt und abgelegt werden und somit Informationen und Komponenten sicher authentisiert werden (siehe SYS.4.3.M9 *Einsatz kryptographischer Prozessoren bzw. Koprozessoren (Trusted Platform Module) bei eingebetteten Systemen*).

Bereits in der Planungsphase sollen Regelungen für den späteren Betrieb festgelegt werden (siehe SYS.4.3.M1 *Regelung des Einsatzes von eingebetteten Systemen*).

Beschaffung

Bevor ein eingebettetes System beschafft wird, müssen dessen Anforderungen ermittelt werden. Die Kriterienliste muss auch die erforderlichen Sicherheitseigenschaften umfassen (siehe SYS.4.3.M4 *Beschaffungskriterien für eingebettete Systeme*). Die beschafften Systeme oder Komponenten müssen genau der Spezifikation entsprechen und der Beschaffungsprozess muss so gestaltet sein, dass er nicht manipulierbar ist (siehe SYS.4.3.M12 *Auswahl einer vertrauenswürdigen Lieferanten- und Logistikkette sowie eines qualifizierten Herstellers für eingebettete Systeme*).

Betrieb

Falls das eingebettete System in rauer Umgebung betrieben wird, sollte es entsprechend geschützt sein (siehe SYS.4.3.M5 *Schutz vor schädigenden Umwelteinflüssen bei eingebetteten Systemen*).

Im operativen Betrieb darf ein eingebettetes System keine Codeelemente enthalten, die nicht Bestandteil der Systemfunktionalität sind (siehe SYS.4.3.M6 *Verhindern von Debugging-Möglichkeiten bei eingebetteten Systemen*).

Ein Mittel im Rahmen der Aufrechterhaltung der Sicherheit eines eingebetteten Systems ist die Überwachung des Systems bzw. seiner Einzelkomponenten. Sicherheitsrelevante Ereignisse im Betrieb eines eingebetteten Systems sind im Rahmen der technischen Möglichkeiten zu dokumentieren (siehe SYS.4.3.M3 *Protokollierung sicherheitsrelevanter Ereignisse bei eingebetteten Systemen*). Darüber hinaus sollten sämtliche Baugruppen eines eingebetteten Systems mit erhöhten Anforderungen an die Verfügbarkeit und Integrität integrierte Selbsttesteinrichtungen besitzen und nutzen (siehe SYS.4.3.M17 *Automatische Überwachung der Baugruppenfunktion (BIST) bei eingebetteten Systemen*).

Aussonderung

Mit der Aussonderung eines eingebetteten Systems dürfen keine vertraulichen Informationen zu Hardware, Software und Daten an Unberechtigte gelangen (siehe SYS.4.3.M11 *Sichere Aussonderung eines eingebetteten Systems*).

Notfallvorsorge

Es sollten Mechanismen vorhanden sein, um die letzte funktionierende Konfiguration und den Auslieferungszustand wiederherzustellen (siehe SYS.4.3.M10 *Wiederherstellung von eingebetteten Systemen).*

Befinden sich auf einem eingebetteten System eingestufte Informationen, muss es eine Notlöschfähigkeit besitzen (siehe ebenfalls SYS.4.3.M10 *Wiederherstellung von eingebetteten Systemen*).

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Eingebettete Systeme" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

SYS.4.3.M1 Regelung des Einsatzes von eingebetteten Systemen [Leiter IT]

Auch im laufenden Betrieb müssen eine Reihe von Sicherheitsanforderungen an den Einsatz von eingebetteten Systemen gestellt werden. Diese Systeme müssen adäquat in das technische und organisatorische Umfeld eingebunden sein, in dem sie eingesetzt werden. Dafür müssen die folgenden organisatorischen Regelungen getroffen werden.

Es sind geeignete personelle Maßnahmen hinsichtlich Schulung, Benutzer-Support, Vertretungsregelungen, Verpflichtungen, Rollenzuteilungen festzulegen bzw. umzusetzen. Die Benutzer sollten im Umgang mit den von ihnen zu bedienenden eingebetteten Systemen bzw. Geräten mit eingebetteten Systemen regelmäßig geschult werden. Handbücher müssen im erforderlichen Umfang und in aktueller Version vorhanden sein.

Es müssen Verantwortliche für Firmware-Aktualisierungen, Wartungs- und Reparaturarbeiten, Protokollauswertung und für die Reaktion auf Sicherheitsverstöße und Fehlfunktionen benannt werden. Bei Ausfällen, Fehlfunktionen und bei Sicherheitsvorfällen muss klar definiert sein, was zu unternehmen ist. Alle Benutzer müssen über die entsprechenden Verhaltensregeln und Meldewege informiert sein.

Es sind Regelungen festzulegen, um die Integrität und Funktionsfähigkeit zu testen. Dabei sind Angaben z. B. zu den Intervallen, zur Vereinbarkeit mit dem Betrieb und zu den Verantwortlichen zu machen. Die Anforderungen an die physische Einsatzumgebung, wie z. B. der Luftfeuchtigkeits- und Temperaturbereich und die Energieversorgung, müssen festgelegt sein. Falls erforderlich sind dafür ergänzende Maßnahmen bei der Infrastruktur zu etablieren.

Für die Benutzer müssen die eingebetteten Systeme durch den Hersteller oder den Administrator so vorkonfiguriert sein, dass eine angemessene Sicherheit und Funktionalität erreicht werden kann. Die Konfiguration eingebetteter Systeme sollte dokumentiert sein, damit sie nach einem Austausch, einer Aktualisierung etc. entsprechend den Verfügbarkeitsanforderungen wieder eingerichtet werden kann.

Bei eingebetteten Systemen mit kryptografischen Anteilen sind weitergehende Regelungen in einem Kryptokonzept festzulegen.

SYS.4.3.M2 Deaktivieren nicht benutzter Schnittstellen und Dienste bei eingebetteten Systemen [Entwickler]

Eingebettete Systeme sind häufig mit einer Vielzahl unterschiedlicher Schnittstellen ausgerüstet. Neben einfachen Ein-/Ausgängen zur Sensorik- und Aktuatorikanbindung finden sich Netzkommunikations-, Bedien- und Anzeigeschnittstellen unterschiedlicher Komplexität.

Physische Schnittstellen

Grundsätzlich sollten nur die benötigten physischen Schnittstellen vorhanden sein. Ist die Hardware vorgegeben und sind nicht benötigte Schnittstellen vorhanden, ist der Zugriff darauf durch bauliche Vorkehrungen zu unterbinden.

Logische Schnittstelle Netzprotokolle

Grundsätzlich dürfen nur benötigte Dienste aktiviert sein. Nicht benötigte Protokolle, die in manchen Konfigurationen standardmäßig vorhanden sind, sind zu deaktivieren, wie z. B. NetBios. Die Dienste für Protokolle, die Daten im Klartext übertragen wie z. B. telnet, http oder ftp sollten deaktiviert sein. Falls notwendig, sind für den entsprechenden Zweck sichere Protokollvarianten bzw. Alternativen einzusetzen. SNMP v1 und v2 Dienste sollten deaktiviert sein.

Logische Schnittstellen Anwendungsebene

Alle in der Applikation nicht genutzten Schnittstellen müssen so konfiguriert werden, dass ein Zugang über diese Schnittstellen auf das eingebettete System nicht möglich ist. Es dürfen nur die Dienste freigeschaltet sein, die für die Aufgabenerfüllung benötigt werden. Bei komplexen Anwendungen mit erforderlicher Authentisierung beim Zugang ist zu überprüfen, für welche Bereiche der Anwendung die Authentisierung gültig ist. Sind z. B. bei einem Webserver die HTML-Seiten über ein Login geschützt, ist noch nicht sichergestellt, dass auch der Zugriff auf Konfigurationsdaten per XML oder JSON darüber abgesichert ist. Um derartige Lücken zu finden, können Webseiten analysiert und Objekte mittels eines HTTP-Clients überprüft werden.

Wird auf dem eingebetteten System ein Betriebssystem genutzt, für das es darauf zugeschnittene automatische Schwachstellenscanner gibt, wie z. B. bei Linux-Systemen, sollten damit Verwundbarkeiten entdeckt und wenn möglich anschließend beseitigt werden. Bei allen Systemen ist mit universellen Portscannern oder Programmen zur Generierung von zufälligen oder spezifizierten Paketen, sogenannten packet buildern, nach Schwachstellen zu suchen.

SYS.4.3.M3 Protokollierung sicherheitsrelevanter Ereignisse bei eingebetteten Systemen

Grundsätzlich sind sicherheitsrelevante Ereignisse im Betrieb des eingebetteten Systems zu dokumentieren. Die technischen Möglichkeiten dazu können bei unterschiedlichen Arten eingebetteter Systeme und deren Umgebung stark variieren. Mögliche Ausprägungen, Funktionalitäten und Parameter sind:

- Protokollierung in einen nicht flüchtigen Speicher, kumulativ durch unterschiedliche Prozesse,
- Datenaufzeichnung in einfachen, formatierten Textdateien, z. B. CSV oder XML,
- Aufzeichnung von Prozessdaten über Datenlogger, im Zeittakt, ereignisgesteuert oder bei Änderungen,
- Strukturierte Speicherung der Ereignisse in einem Datenbanksystem,
- Echtzeitüberwachung mit Information eines Anwenders und der Möglichkeit einer Interaktion zur Laufzeit,
- Protokollierung aller oder konfigurierbarer Zustands- und Transitionsänderungen,
- Variablenablaufverfolgung, z. B. Audit Trails,
- Statistische Auswertung in Berichtsform oder als grafische Darstellung und
- Korrelation, Bewertung.

Soweit möglich, müssen bei eingebetteten Systemen zumindest Sicherheitsverstöße protokolliert werden, wie versuchter und durchgeführter unautorisierter Zugang und Zugriff. Insbesondere sind die Aktivitäten von privilegierten Benutzern zu überwachen, wie z. B. Administratoren. Dadurch kann zwar der Missbrauch von Rechten nicht verhindert werden, es ist aber die Voraussetzung, um gezielt Schwachstellen zu schließen. Daneben wirkt sich die Protokollierung, zumindest hinsichtlich des Risikos entdeckt zu werden, abschreckend auf potentielle Täter aus.

Ist eine elektronische Protokollierung wegen konzeptioneller Einschränkungen durch die begrenzten Ressourcen nicht oder nur sehr begrenzt realisierbar, sollten organisatorische Regelungen geschaffen werden. Zum einen sollten alle Arbeiten an einem eingebetteten System mit Angaben zu Ort, Zeit, Ausführendem sowie Art und Grund der Tätigkeit in einem Logbuch festgehalten werden. Zum anderen sollten alle Ausfälle, offensichtliche Zugangs- und Zugriffsverletzungen und sonstige Auffälligkeiten im Logbuch dokumentiert werden. Die Einträge sollten regelmäßig und anlassbezogen ausgewertet werden.

Sowohl automatisch erzeugte Protokolle als auch Aufzeichnungen durch das Personal sind gegen unerlaubte nachträgliche Veränderung zu schützen. Nur dezidiert Berechtigte dürfen auf die Protokolle zugreifen können. Soweit technisch möglich, sind Vorkehrungen zu treffen, damit die Protokolldaten auch nicht von privilegierten Nutzern gelöscht oder geändert werden können, z. B. durch Speicherung auf nicht wiederbeschreibbaren Datenträgern oder mittels elektronischer Signatur. Datenträger mit Protokolldaten sind sicher zu verwahren und die beteiligten Personen sind über den korrekten Umgang zu belehren.

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich SYS.4.3 *Eingebettete Systeme*.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Eingebettete Systeme".

SYS.4.3.M4 Beschaffungskriterien für eingebettete Systeme [Beschaffer, Leiter IT]

Eingebettete Systeme werden im Zuge der Entwicklung übergeordneter Systeme beschafft oder sie sind Teil von zu beschaffenden übergeordneten Systemen. Zusammen mit der reinen Hardware und Firmware können auch noch zusätzliche Komponenten und Leistungen beschafft werden.

Werden bei der Beschaffung eines eingebetteten Systems Fehler gemacht, so kann dies negative Folgen auf den sicheren Betrieb des übergeordneten Systems bzw. die sichere Durchführung einer Anwendung oder Fachaufgabe haben. Bevor ein eingebettetes System beschafft wird, muss daher eine Anforderungsliste erstellt werden, anhand derer die in Frage kommenden Systeme oder Komponenten bewertet werden. Aufgrund der Bewertung kann dann eine fundierte Kaufentscheidung erfolgen, die sicherstellt, dass das eingebettete System im praktischen Betrieb den Sicherheitsanforderungen genügt. Die Anforderungsliste sollte im Wesentlichen die im Folgenden dargestellten sicherheitsrelevanten Bereiche und Kriterien umfassen.

Organisatorische Randbedingungen

Die folgenden Aspekte sollten bei der Beschaffung berücksichtigt werden:

- Kann ein effektiver Prozess zur Versorgung mit sicherheitsrelevanten Firmwareupdates etabliert werden?
- Informiert der Hersteller die betroffenen Stellen, wenn Sicherheitslücken bekannt werden?
- Bietet der Hersteller einen technischen Kundendienst an, der in der Lage ist, in einer vertretbaren Zeit Auskunft zu geben bzw. Fehlfunktionen zu beheben?
- Bietet der Hersteller Schulungen oder Handbücher zur Sicherheit des eingebetteten Systems an?

Vorgaben aus dem Anwendungsgebiet

Das eingebettete System muss im jeweiligen Anwendungsgebiet geltenden Standards und Normen entsprechen, sowie, falls zutreffend, die Kriterien für eine produktspezifische Zulassung erfüllen. Derartige Zulassungen sind z. B. in den Bereichen Luftverkehr, Straßenverkehr und Medizintechnik üblich.

Materielle Sicherheit

Wird das eingebettete System bei rauen Umweltbedingungen wie Feuchtigkeit, extremen Temperaturen, mechanischen Belastungen und Staub eingesetzt, sollte es physisch robust sein. Es sollten keine oder nur wenige zuverlässige Steckverbindungen vorhanden sein. Empfindliche Komponenten sollten speziell gekapselt und mit Dämpfungsvorrichtungen versehen sein. Auf Bauteile mit beweglichen Komponenten sollte soweit wie möglich verzichtet werden.

Ausfall- und Betriebssicherheit

Abhängig von der geforderten Verfügbarkeit sind an das eingebettete System Anforderungen zur Ausfallsicherheit, zur elektromagnetischen Verträglichkeit, zu internen Überwachungs- und Selbsttestmechanismen und zum Wiederanlauf zu stellen.

Prozessorarchitektur

Die Bandbreite für Prozessorarchitekturen ist sehr groß. Neben Neuentwicklungen kommen, anders als im PC- oder Serverbereich, auch oftmals ältere Architekturen zum Einsatz. Gründe dafür sind die niedrigeren Kosten für den Prozessor selbst und die Möglichkeit das Anwendungsdesign, Programmcode und Entwicklungswerkzeuge sowie Debugtools wiederverwenden zu können. Es ist darauf zu achten, dass die gewählte Prozessorarchitektur geeignet ist, die notwendigen Sicherheitsfunktionen zu realisieren.

Firmware-Speicher

Die Firmware kann sich auf einem ROM, EPROM, EEPROM oder einem Flash-Speicher befinden. Beim Flash-Speicher kann ein Firmware-Update erfolgen, ohne dass der Chip ausgewechselt werden muss. Bei einem ROM muss meistens der gesamte Chip ausgewechselt werden, manchmal auch die gesamte Schaltung. Der Firmware-Speicher soll so realisiert sein, dass zusammen mit dem geplanten Wartungsprozess ein sicheres Update möglich ist.

Betriebssystem und Anwendungssoftware

Wird das eingebettete System zusammen mit einem Betriebssystem und/oder Anwendungssoftware beschafft, muss festgelegt werden, welche sicherheitsrelevanten Merkmale diese aufweisen sollen, z. B. hinsichtlich

- Sicherem Bootprozess
- Nutzung sicherer Kommunikationsprotokolle
- Sicherer Installation und Aktualisierung
- Absicherung von Zugang und Zugriff
- Benutzer- und Rechteverwaltung
- Protokollierung
- Alarmierung
- Integritätsschutz

Entwicklungsumgebung

Falls mit dem eingebetteten System auch eine Entwicklungsumgebung mit beschafft wird, ist darauf zu achten, dass diese neben der erforderlichen Funktionalität auch die nötigen Sicherheitseigenschaften aufweist. Beispielsweise dürfen bei den Schritten zur Codeerzeugung keine ungewollten Funktionen oder Hintertüren entstehen und die Entwicklungsumgebung sollte über Mechanismen verfügen, um selbst gegen Manipulationen geschützt werden zu können. Wenn möglich sollten zertifizierte Werkzeuge beschafft werden.

Kriterien ohne direkten Sicherheitsbezug

Kriterien wie z. B.

- Stromverbrauch,
- Grad der Integration,
- Signallaufzeiten,
- Erfüllung von Echtzeitanforderungen,
- Platzbedarf und
- Kosten

haben keine direkte Auswirkung auf die Informationssicherheit. Allerdings muss beachtet werden, dass die sicherheitsrelevanten Kriterien unter Umständen anders bewertet werden, wenn die oben genannten Kriterien optimiert werden.

Prüfsiegel und Zertifizierungen

Für eingebettete Systeme bzw. generell für elektronische Komponenten existieren zahlreiche Prüfsiegel und Zertifizierungen. Wenn Anforderungen hierzu in die Beschaffungskriterien mit einfließen, muss beachtet werden, dass es auch gefälschte, qualitativ minderwertige und irreführende Ausprägungen davon gibt.

SYS.4.3.M5 Schutz vor schädigenden Umwelteinflüssen bei eingebetteten Systemen [Entwickler, Planer]

Eingebettete Systeme dürfen nicht aufgrund von schädigenden Umwelteinflüssen ausfallen oder versagen. Eingebettete Systeme sind entsprechend ihrer vorgesehenen Einsatzart und des vorgesehenen Einsatzorts vor Staub, Verschmutzungen, Hitze, Feuchtigkeit etc. zu schützen. Das eingebettete System kann in ein umschließendes, robustes Gehäuse eingebaut werden oder an einer geschützten Stelle im Inneren des umgebenden Systems oder der tragenden Infrastruktur verbaut werden.

Falls Systeme wegen einer notwendigen Luftzufuhr nicht ausreichend ummantelt werden können, sind Luftfilter vorzusehen. Diese müssen hinsichtlich Dimensionierung und Filterleistung für die vorgesehenen Einsatzarten geeignet sein.

Die Vorkehrungen zum Schutz gegen schädigende Umwelteinflüsse sind bereits in der Planung zu berücksichtigen.

SYS.4.3.M6 Verhindern von Debugging-Möglichkeiten bei eingebetteten Systemen [Entwickler]

Verbreitete Vorgehensweisen zum Debugging (also zum Diagnostizieren und Beseitigen von Fehlern) von eingebetteten Systemen sind In-Circuit-Emulation (ICE) und On-Chip-Debugging (OCD). ICE-Geräte ersetzen den eigentlichen Controller auf dem Zielsystem durch eine Hardware, in der die notwendigen Analysefunktionen eingebaut sind. Das später eingesetzte Zielsystem besitzt diese Zusatzfunktionen nicht und stellt somit keine ungewollten Debugging-Möglichkeiten bereit. Aufgrund zeitlicher, technischer oder finanzieller Zwänge kommt allerdings vermehrt OCD zum Einsatz. Dabei werden Debugging-Möglichkeiten auf den Serienbausteinen selbst implementiert. OCD kann somit in den Programmablauf eingreifen, z. B. um Werte aus Registern oder einem Trace-Speicher auszulesen oder zusätzliche kleine Monitoring-Programme auszuführen, die Debug-Informationen sammeln und nach außen geben.

Bei eingebetteten Systemen befindet sich die zu untersuchende Software meist nicht auf demselben Rechner wie der Debugger. Daher wird Remote Debugging verwendet, d. h. der Entwickler startet auf dem eingebetteten System eine Applikation, mit der sich der Debugger auf dem Entwicklungssystem z. B. über Ethernet oder RS232 verbindet.

Wird z. B. der GNU Debuggers (GDB) genutzt, führt das eingebettete System einen GDB-Server aus, bei dem sich der GDB-Client auf dem Entwicklungssystem anmeldet. Der Client bzw. der Programmierer übergeben dem Server auf dem eingebetteten System Anweisungen zum Untersuchen der Applikation. Der Server setzt die Anweisungen um und schickt die Resultate an das Entwicklungssystem zurück.

Soweit möglich, sind die aus der Hard- und Softwareentwicklung im System oder der Software installierten Hilfsmittel zum Debugging vollständig aus dem Entwurf für die Serie zu entfernen. Aus dem Produktionscode von Software sind alle Codeelemente zu entfernen, die nicht Bestandteil der Systemfunktionalität sind. Dazu zählen z. B. Breakpoints und nicht genutzter Code. Wird On-Chip-Debugging genutzt, ist sicherzustellen, dass Debugging-Funktionen nicht durch Unberechtigte genutzt oder aktiviert werden können. Im Bereich der Hardware ist sicherzustellen, dass keine Eingabeschnittstellen für Testsignale und Messpunkte zum Anschluss von Analysatoren aktiviert bzw. für Unberechtigte nutzbar sind.

SYS.4.3.M7 Hardware-Realisierung von Funktionen eingebetteter Systeme [Beschaffer, Entwickler, Planer]

Wird ein eingebettetes System entworfen, wird festgelegt, welche Funktionen auf einem programmierbaren Prozessor ablaufen sollen und welche unmittelbar in Hardware implementiert werden sollen. Die potenzielle Bandbreite bei der Hardware-Software-Partitionierung ist groß. An einem Ende der Skala stehen universell programmierbare Mehrzweck-Prozessoren (General Purpose Processor, GPP), wie sie auch im Bereich der Arbeitsplatzrechner eingesetzt werden. Am anderen stehen hochspezialisierte digitale Hardware-Systeme, die nur ein Programm ausführen (Single Purpose Processor, SPP). Einen Mittelweg zwischen voll programmierbaren Prozessoren und reinen Hardware-Implementierungen stellen programmierbare Prozessorkerne mit anwendungsspezifischem Befehlssatz (Application Specific Instruction set Processor, ASIP) dar. Es sind Prozessoren, deren Befehlssatz für bestimmte Anwendungsarten, z. B. digitale Signalverarbeitung oder Steuerungsfunktionen optimiert wurde.

Auch bei den Hardware-Implementierungen gibt es verschiedene Abstufungen. Bei den Optionen, um integrierte Schaltkreise zu implementieren, reicht die Bandbreite von Chips, die individuell für bestimmte Kunden entworfen und hergestellt werden ("Application Specific Integrated Circuit", ASIC) bis zu Chips, die zwar für spezielle Aufgaben entwickelt werden, aber so allgemein gehalten sind, dass sie in einer Vielzahl unterschiedlicher Produkte eingesetzt werden können ("Application Specific Standard Product", ASSP). Dazu kommen einige Mischformen wie z. B. Chips, die auf Kundenwunsch hin vom Hersteller angepasst werden ("Customer Specific Standard Product", CSSP), Chips mit einigen vorimplementierten Elementen (englisch: "structured ASIC") und Chips mit einem vordefinierten Bereich und einem für Kundenkonfigurationen freien Bereich (englisch: "platform ASIC").

Weit verbreitet, insbesondere zur Prototypenentwicklung sind programmierbare ASICs. Die wichtigsten Vertreter dieser Technik sind Field Programmable Gate Array (FPGA) und Complex Programmable Logic Device (CPLD). Beides sind integrierte Schaltkreise, in die eine logische Schaltung programmiert werden kann, wobei damit gemeint ist, dass die Funktionsstruktur des Schaltkreises definiert wird und nicht, dass zeitliche Abläufe festgelegt werden. CPLDs weisen im Vergleich zu FPGAs eine wesentlich einfachere Struktur auf. Sie besitzen kein feinmaschiges Array von Logikblöcken und Flip-Flops, sondern nur eine konfigurierbare Schaltmatrix, die verschiedene Eingangssignale zu verschiedenen Ausgangssignalen verbinden kann. Ein CPLD ist sofort nach dem Einschalten betriebsbereit, ebenso wie ein nur einmal programmierbares FPGA. Rekonfigurierbare FPGA mit static random-access memory (SRAM)-basierenden Zellen benötigen erst einen Ladezyklus für die Konfiguration. FPGA Bausteine sind größer als CPLD Bausteine und haben einen höheren Stromverbrauch.

Programmierbare Logik-Bausteine können außerhalb des Zielsystems oder, falls die entsprechenden Schnittstellen vorhanden sind, auch innerhalb des Zielsystems programmiert werden. Sie werden oft verwendet, um einen Prototypen zu entwickeln. Im produktiven System werden sie meist durch ASICs ersetzt. Eine Weiterentwicklung stellen rekonfigurierbare ASICs dar, die sich während der Laufzeit umprogrammieren und so an aktuelle Erfordernisse anpassen können.

Die unterschiedlichen Sicherheitseigenschaften der Realisierungen in Software oder Hardware sind beim Entwurf eines eingebetteten Systems zu berücksichtigen und mit den jeweiligen Sicherheitsanforderungen in Einklang zu bringen. Festverdrahtete Algorithmen, z. B. als ASIC oder FPGA, stellen einerseits einer Manipulation der Funktionalität höhere Hürden entgegen als typische softwarebasierte Implementationen, andererseits sind sie weniger flexibel und erlauben im Allgemeinen keine nachträgliche Integration zusätzlicher Sicherheitsmechanismen. Werden die Sicherheitsmechanismen allerdings von Anfang an beim Entwickeln der Hardware einbezogen, lassen sie sich effizient realisieren. Auch parallele Prozesse können sehr gut in Hardware realisiert werden, z. B. kann die virtuelle Maschine für Java nicht als Software, sondern durch einen Java-Prozessor als Hardware realisiert werden.

Wird entschieden die Funktionen in Hardware zu realisieren, ist zu beachten, dass ASICs und FPGAs unterschiedliche Stärken und Schwächen hinsichtlich der Informationssicherheit aufweisen. Bei ASICs gibt es Risiken im Entwurf und der Fertigung. Um zu verhindern, dass ein Angreifer nicht gewollte Funktionen oder Hintertüren einbaut oder vertrauliche Informationen ausspäht, sollten die Chips entsprechend getestet werden und die Entwicklungs- und Herstellungskette sollte vertraulich sein (siehe SYS.4.3.M12 *Auswahl einer vertrauenswürdigen Lieferanten- und Logistikkette sowie eines qualifizierten Herstellers für eingebettete Systeme*). Bei FPGAs wird die Schaltung zunächst in einer Hardwarebeschreibungssprache formuliert, wobei auch fremdes geistiges Eigentum einfließen kann. Mittels spezieller Entwurfswerkzeuge wird die Schaltung synthetisiert und implementiert. Anschließend werden die Konfigurationsdaten auf das FPGA übertragen. Es ist darauf zu achten, dass eventuell verwendetes fremdes geistiges Eigentum vertrauenswürdig ist, die Entwurfstools nicht manipuliert sind und die Daten in einer gesicherten Umgebung auf das FPGA übertragen werden. Falls erforderlich, ist die Übertragung zu verschlüsseln.

Bei den Logik-Bausteinen gibt es auch Unterschiede in der elektromagnetischen Verträglichkeit. FPGAs sind empfindlicher gegenüber Teilchenstrahlung und elektromagnetischen Wellen als ASICs.

Wird ein eingebettetes System nicht selbst entwickelt, sondern als ganzes oder in Komponenten beschafft, gelten die genannten Empfehlungen entsprechend.

SYS.4.3.M8 Sicheres Betriebssystem für eingebettete Systeme [Beschaffer, Entwickler, Planer]

Für eingebettete Systeme gibt es sehr viele verschiedene Betriebssysteme. Einige hochspezialisierte Systeme benötigen gar kein Betriebssystem, andere sind eingebettete Betriebssysteme, die aus Mehrzweckbetriebssystemen heraus entwickelt wurden, z. B. Embedded Linux Varianten oder Windows CE. Dazwischen existieren zahlreiche unter verschiedensten Aspekten für eingebettete Systeme spezialisierte (Echtzeit) Betriebssysteme, wie z. B. RTOS oder VxWorks.

Auf der einen Seite wird von den Merkmalen eines Mehrzweckbetriebssystems in der Regel nur ein Teil benötigt, z. B.

- sind Adressraumdeskriptoren nur notwendig im Falle von Systemen, die eine Adressraumisolation erfordern,
- spielen Dateisystem und Dateienverwaltung bei einigen Einsatzbereichen keine Rolle,
- benötigen ROM-basierte Systeme, auf denen lediglich automatisiert ein einziges Programm abläuft, keine prozessbezogene Benutzerrechteverwaltung,
- kann auf eine aufwändige Verwaltung von Prozesszuständen verzichtet werden, wenn der Ablaufplan für die Prozesse vorab festgelegt wird und sich nicht mehr ändert,
- wird eine Ereignisverwaltung nur bei ereignisgesteuerten und/oder präemptiven Systemen benötigt.

Auf der anderen Seite können für eingebettete Systeme Anforderungen vorliegen, die mit Mehrzweckbetriebssystemen nicht oder schwierig umzusetzen sind, z. B.

- harte Echtzeit-Zusicherungen,
- weitergehende Mechanismen zur Fehlererkennung und -behandlung sowie
- Zwang, ressourcenschonend zu arbeiten.

Wird ein eingebettetes System konzipiert oder beschafft, ist daher darauf zu achten, dass das Betriebssystem und seine Konfiguration für den vorgesehenen Betrieb unter den vorgegebenen Bedingungen, einschließlich der Sicherheitsanforderungen, geeignet sind. Das Betriebssystem ist gemäß den spezifischen Sicherheitsanforderungen des Gesamtsystems zu konfigurieren. Die Sicherheitsanforderungen sollten in der Sicherheitsrichtlinie und im Software-Entwicklungsprozess dokumentiert sein. Grundsätzlich sollte das Betriebssystem nur die für die vorgesehene Aufgabe notwendigen Dienste, Funktionen und Eigenschaften aufweisen. Es dürfen nur Treiber genutzter Schnittstellen eingebunden werden.

Sicherheitsaspekte eines Betriebssystems sollten in unterschiedlichen Bereichen und Betriebsphasen berücksichtigt werden. Das System sollte in einem sicheren planvollen Prozess entwickelt werden. Die Systemarchitektur sollte den Kernel, von Paketen wie Middleware, Netz-Protokollen und Applikationen trennen. Es sollte möglich sein, diese Komponenten zu ergänzen und zu verändern, ohne dass der Kernel geändert werden muss. Das kann mit einem sogenannten Mikrokern (englisch: Microkernel) erreicht werden. Ein Mikrokern verfügt im Gegensatz zu einem monolithischen Kernel nur über grundlegende Funktionen zur Speicher- und Prozessverwaltung und zur Synchronisation und Kommunikation. Er ist somit weniger angreifbar und auch absturzsicherer.

Wie in SYS.4.3.M14 *Abgesicherter und authentisierter Bootprozess bei eingebetteten Systemen* und SYS.4.3.M9 *Einsatz kryptographischer Prozessoren bzw. Koprozessoren (Trusted Platform Module) bei eingebetteten Systemen,* muss das Betriebssystem Mechanismen zum sicheren Booten und zur sicheren Programmausführung bereitstellen. Dazu muss es in der Lage sein, ein Trusted Plattform Module (TPM) zu integrieren und zu nutzen.

Während des laufenden Betriebs sollte das System Angriffe abwehren können. Dies kann auch dadurch erreicht werden, dass zusätzliche Sicherheitsprodukte installiert und genutzt werden. Im Ruhezustand darf es für einen Angreifer nicht möglich sein auf Daten zuzugreifen.

Ein Chipkartenbetriebssystem sollte insbesondere folgende Mechanismen und Dienste bereitstellen:

- Benutzeridentifizierung und Authentikation mittels PIN, PUK oder biometrischen Verfahren
- Zugriffskontrolle mit Rechteverwaltung
- Gegenseitige Authentisierung von Chipkarten und anderen Rechnern
- Sichere Datenübertragung ("Secure Messaging") gegen Ausforschung und Manipulation
- Bereitstellung von Signier- und Verschlüsselungsfunktionen im gesicherten Zusammenwirken mit Kryptoterminals
- I/O-Kontrolle aller Schnittstellen durch das Betriebssystem gegen unerlaubte Zugriffe
- Gewährleistung der Interferenzfreiheit einzelner Anwendungen: verschiedene Anwendungen dürfen sich nicht gegenseitig beeinflussen
- Möglichkeit die Chipkarte zu deaktivieren

SYS.4.3.M9 Einsatz kryptografischer Prozessoren bzw. Koprozessoren bei eingebetteten Systemen [Beschaffer, Entwickler, Planer]

Bei eingebetteten Systemen kann ein zusätzlicher Mikrocontroller verwendet werden, um kryptographische Algorithmen und Protokolle abzuarbeiten, z. B. um Hash-Funktionen und Signaturverifikation zu beschleunigen. Dieser kommuniziert mit dem System-Mikrocontroller über die Gültigkeit der Firmware-Authentifizierung.

Ab einem hohen Schutzbedarf der Vertraulichkeit oder der Integrität ist diese Kommunikation gegen Hardwareattacken widerstandsfähig zu machen, indem

- die Leiterbahnen auf den inneren Lagen der Leiterplatte verlaufen,
- dynamische Signale (Impulse) verwendet werden, um dem Haupt-Mikrocontroller einen erfolgreichen Bootvorgang zu signalisieren und
- nach Möglichkeit mehrere Pins mit unterschiedlichen dynamischen Signalen verwendet werden.

Das Prinzip von Trusted Computing wird durch die Trusted Computing Group (TCG) anhand einer Reihe von Ankern für Vertrauen in einem System definiert. Wichtige Anker im Zusammenhang mit eingebetteten Systemen sind die Root of Trust for Measurement (RTM), die Root of Trust for Storage (RTS), sowie die Root of Trust for Reporting (RTR). Die Aufgabe der RTM ist es, als Anker für die Erhebung der Konfiguration einer Plattform zu dienen. Sie wird noch initialisiert, bevor das Betriebssystem gestartet wird. Beim Starten des RTM misst diese die Konfiguration der Hardware-Plattform, während diese initialisiert wird, sowie die erste gestartete Software-Komponente. Danach ist sie beendet und führt keine weiteren Aktionen mehr durch. Es lassen sich also alle Änderungen an der Plattform oder der zuerst gestarteten Software-Komponente, etwa dem Bootloader, erkennen. Veränderungen an danach gestarteten Software-Komponenten, wie dem Betriebssystem oder Applikationen, werden damit nicht erkannt. Der Mechanismus für diesen Zweck verlangt, dass jede Software-Komponente die jeweils als nächste zu startende Software-Komponente misst und die Korrektheit feststellt. Somit entsteht eine sogenannte "Trusted Chain of Measurement". Die RTM stellt hierbei den Beginn der Kette dar. Die Messwerte werden mittels kryptografischer Funktionen zu Hashwerten reduziert und in gesicherten Speicherbereichen als Referenzwerte abgelegt. Die Root of Trust for Storage dient dazu, Daten sicher zu speichern und die Root of Trust for Reporting dazu sicherheitsrelevante Informationen korrekt wiederzugeben.

Eingebettete Systeme sind zwar spezialisierte Geräte aber im Gegensatz zur reinen Hardwareimplementierung (ASIC) universelle Rechner. Deshalb ist es auch bei eingebetteten Systemen sinnvoll und nötig, Gerätekonfiguration, Software und Daten genauer zu prüfen, ob sie verändert wurden. Die Informationen in Systemen mit hohen Anforderungen an die Integrität sollten durch den Einsatz kryptographischer Prozessoren oder Hardware-Sicherheitsmodule (Trusted Platform Module) durch das verarbeitende System authentisiert werden. Bei eingebetteten Systemen mit Kommunikationsfunktionen sollte es möglich sein, Geräte sicher zu identifizieren und mit diesen Geräten vertrauenswürdig zu kommunizieren. Darüber hinaus sollen verlässlich Zustandsinformationen über ein Gerät eingeholt werden können. Insbesondere darf es dabei nicht möglich sein, dass ein Gerät die Identität eines anderen Gerätes duplizieren kann oder dass ein Gerät Statusinformationen eines anderen Gerätes anstelle seiner selbst ausliefert.

Vertrauensanker und darauf basierende Überprüfungen können bei eingebetteten Systemen meist einfacher realisiert werden als bei einem Standard-Rechner, beispielsweise wenn Firmware zusammen mit dem Read-Only Dateisystem squashfs genutzt wird und Konfiguration und Zustand getrennt von der Software gespeichert werden. Ein RTM kann dann die komplette Firmware messen, bevor sie gestartet wird, und es muss keine komplexe Vertrauenskette aufgebaut werden. Betriebssysteme müssen dadurch nicht angepasst werden und das Laufzeitverhalten ändert sich nicht. Auch ist es nicht nötig, jede Software-Komponente einzeln zu messen. Es kann das gesamte Firmware-Image gemessen und gegen einen Referenzwert abgeglichen werden.

SYS.4.3.M10 Wiederherstellung von eingebetteten Systemen

Wenn eine neue Version der Software auf ein eingebettetes System geladen wird, muss es möglich sein, das System vollständig auf den Zustand vor dem Beginn der Änderung zurückzuführen. Falls dies nicht durch systemeigene Mechanismen möglich ist, muss vorher sichergestellt sein, dass die bisherige funktionsfähige Softwareversion zur Verfügung steht und bei missglücktem Update manuell wieder eingespielt werden kann. Bei erhöhten Anforderungen an die Verfügbarkeit sollte es jederzeit möglich sein, die letzte funktionierende Konfiguration und den Auslieferungszustand wieder herzustellen. Dazu ist vor jeder Änderung der vollständige Konfigurationszustand zu speichern. Es ist auch zu erwägen, mit der letzten funktionierenden Konfiguration fertig konfigurierte Rückfallsysteme vorzuhalten. Diese könnten im Fehlerfall die veränderten, mit der neuen Version nicht mehr korrekt arbeitenden Systeme, schnell ersetzen.

SYS.4.3.M11 Sichere Aussonderung eines eingebetteten Systems [Leiter IT]

tbd: Hier kann noch Text ergänzt werden. Das BSI nimmt hierzu gerne Vorschläge aus der Community entgegen.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

SYS.4.3.M12 Auswahl einer vertrauenswürdigen Lieferanten- und Logistikkette sowie qualifizierter Hersteller für eingebettete Systeme [Beschaffer, Leiter IT] (CI)

Schaltungen und Chips werden häufig von unterschiedlichen Institutionen funktional beschrieben und physisch produziert. Sowohl viele bekannte Chiphersteller als auch hochspezialisierte Kleinunternehmen sind sogenannte "fabless companies". Sie entwickeln Schaltungen und Chips, produzieren diese aber nicht selbst. Die Fertigung erfolgt durch darauf spezialisierte Firmen, sogenannte "silicon foundries", in der ganzen Welt, zumeist außerhalb von Europa. Die gefertigten Chips werden von dort direkt an die Kunden oder den Großhändler ausgeliefert. Auch die bekannten Distributoren sind weltweit verstreut.

Der Systemhersteller muss deshalb sicherstellen, dass die hergestellten Bauteile absolut genau der Spezifikation entsprechen, keine verdeckten Zusatzfunktionen enthalten und alle Qualitätsanforderungen einhalten. Bei der Lagerung, beim Zwischenhandel und während des Transports darf es nicht möglich sein, die programmierbaren Logikbausteine zu manipulieren oder Komponenten zu tauschen. In der Logistikkette sind dahingehend wirksame Kontrollen durchzuführen. Die Hersteller und Logistikunternehmen sollten nach anerkannten Standards zertifiziert sein.

Hersteller und deren Subunternehmer sollten nachweisen, dass sie vertrauenswürdig sind Hard- und Software herzustellen. Der Nachweis ist zu dokumentieren. Eine Hersteller-Qualifizierung muss regelmäßig erneuert werden.

Bei allen mit der Entwicklung und Instandsetzung betrauten Fremdfirmen dürfen keine zu schützenden Informationen über das eingebettete System und die sich darauf befindlichen Daten nach außen gelangen. Hierzu ist ein Sicherheitskonzept zu planen und umzusetzen. Die Mitarbeiter sind geeignet zu schulen und zu sensibilisieren. Es sind Regelungen zur Weitergabe von Informationen zu treffen. Vorfälle sind zu melden und zu kategorisieren. Nach einem Vorfall sind die Regelungen zu überprüfen und im Falle von Lücken oder zu weichen Forderungen entsprechend anzupassen. Seitens des Auftraggebers ist sicherzustellen, dass Fremdfirmen die Anforderungen des Sicherheitskonzeptes umsetzen.

SYS.4.3.M13 Einsatz eines zertifizierten Betriebssystems [Beschaffer, Entwickler, Planer] (CI)

Für Systeme mit hohem oder sehr hohem Schutzbedarf sollte geprüft werden, ob es erforderlich ist, das Betriebssystem zu evaluieren, z. B. nach ISO 15408 (siehe [15408]). Statt ein ganzes Betriebssystem komplett zu evaluieren, ist es ratsam, das BSI-Schutzprofil "Operating System Protection Profile (OSPP)" zu beachten (siehe [OSPP]).

SYS.4.3.M14 Abgesicherter und authentisierter Bootprozess bei eingebetteten Systemen [Beschaffer, Entwickler, Planer] (CI)

Der Bootprozess eines eingebetteten Systems darf nicht kompromittierbar sein. Es darf nicht möglich sein, von unauthentisierten Bootmedien zu starten oder Daten zu übernehmen. Es muss sichergestellt werden, dass die verwendete Software von einer autorisierten Instanz geschrieben oder freigegeben wurde.

Der Bootprozess sollte abgesichert sein, indem der Bootloader die Integrität des Betriebssystems überprüft und es nur dann lädt, wenn es als korrekt eingestuft wurde. Das Betriebssystem sollte nur starten, wenn der Bootloader durch eine Rückwärtsprüfung als vertrauenswürdig bestätigt wurde.

Dies kann mittels asymmetrischer Kryptografieverfahren überprüft werden. Aktuell kommen dafür z. B. Elliptic Curve Digital Signature Algorithm (ECDSA) und RSA (Rivest, Shamir und Adleman) in Kombination mit SHA (secure hash algorithm) in Frage. Von der Original-Software wird ein Hashwert berechnet und mit dem privaten Schlüssel des Herausgebers signiert. Überprüft wird er mit dem öffentlichen Schlüssel. Die Authentizität des öffentlichen Schlüssels muss über PKI-Verfahren sichergestellt werden.

Ein sicherer Bootprozess sollte in Stufen ausgeführt werden. Zuerst muss ein minimaler, bei der Herstellung fest in das ROM programmierter Bootloader (ROM-Loader) ablaufen. Dieser muss über einen vorher fest einprogrammierten kryptographischen Schlüssel verfügen, um seinerseits die digitale Signatur des nächsten Boot-Loaders zu verifizieren. Diesen anfänglichen Verifikationsschlüssel muss die Hardware bereitstellen, er kann über eine einmal programmierbare Sicherung in das ROM integriert oder in einem lokalen Trusted Platform Module (TPM) abgelegt werden, siehe hierzu auch SYS.4.3.M9 *Einsatz kryptographischer Prozessoren bzw. Koprozessoren (Trusted Platform Module) bei eingebetteten Systemen*. Der ROM-Loader lädt einen weiteren Boot Loader mit mehr Funktionen, der dann das Betriebssystem oder wiederum einen Loader startet. Die Signatur muss ebenfalls im hardwaregeschützten Bereich gespeichert sein, weil mit dem Signaturschlüssel geprüft wird, ob die Komponenten in der zweiten (und ggf. weiteren) Stufe des Boot-Ablaufs echt sind. Die auszuführende Software kann mehrstufig geladen werden, wobei die Signatur der jeweils nächsten Stufe von der aktuellen Stufe geprüft wird. Scheitert eine Signaturverifikation oder wird eine Verbindung unterbrochen, muss angenommen werden, dass der sichere Zustand verletzt ist.

Oft werden in eingebetteten Systemen keine x86 basierten Computer mit BIOS (Basic Input/Output System) oder UEFI (Unified Extensible Firmware Interface), sondern ARM basierte Geräte mit dem Universal Boot Loader (U-Boot) eingesetzt. Die TCG bezieht sich in ihren Spezifikationen aber insbesondere auf eine Implementierung des RTM im pre-BIOS bzw. im UEFI in denen der RTM besonders zu schützen ist. Auf ARM Plattformen gibt es in vielen Fällen allerdings bereits ohne Trusted Computing die Möglichkeit eines gesicherten Starts von Software, wie z. B. ARM Secure Boot oder von nur einmal beschreibbarem Speicher, der auch gegen physische Manipulationen geschützt ist.

SYS.4.3.M15 Speicherschutz bei eingebetteten Systemen [Beschaffer, Entwickler, Planer] (CI)

Wenn in einem eingebetteten System mehrere Softwarekomponenten ablaufen, kann es sinnvoll sein, diese zu separieren. Soll nicht für jede Komponente ein eigener Mikrocontroller verwendet werden, kann dies auch durch Speicherschutztechniken erreicht werden. Ziel des Speicherschutzes ist es, Arbeitsspeicher so zu strukturieren und Bereiche so zu separieren, dass ein Programmierfehler oder Absturz eines einzelnen Programms nicht die Stabilität anderer Programme oder des Gesamtsystems beeinträchtigt. Programme sollen daran gehindert werden, auf den Speicherbereich anderer Programme zuzugreifen.

Um Daten auf dem eingebetteten System mit erhöhten Anforderungen an die Integrität und Verfügbarkeit besser abzusichern, sollen Speicherschutzmechanismen bereits im Entwurf des Systems berücksichtigt werden. Es ist eine Realisierungsform zu wählen, die das benötigte Sicherheitsniveau gewährleistet und den Einsatzerfordernissen des eingebetteten Systems nicht entgegensteht. Die beiden grundsätzlichen Realisierungen sind Hardware-Speicherschutz und Software-Speicherschutz.

Hardwareseitig kann eine Speicherverwaltungseinheit ("Memory Management Unit", MMU) oder eine einfachere Speicherschutzeinheit ("Memory Protection Unit", MPU) den Speicherschutz unterstützen. Mit einer MMU ist es möglich, mehrere virtuelle Prozessoren auf einem physischen Prozessor zu vereinen, der durch das Betriebssystem verwaltet wird. Jedes Programm kann seinen eigenen virtuellen Mikrocontroller erhalten und die Ressourcen des physischen Mikrocontrollers lassen sich flexibel zuordnen. MMU sind standardmäßig Bestandteil von Servern, PCs und modernen Smartphones, in kleinen eingebetteten Systemen sind sie normalerweise nicht vorhanden.

Bei einer MPU nutzen alle Programme den gemeinsamen Adressraum des physischen Speichers. Die MPU überwacht, auf welchen Speicherbereich ein Programm zugreift. Ist ein Zugriff nicht erlaubt, so kann das Betriebssystem den Speicherzugriff abfangen, bevor die Daten im Speicher verändert werden. Theoretisch könnte jedes Programm einen separaten, sogenannten Schutzraum bekommen. Aufgrund der meist knappen Ressourcen bei eingebetteten Systemen sollten aber nur so viele Schutzräume etabliert werden wie nötig, z. B. zwei, um die Ausführung von vertrauenswürdigen Programmen gegenüber der von nicht-vertrauenswürdigen zu trennen.

Bei hardwarebasiertem Speicherschutz werden die Speicherzugriffe durch die Hardware überwacht. Dieser Ansatz funktioniert auch, wenn die nicht vertrauenswürdige Softwarekomponente direkt in einer Maschinensprache programmiert wurde. Die überwachten Speicherzugriffe umfassen nicht nur die Lade- und Speicherbefehle, sondern auch Maschinenbefehle, die vor ihrer Ausführung geladen werden. Schlägt die Überprüfung beim Speicherzugriff fehl, so unterbricht die Hardware den Ablauf des aktuellen Maschinenprogramms und wechselt zu einer Unterbrechungsbehandlung in die Systemsoftware. Welche Rechte für welchen Speicherbereich gelten, wird durch spezielle, zugriffsgeschützte Register beschrieben. Eine für hardwarebasierten Speicherschutz geeignete CPU benötigt eine Hardware, die einen privilegierten und einen unprivilegierten Betriebsmodus unterstützt.

Beim softwarebasierten Speicherschutz werden die Speicherzugriffe nicht implizit durch die Hardware überprüft, sondern vorab explizit durch die Software. Die Überprüfung kann dabei zum Teil zum Übersetzungszeitpunkt stattfinden oder auch zur Laufzeit, zum Beispiel durch automatisch generierte Überprüfungen.

SYS.4.3.M16 Tamper-Schutz bei eingebetteten Systemen [Planer] (CI)

Für eingebettete Systeme ist ab einem hohen Schutzbedarf für die Vertraulichkeit oder Integrität ein Tamper-Schutz-Konzept zu planen und umzusetzen.

Ein umfassender Tamper-Schutz besteht aus den drei Funktionsbereichen: "Verhinderung", "Erkennung und Nachweis" und "Reaktion und Abwehr". In der Fachliteratur werden dafür meist die englischen Begriffe "tamper resistance", "tamper evidence" und "tamper response" verwendet. Tamper-Schutz kann Infrastrukturelemente, Hardware und Software betreffen. Bei letzterem kommen kryptografische Mechanismen zum Einsatz (siehe SYS.4.3.M9 *Einsatz kryptographischer Prozessoren bzw. Koprozessoren (Trusted Platform Module) bei eingebetteten Systemen*).

Um Tamper-Angriffe auf Infrastrukturelemente und Hardware zu verhindern, ist es notwendig, ein einbruchssicheres ("tamper resistant") System herzustellen, das auf Grund seiner Konstruktion nicht unautorisiert verändert werden kann. Für den Fall, dass ein Angreifer frei über ein System verfügen kann, ist ein vollkommener Schutz nicht möglich. Allerdings können durch bauliche und technische Vorkehrungen die für ihn zu überwindenden Hürden sehr hoch gesetzt werden. Ein solches System zu realisieren kann aufwändig sein und das Resultat ist möglicherweise ein kompliziertes, wenig flexibles System. Bevor dieser Weg eingeschlagen wird, sollte daher analysiert und bewertet werden, welcher Aufwand aufgrund des Schutzbedarfs des Systems erforderlich und sinnvoll ist. Verschiedene Konstruktionselemente können dazu beitragen, die Einbruchsicherheit zu erhöhen. Beispiele sind spezielle Schrauben wie Torx-TR mit einem Stift in der Profilmitte, der verhindert, dass diese Schraube mit einem normalen Torx- oder Schlitz-Schraubendreher zu drehen ist, oder Ummantelungen, Schutzschichten und passive oder aktive Metallleitungen. Eingebettete Systeme können auch bautechnisch so mit einer Umgebung verbunden werden, dass sie nur sehr schwer herausgelöst werden können und zusammen mit der Umgebung nicht transportabel wären, z. B. durch Metall oder Beton.

Deutlich aufwändiger ist es Vorkehrungen zu treffen, die Einbrüche erkennen und dokumentieren ("tamper evidence"). Diese erlauben es, Modifikationen an einem System automatisiert zu erkennen oder durch externe Prüfer die Korrektheit eines Systems zu bestätigen. Beispiele für derartige Mechanismen sind Plomben und Siegel, aktiv getriebene Metallleitungen mit Sensoren, die auf Licht, Druck oder Widerstands- und Kapazitätsänderungen reagieren.

Als Reaktion auf einen Tamper-Angriff ("tamper response") kann ein Alarm an eine übergeordnete Managementeinheit abgesendet werden. Zudem sollten schützenswerte Daten des Systems möglichst automatisch gelöscht werden. Abhängig vom Schutzbedarf der Daten sollten verschiedene Optionen betrachtet werden. Einfach zu realisieren ist die Energieversorgung des RAM zu unterbrechen, allerdings könnte ein Angreifer mit entsprechender Ausrüstung und Expertise die Daten rekonstruieren. Außerdem betrifft dies nur einen Teil der Daten eines eingebetteten Systems. Eine verbreitete Methode besteht darin, das RAM mehrfach zu überschreiben.

SYS.4.3.M17 Automatische Überwachung der Baugruppenfunktion [Beschaffer, Planer] (IA)

Mit einem eingebauten Selbsttest (Built-In Self Test, BIST) kann sich ein Schaltkreis, ein Gerät oder System selbst testen. Dazu werden Testsignale erzeugt, an die zu testende Komponente angelegt und die Antwortsignale ausgewertet, meist durch Vergleich mit vorgegebenen richtigen Antwort-Signalen. Bei einem BIST werden die Funktionen der Testumgebung (Automatic Test Equipment, ATE) wie Testsignalgeneratoren oder Auswerteeinheiten ganz oder teilweise direkt auf dem Chip implementiert. Dies führt zu verkürzten Signalpfaden, ungewollte Kopplungen werden verringert und die Signalintegrität auf den Testleitungen wird verbessert.

Ein Selbsttest kann im normalen Betrieb, während der Initialisierungsphase, während Ruhezeiten, vor dem Ausschalten oder außerhalb der Betriebsumgebung als funktionaler diagnostischer Test der Soft- und Hardware erfolgen. Beispiele für verschiedene Arten von BIST sind:

- Logik-BIST: Ein Pseudomuster- oder Pseudozufallsgenerator erzeugt ein Zufallsmuster mit dem die logischen Zustände überprüft werden. Entsprechen die Ausgangszustände nicht der Wahrheitstabelle, dann arbeitet die Logik fehlerhaft.
- Speicher-BIST: Mittels eines Testkreises werden Speicherbausteine ausgelesen und deren Ausgangszustände mit einem vorgegebenen Muster verglichen.
- Signaturanalyse: Signale aus Schaltungsteilen werden über einen längeren Zeitraum gesammelt und daraus eine Signatur ermittelt. Diese wird mit einem Sollwert verglichen und daraus die korrekte oder fehlerhafte Funktion der Gesamtschaltung gefolgert.
- Boundary Scan Test: Mit Hilfe zusätzlicher Zellen, sogenannten Latches, werden Signale über vordefinierte Pfade von außen in die zu testende Schaltung injiziert. Die Signale aus der Schaltung, die an Pins des Schaltkreises anliegen, können über den Scanpfad erfasst werden. Im Normalbetrieb sind die Latches passiv, es besteht kein funktionaler Unterschied zum ursprünglichen Schaltkreis.
- Analog- und Mixed-Signal-BIST: Zuerst werden die digitalen Komponenten mit Hilfe einer digitalen BIST-Schaltung vollständig verifiziert. Dann werden der Analog-Digital-Converter (ADC) und der Digital-Analog-Converter (DAC) verifiziert. Anschließend können andere Komponenten verifiziert werden, indem sie zwischen DAC und ADC mit Hilfe von analogen Multiplexern platziert werden.

Sämtliche Baugruppen des eingebetteten Systems mit erhöhten Anforderungen an die Verfügbarkeit und Integrität sollten integrierte Selbsttesteinrichtungen besitzen. Tests müssen während des Einschaltvorgangs und in angemessenen zeitlichen Intervallen während des Betriebs die Integrität des Systems prüfen. Soweit möglich, sollten die Selbsttestfunktionalitäten auch Sicherheitsfunktionen bzw. Sicherheitseigenschaften der Baugruppe überprüfen.

Bei Komponenten mit höherem Schutzbedarf, z. B. in kritischen Steuerungssystemen, sollte regelmäßig die Integrität der Speicher und I/O-Komponenten in Rahmen des BIST geprüft werden. Bestehende BIST-Funktionen sind, falls möglich, um die erforderlichen Funktionen zu ergänzen.

SYS.4.3.M18 Widerstandsfähigkeit eingebetteter Systeme gegen Seitenkanalangriffe [Beschaffer, Entwickler] (C)

Durch einen oder mehrere der nachfolgend beschriebenen Mechanismen ist das eingebettete System entsprechend seinem Schutzbedarf gegenüber Seitenkanalangriffen zu härten. Diese Maßnahme beschreibt die möglichen Angriffsformen und Gegenmaßnahmen zu deren Abwehr.

Arten von Seitenkanalangriffen

Wenn IT-Systeme Kryptografie einsetzen, findet dies nicht in einem abstrakten mathematischen System statt, sondern wird durch programmierte integrierte Schaltkreise geleistet. Diese interagieren gemäß den Naturgesetzen mit ihrer Umgebung und geben dadurch Informationen über die verarbeiteten Daten preis. Ein Seitenkanalangriff ist eine kryptoanalytische Vorgehensweise, um Kryptovariablen zu kompromittieren, indem die physische Implementierung eines Kryptosystems in einem Gerät oder in einer Software ausgenutzt wird. Seitenkanalangriffe sind zeitaufwändig. Sie erfordern den vollständigen Zugang zum Gerät, der häufig nur in ausgebautem Zustand gegeben ist.

Seitenkanalangriffe lassen sich grundsätzlich in nicht-invasive und invasive Angriffe unterteilen.

Nicht-invasive Angriffe

Nicht-invasive oder passive Angriffe beobachten physische Parameter wie z. B. Stromverbrauch, Laufzeiten und Speichernutzung während relevante kryptografische Codeanteile ablaufen und schließen daraus auf geschützte Daten, wie Schlüssel und Passwörter.

Analyse des Energieverbrauchs

Simple Power Analysis ist eine Methode, bei der der Energieverbrauch eines Mikroprozessors während kryptologischer Berechnungen direkt aufgezeichnet wird. Der Energieverbrauch variiert abhängig von den jeweils ausgeführten Mikroprozessorbefehlen. Er gibt somit Aufschluss über die ausgeführten Operationen sowie über den Schlüssel. Durch den Vergleich von Energieverbrauchsmessungen einer kryptologischen Operation können Muster wie etwa DES-Runden oder RSA-Operationen entdeckt werden und Rückschlüsse auf den geheimen Schlüssel gezogen werden.

Die Differential Power Analysis (DPA) setzt zusätzlich statistische Methoden ein. Damit kann ein Angreifer auch bei komplexeren Verarbeitungsarten wie Parallelität oder Speicherdirektzugriff (Direct Memory Access, DMA) an sein Ziel kommen.

Analyse des Zeitverhaltens

Rechenzeitangriffe nutzen den Umstand, dass Kryptosysteme in Abhängigkeit vom Schlüssel für unterschiedliche Klartexte oder Chiffrate leicht unterschiedliche Ausführzeiten benötigen. Wenn ein Angreifer Zugriff auf das System hat, kann er durch Ausprobieren von verschiedenen Eingaben mittels Laufzeitanalyse den Schlüssel nach und nach rekonstruieren. Rechenzeitangriffe sind sowohl gegen Chipkarten als auch gegen Software-Implementierungen veröffentlicht worden.

Mikroarchitekturelle Angriffe (z. B. Cache-Angriffe, Instruktions-Cache-Angriffe)

Die Angriffe richten sich gegen software-implementierte Kryptosysteme. Die Idee des Angriffs basiert darauf, dass beim Ausführen kryptologischer Software Daten und Routinen schlüsselabhängig in den Cache bzw. Instruktionscache geladen werden. Ziel ist es; die mikroarchitekturellen Prozessoreigenschaften/-funktionen auszunutzen und so an den Schlüssel zu gelangen.

Weitere Ansatzpunkte für nicht-invasive Seitenkanalangriffe sind Rechenfehler in fehlerhaften Mikroprozessoren, elektromagnetische Abstrahlung und Schallemissionen. Unterschiedliche Seitenkanalangriffsarten können auch kombiniert werden.

(Semi-) Invasive Angriffe

Als invasiv oder aktiv werden Angriffe bezeichnet, bei denen in ein Gerät physisch eingegriffen wird. Nachdem eine kurzfristige Fehlfunktion der entscheidenden Sicherheitsfunktionen erzeugt wurde, können die fehlerhaften Ergebnisse untereinander und / oder mit dem korrekten Ergebnis verglichen werden. Dies ist für einen Angreifer besonders interessant, wenn kryptografische Algorithmen ablaufen, z. B. bei der Signaturerzeugung. Aus den gewonnenen Daten kann auf den geheimen Schlüssel geschlossen werden. Die Fehlfunktion kann im Moment der Ausführung des kritischen Codes hervorgerufen werden, z. B. können Spannungsschwankungen wie Spikes (Impulsspitzen) oder Glitches (Störimpulse) erzeugt werden. Das System kann auch elektromagnetischer Strahlung oder extremen Temperaturen ausgesetzt werden. Diese Attacken werden in der Fachliteratur auch als "semi-invasiv" bezeichnet, da zwar physisch eingegriffen, der Chip aber nicht zerstört oder dauerhaft beschädigt bzw. manipuliert wird.

Weitere Verfahren für Seitenkanalangriffe sind Gegenstand der aktuellen Forschung, z. B. photonische Seitenkanalangriffe durch photonische Emissionsanalyse oder photonische Fehlerinduktion.

Abwehrmöglichkeiten gegenüber Seitenkanalangriffen

Da jedes physische System mit seiner Umgebung interagiert, ist ein hundertprozentiger Schutz gegen Seitenkanalangriffe nicht möglich. Ziel ist es daher, deren Erfolgswahrscheinlichkeit herabzusetzen. Widerstandsfähigkeit gegen Seitenkanalangriffe bedeutet also nicht, dass diese bzw. deren Erfolg absolut unmöglich gemacht wird, sondern dass sie erschwert werden. Das wesentliche Konzept dazu besteht darin, die erforderliche Anzahl von Messungen für den Erfolg einer Attacke so zu erhöhen, dass ein Restrisiko getragen oder anderweitig abgefangen werden kann.

Maskieren der Daten

Ziel ist es, den Zusammenhang zwischen den tatsächlichen geheimen Daten und der vom Angreifer gemessenen Seitenkanalinformation zu verwischen. Die Zwischenergebnisse werden mit einem geheimen Maskenwert randomisiert. Dadurch wird der Zusammenhang zwischen den tatsächlichen Daten und der gemessenen Seitenkanalinformation gebrochen. Die Maskierung kann sowohl auf Algorithmusebene als auch auf der Gatterebene erfolgen.

Bei der softwaretechnischen Lösung werden nach einem Maskierungsschema Masken spezifiziert und durch den Algorithmus auf alle Zwischenresultate angewendet. Auf der Gatterebene können spezielle Logikstile, wie z. B. mCMOS, MDPL oder iMDPL, verwendet werden, die ein einheitliches Stromprofil während des Verschlüsselungs- und Entschlüsselungsvorganges herstellen sollen. Weit verbreitete Hardware basierend auf CMOS Logik erfüllt diese Bedingungen nicht und ihre Stromaufnahme hängt stark von den verarbeiteten Daten ab.

Verrauschen oder Filtern des Stromverbrauchs

Ziel ist es, im Rauschen das Signal zu verstecken, das die Seitenkanalinformation beinhaltet. Typische Ansätze sind das vorhandene Rauschen durch den Einsatz von Rauschgeneratoren zu verstärken oder die Amplitude des Signals, das die Seitenkanalinformation trägt zu verringern. Letzteres kann durch einen möglichst konstanten, datenunabhängigen Stromverbrauch des zu schützenden Geräts weitgehend erreicht werden. Es können auch künstliche Stromrauschquellen hinzugefügt und es kann auch willkürlich Strom verbraucht werden.

Härten gegen Laufzeitattacken

Ziel ist es, das zeitliche Verhalten des Systems zu verschleiern, während es sensible Daten verarbeitet. Dazu können Dummy-Operationen oder zufällige Wartezyklen in den Programmablauf eingefügt werden, z. B. bei einem kryptographischen Algorithmus.

Ein wirkungsvoller Schutz gegen verschiedene Laufzeitattacken und Power-Analysen ist mit Randomisierungstechniken, dem sogenannten Blinding zu erreichen. Dabei wird zu Zwischenwerten ein Zufallswert addiert oder multipliziert. Abhängig davon, mit welchen Größen in einem kryptografischen Algorithmus dies geschieht, wird von Basis-Blinding, Modulus-Blinding oder Exponenten-Blinding gesprochen. Sie verhindern, dass einem Angreifer Zwischenwerte des modularen Exponentiationsalgorithmus zur Kenntnis kommen, der bei kryptografischen Verfahren eingesetzt wird.

Härten gegen (Semi-) Invasive Angriffe

Angriffe durch differentielle Fehleranalyse können erkannt bzw. qualifiziert vermutet werden, wenn Berechnungsschritte redundant durchgeführt werden und die Ergebnisse nicht übereinstimmen. Filter können eingebaut werden, um Unregelmäßigkeiten in der Spannungsversorgung auszugleichen bzw. die Toleranz gegenüber gestörten Taktsignalen zu erhöhen. Optische Eingriffe mit Lasern können mittels Lichtdetektoren und speziellen Schutzschichten erkannt bzw. erschwert werden. Eingebettete Systeme können auch mit Speicherelementen ausgestattet werden, deren Inhalt sich im Normalbetrieb nicht ändert. Wird eine Änderung erkannt, liegt der Verdacht auf einen Angriff mittels differentieller Fehleranalyse nahe. Dafür wird zusätzlicher Speicherplatz bzw. zusätzliche Rechenzeit benötigt.

3 Weiterführende Informationen

3.1 Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Eingebettete Systeme" finden sich unter anderem in folgenden Veröffentlichungen:

[15408] ISO/IEC 15408-2:2008

Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security funktional components, International Oranziation for Standardization (Hrsg.), ISO/IEC JTC 1/SC 7, August 2008

[ICSSK] ICS-Security-Kompendium

Testempfehlungen und Anforderungen für Hersteller von Komponenten, Bundesamt für Sicherheit in der Informationstechnik (BSI), November 2014 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security-Kompendium-Hersteller.html, zuletzt abgerufen am 05.10.2018

[ICSSKfH] ICS-Security-Kompendium

Testempfehlungen und Anforderungen für Hersteller von Komponenten, Bundesamt für Sicherheit in der Informationstechnik (BSI), November 2014 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security-Kompendium-Hersteller.html, zuletzt abgerufen am 05.10.2018

[OSPP] Operating System Protection Profile (OSPP)

Bundesamt für Sicherheit in der Informationstechnik (BSI), Jnui 2010 https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0067.html, zuletzt abgerufen am 14.05.2018

Umsetzungshinweise zum Baustein SYS.4.4 Allgemeines IoT-Gerät

1 Beschreibung

1.1 Einleitung

In diesem Baustein werden Geräte mit Funktionalitäten aus dem Bereich Internet of Things (IoT) betrachtet. Dies sind im Gegensatz zu "klassischen" IT-Systemen "intelligente" Gegenstände, die zusätzliche "smarte" Funktionen enthalten. IoT-Geräte werden in der Regel an Datennetze angeschlossen, in vielen Fällen drahtlos, und können sogar oft auf das Internet zugreifen und darüber erreicht werden. Hierdurch können sie Auswirkungen auf die Informationssicherheit des gesamten Informationsverbunds haben.

IoT-Geräte können in Institutionen vorhanden sein, weil sie durch Mitarbeiter oder Externe mitgebracht werden, z. B. Smartwatches oder Wearables. In vielen Institutionen werden aber auch IoT-Geräte beschafft und betrieben, z. B. Geräte wie Brand-, Gas- und andere Warnmelder, Kaffeemaschinen oder Elemente der Gebäudesteuerung wie Kameras und HVAC (Heating, Ventilation and Air Conditioning).

Generell kann zwischen direkt adressierbaren IoT-Geräten und IoT-Geräten, die eine zentrale Steuereinheit voraussetzen, unterschieden werden. Direkt adressierbare Geräte werden in der Regel mit einer eigenen IP-Adresse an ein Datennetz angeschlossen und können autark agieren oder durch eine zentralen Steuereinheit verwaltet werden. Es gibt aber auch IoT-Geräte, die ausschließlich direkt mit Steuereinheiten kommunizieren, z. B. über Funknetze wie Bluetooth oder ZigBee, und somit nicht direkt an Datennetze angeschlossen werden. Die Reichweite dieser Funkverbindungen kann, wenn vorgesehen, über ein separates, vermaschtes Netz vergrößert werden, indem jedes Gerät mit jedem Gerät eine Funkverbindung aufbaut.

1.2 Lebenszyklus

Planung und Konzeption

In der Planungs- und Konzeptionsphase soll der Einsatz der IoT-Geräte innerhalb der Institution definiert werden. Hierbei muss der Einsatz von IoT-Geräten sorgfältig dokumentiert und geplant werden (siehe *SYS.4.4.M6 Aufnahme von IoT-Geräten in die Sicherheitsrichtlinie der Institution* sowie *SYS.4.4.M7 Planung des Einsatzes von IoT-Geräten*).

Beschaffung

Um geeignete IoT-Geräte für die Institution auswählen zu können, müssen die Geräte hierzu bezüglich der Sicherheitskriterien, z. B. Update-Funktionen, Update-Prozess oder Authentisierung-Varianten, gesichtet werden (siehe *SYS.4.4.M1 Einsatzkriterien für IoT-Geräte*). Anderweitige Kriterien, wie z. B. organisatorische Randbedingungen oder materielle Sicherheit, sollten ebenso berücksichtigt werden (siehe *SYS.4.4.M8 Beschaffungskriterien für IoT-Geräte).*

Umsetzung

Nachdem Planung und Beschaffung abgeschlossen sind, müssen die Geräte anhand der Sicherheitsanforderungen installiert und konfiguriert werden. Bevor die IoT-Geräte installiert werden, sollten Einsatzumgebung und Stromversorgung geprüft werden, um den sicheren Betrieb der Geräte zu gewährleisten (siehe *SYS.4.4.M21 Einsatzumgebung und Stromversorgung).* Bei der Installation sollten verschiedene Einstellungsmöglichkeiten berücksichtigt und vorgenommen werden, die z. B. den Zugriff auf die Geräte zu regeln und abzusichern (siehe *SYS.4.4.M10 Sichere Installation und Konfiguration von IoT-Geräten).*

Betrieb

Bevor IoT-Geräte in Betrieb genommen werden, sollte deren Einsatz, anhand der Prüfung der Installations- und Konfigurationsdokumentation, freigegeben werden. Während des laufenden Betriebs ist neben der Protokollierung wichtiger und sicherheitsrelevanter Ereignisse auch die Überwachung des Netzverkehrs der IoT-Geräte von Wichtigkeit (siehe *SYS.4.4.M17 Überwachung des Netzverkehrs von IoT-Geräten* sowie *SYS.4.4.M18 Protokollierung sicherheitsrelevanter Ereignisse bei IoT-Geräten*).

Aussonderung

Wenn IoT-Geräte ausgesondert werden, sollte sichergestellt sein, dass keine wichtigen oder sensitiven Daten auf den IoT-Geräten zurück bleiben (S*YS.4.4.M20 Geregelte Außerbetriebnahme von IoT-Geräten*).

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Allgemeines IoT-Gerät" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

SYS.4.4.M1 Einsatzkriterien für IoT-Geräte

Viele auf dem Markt vorhandene IoT-Geräte weisen wenig bis gar keine Sicherheitsmechanismen auf und enthalten teilweise diverse Schwachstellen. Damit IoT-Geräte in Institutionen eingesetzt werden können, müssen sie ein Minimum an Sicherheitskriterien erfüllen.

Die Geräte müssen Update-Funktionen besitzen und der Hersteller muss einen Update-Prozess anbieten. Wenn IoT-Lösungen ein unzureichendes oder fehlendes Patchmanagement mitbringen, können keine Schwachstellen behoben werden. Ersatzweise müssten die Sicherheitslücken anderweitig abgeschirmt werden. Dies kann sehr aufwendig werden und auch das ganze Nutzungskonzept eines IoT-Gerätes ad absurdum führen.

Ein weiteres großes Problem bei IoT-Geräten sind voreingestellte und teilweise sogar fest codierte Standard-Passwörter. Geräte, bei denen keine Authentisierung möglich ist oder bei denen Standard-Passwörter nicht geändert werden können, dürfen nicht eingesetzt werden.

Wenn sich im laufenden Betrieb herausstellt, dass in einem Gerät Zugangsdaten fest codiert sind, muss es vom Netz genommen werden. Dies gilt auch, wenn Zugangsmöglichkeiten mit Missbrauchspotential erst später bekannt werden, etwa zusätzliche Schnittstellen für den Fernzugriff (wie z. B. Telnet) oder Masterpasswörter des Herstellers, und sich diese nicht zuverlässig abschalten oder verhindern lassen.

SYS.4.4.M2 Authentisierung

In Unternehmen und Behörden sollten nur IoT-Geräte eingesetzt werden, die eine Authentisierung ermöglichen. Diese muss aktiviert sein. Werden hierfür Passwörter verwendet, müssen sichere Passwörter benutzt werden. Hierfür sollte es eine Passwort-Richtlinie geben (siehe auch ORP.4 Identitäts- und Berechtigungsmanagement). Grundsätzlich müssen die gewählten Passwörter komplex genug sein, geheim gehalten und regelmäßig gewechselt werden. Voreingestellte Passwörter müssen bei Inbetriebnahme geändert werden, sofern möglich, bevor ein Gerät online geht. Zusätzlich empfiehlt sich die Verwendung von alternativen Authentisierungsmechanismen, wie z. B. zertifikatsbasierte Authentisierung. Leider bieten nicht alle IoT-Geräte entsprechende Möglichkeiten.

SYS.4.4.M3 Regelmäßige Aktualisierung

Während des Betriebes der IoT-Geräte muss regelmäßig überprüft werden, ob neue Updates/Patches für die eingesetzten IoT-Geräte und zugehörige Komponenten wie Sensoren oder Management-Systeme zur Verfügung stehen, z. B. über einschlägige Webseiten mit Sicherheitsinformationen oder beim Hersteller. Vorhandene Patches und Updates müssen zeitnah installiert werden oder anderweitige Sicherheitsmaßnahmen ergriffen werden, wenn keine Patches zur Verfügung stehen. Im äußersten Fall dürfen die Geräte bei bekannten, nicht behebbaren Schwachstellen nicht mehr betrieben werden. Zusätzlich zur Firmware der IoT-Geräte sollten auch Drittkomponenten, wie z. B. Administrations- oder Managementsoftware, auf Aktualität überprüft werden. Falls neue Updates verfügbar sind, sind diese zeitnah einzuspielen. Generell muss darauf geachtet werden, dass Patches und Updates nur aus vertrauenswürdigen Quellen bezogen werden, in erster Linie ist dies der jeweilige Hersteller selbst.

SYS.4.4.M4 Aktivieren von Autoupdate-Mechanismen

Automatische Update-Mechanismen (Autoupdate) stellen eine regelmäßige Aktualisierung der Software auf den IoT-Geräten sicher. In kritischen Umgebungen oder bei hohen Ansprüchen vor allem an die Verfügbarkeit sollte jedoch die Durchführbarkeit einer manuellen Wartung vorrangig geprüft werden, da automatische, ungetestete Updates unerwartete Auswirkungen oder gar Ausfälle zur Folge haben können.

Auch bei automatischen Updates ist es wichtig, dass diese aus vertrauenswürdigen Quellen bezogen werden und der Download geeignet abgesichert ist, etwa durch entsprechende Authentisierung und eine Transportverschlüsselung (z. B. HTTPS). Es darf nicht möglich sein, dass ein Angreifer durch den Missbrauch von Updates (etwa durch Man-in-the-Middle-Angriffe) Zugriff auf die IoT-Geräte erlangen kann.

SYS.4.4.M5 Einschränkung des Netzzugriffs

Um den Netzzugriff der IoT-Geräte auf ein Minimum zu beschränken, sollten mittels einer Firewall nur zuvor definierte ein- und ausgehende Verbindungen erlaubt werden. Insgesamt sind ausgehende Verbindungen zu minimieren, sowohl im internen Netz als auch zum Internet hin.

Für ausgehende Verbindungen sollten die validen Ziele einer Verbindung, wie z. B. Update-Server des Herstellers, Speicherort der Videodaten und Managementsystem, konfiguriert werden. Ob und wie IoT-Geräte die Server des Herstellers kontaktieren müssen, um die Verfügbarkeit von Updates zu prüfen, sollte in der Produktdokumentation recherchiert werden.

Sollte eine Erreichbarkeit der IoT-Geräte von außen (d. h. aus dem Internet eingehend) erforderlich sein, so sollte dies nur mit hinreichender Authentisierung erfolgen.

Die Freigabe von extern eingehenden Verbindungen im Router sollte vermieden werden. Bei der Inbetriebnahme von IoT-Geräten muss außerdem sichergestellt werden, dass die UPnP-Funktion an allen Routern deaktiviert ist.

Am Perimeter (Router, Firewall) darf auf keinen Fall der Zugriff über Telnet (Port 23) von außen freigegeben werden.

Am Perimeter darf der Zugriff über SSH (Port 22) nur freigegeben werden, wenn dieser mit hinreichend sicheren individuellen Passwörtern geschützt ist. Eine höhere Sicherheit wird erreicht, wenn der Zugriff nicht über Benutzername und Passwort, sondern durch ein Softwarezertifikat gesichert wird. Auch hier sollte nach außen nicht einer der standardmäßig verwendeten Ports (22, 1022, 2222) genutzt werden, sondern ein Zufallswert im Bereich 10000 bis 65535.

Gegebenenfalls kann der Zugriff zusätzlich durch die Verwendung von VPN weiter abgesichert werden. Bei der Verwendung von VPN ist darauf zu achten, dass ausreichend starke kryptografische Verfahren und entsprechende Schlüssellängen verwendet werden.

Es empfiehlt sich auch, die IoT-Geräte in einem separaten physischen Netzbereich bzw. innerhalb eines separaten Virtual Local Area Networks (VLANs) zu betreiben, um ein laterales Ausbreiten bei einer Kompromittierung der IoT-Geräte zu vermeiden.

Basierend auf einem gepflegten Assetmanagement-System können folgende Maßnahmen ungewollte Kommunikation verhindern:

- Verkehrskontrolle an Netzübergängen, z. B. durch Regelwerke auf Firewalls und Access Control Lists (ACLs) auf Routern
- Restriktive Konfiguration des Routings auf IoT-Geräten und Sensoren, insbesondere die Unterdrückung von Default-Routen
- Signaturen auf Intrusion-Prevention-Systemen (IPS)
- Zusammenfassung der IoT-Geräte und Sensoren in einem eigenen Netzsegment, welches ausschließlich mit dem Netzsegment für das Management kommunizieren darf
- Konfiguration von Virtual Private Networks (VPNs) zwischen den IoT-Geräten und Sensor-Netzen und den Management-Netzen
- Deaktivierung der UPnP-Funktion an allen Routern

Abhängig vom Einsatzort der IoT-Geräte sollte ein physischer Zugriffsschutz umgesetzt werden. Dieser schützt nicht nur vor Vandalismus, sondern auch vor einer Veränderung der Konfiguration, die häufig durch das Zurücksetzen auf den Werkszustand ermöglicht wird.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Allgemeines IoT-Gerät".

SYS.4.4.M6 Aufnahme von IoT-Geräten in die Sicherheitsrichtlinie der Institution

Die Sicherheitsvorgaben für IoT-Geräte ergeben sich aus der institutionsweiten Sicherheitsrichtlinie. Ausgehend von der allgemeinen Richtlinie müssen die Anforderungen für den gegebenen Kontext konkretisiert werden und in einer Sicherheitsrichtlinie für die jeweilige Gruppe von IoT-Geräten zusammengefasst werden. In diesem Zusammenhang ist zu prüfen, ob neben der institutionsweiten Sicherheitsleitlinie weitere übergeordnete Vorgaben wie IT-Richtlinien, Passwortrichtlinien oder Vorgaben zur Internet-Nutzung zu berücksichtigen sind.

Die Sicherheitsrichtlinie muss allen Fachverantwortlichen und anderen Personen, die an der Beschaffung und dem Betrieb der IoT-Geräte beteiligt sind, bekannt sein und Grundlage für deren Arbeit sein. Wie bei allen Richtlinien sind ihre Inhalte und ihre Umsetzung im Rahmen einer übergeordneten Revision regelmäßig zu prüfen.

Die Sicherheitsrichtlinie sollte das generell zu erreichende Sicherheitsniveau spezifizieren und grundlegende Festlegungen treffen. Um die Übersichtlichkeit zu verbessern, kann es sinnvoll sein, für verschiedene Einsatzgebiete gesonderte Sicherheitsrichtlinien zu entwickeln.

Bei der Erstellung einer Sicherheitsrichtlinie ist es empfehlenswert, so vorzugehen, dass zunächst ein Maximum an Forderungen und Vorgaben für die Sicherheit der IoT-Geräte aufgestellt wird. Diese können anschließend den tatsächlichen Gegebenheiten angepasst werden. Idealerweise wird so erreicht, dass alle notwendigen Aspekte berücksichtigt werden. Für jede im zweiten Schritt verworfene oder abgeschwächte Vorgabe sollte der Grund für die Nicht-Berücksichtigung dokumentiert werden. Während die Sicherheitsrichtlinie für IoT-Geräte formuliert wird, ist es auch wichtig, eine Balance zwischen Sicherheit und Funktionalität zu finden.

SYS.4.4.M7 Planung des Einsatzes von IoT-Geräten

Eine grundlegende Voraussetzung dafür, dass IoT-Geräte sicher betrieben werden können, ist ein angemessenes Maß an Planung im Vorfeld. Die Planung betrifft dabei nicht nur Aspekte, die klassischerweise mit dem Begriff Informationssicherheit verknüpft werden, sondern auch Aspekte der physischen, materiellen und funktionalen Sicherheit ebenso wie normale betriebliche Aspekte, die Anforderungen im Bereich der Sicherheit nach sich ziehen.

In einem Grobkonzept sollten beispielsweise folgende typische Fragestellungen behandelt werden:

- Welche Aufgaben sollen die IoT-Geräte erfüllen? Auf welche Dienste muss von den IoT-Geräten zugegriffen werden können? Gibt es besondere Anforderungen an die Verfügbarkeit der IoT-Geräte oder an die Vertraulichkeit oder Integrität der gespeicherten oder verarbeiteten Daten?
- Welche Anforderungen an die IoT-Geräte ergeben sich aus den allgemeinen Anforderungen?

Es wird empfohlen, ein oder mehrere generische Anforderungsprofile (beispielsweise "Allgemeine IoT-Geräte", "Kameras" oder "IoT-Geräte zur Gebäudesteuerung") zu erstellen, die bei konkreten Planungen als Grundlage dienen können.

Die folgenden Teilkonzepte sollten bei der Planung berücksichtigt werden:

- Authentisierung: Welche Art der Benutzer-Authentisierung soll genutzt werden? Ist es erforderlich, Benutzer einzurichten?
- Administration: Wie sollen die IoT-Geräte administriert werden? Werden alle Einstellungen lokal vorgenommen oder sollen bzw. können die IoT-Geräte in ein zentrales Administrations- und Konfigurationsmanagement integriert werden?
- Netzdienste und Netzanbindung: Die Netzanbindung der IoT-Geräte sollte geplant werden. Hier sollten vor allem die notwendigen Einschränkungen und Überwachungsmaßnahmen geplant werden.
- Protokollierung: Auch bei IoT-Geräten spielt die Protokollierung eine wichtige Rolle, beispielsweise bei der Diagnose und Behebung von Störungen oder bei der Erkennung und Aufklärung von Angriffen. Sinnvollerweise sollte bereits in der Planungsphase festgelegt werden, wie und zu welchen Zeitpunkten Protokolldaten ausgewertet werden sollen.

Alle Entscheidungen, die in der Planungsphase getroffen wurden, müssen so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können. Dabei ist zu beachten, dass meist andere Personen neben dem Autor diese Informationen auswerten müssen. Daher ist auf passende Strukturierung und Verständlichkeit zu achten.

SYS.4.4.M8 Beschaffungskriterien für IoT-Geräte [Beschaffungsstelle, Informationssicherheitsbeauftragter (ISB)]

Schon bei der Produktwahl sollten nicht nur das Preis-Leistungs-Verhältnis betrachtet werden, sondern auch Aspekte der Informationssicherheit. Hier spielt vor allem die angebotene Funktionalität des Produktes und die Unterstützung durch den Herstellers eine wichtige Rolle. Der ISB sollte auch bei Beschaffungen von Geräten, die keine offensichtliche IT-Funktionalität haben, beteiligt werden, um einschätzen zu können, ob diese in die Sicherheitskonzeption der Institution eingebunden werden müssen.

Grundsätzlich ist von der Verwendung von IoT-Geräten mit einem Cloud-Konzept abzuraten. In diesem Falle fließen sensible Daten über Dritte (z. B. Kamerahersteller) und werden dort für einen Zugriff über das Internet gespeichert. Auch die Verwendung von WLAN – insbesondere in kritischen Einsatzbereichen – sollte vermieden werden, sofern dies die Einsatzbedingungen erlauben.

Ein grundlegendes Ziel zum sicheren Einsatz von IoT-Geräten ist die Minimierung der Angriffsfläche. Um diese von Beginn an gering zu halten, empfiehlt es sich, IoT-Geräte zu beschaffen, auf denen nur die für den konkreten Einsatzzweck erforderlichen Dienste/Ports vorhanden sind. Alternativ sollte es möglich sein, nicht benötigte Dienste zu deaktivieren. Ist auch dies nicht möglich, müssen entsprechende Einschränkungen bei der Inbetriebnahme auf Netzebene (z. B. Firewall) vorgenommen werden, um die Verwendung von nicht benötigten Diensten zu verhindern.

Um eine vertrauliche Übertragung von Nutz- und Konfigurationsdaten zu gewährleisten, sollte das IoT-Gerät ein auf Verschlüsselung basierendes Protokoll (z. B. SSL/TLS bzw. SSH) unterstützen. Bietet das Produkt selbst keine Verschlüsselung, muss dies bei der Inbetriebnahme, z. B. über ein Virtual Private Network (VPN), flankierend umgesetzt werden.

Sofern der Einsatzzweck dies erfordert, sollten die IoT-Geräte ein differenziertes Rollen-/Rechtekonzept für unterschiedliche Benutzer bereitstellen.

Weiterhin muss der Hersteller für einen hinreichend langen Zeitraum die Bereitstellung von Patches bzw. Updates gewährleisten. Dies wird meist mit End Of Service (EOS) beschrieben – nicht zu verwechseln mit End Of Life (EOL), was das Ende der Herstellung und des Verkaufs eines Produktes bezeichnet.

IoT-Geräte werden häufig in Zusammenhang mit übergeordneten Systemen beschafft, z.B. Gebäudesteuerungssystemen. Zusammen mit der reinen Hardware und Firmware können auch noch zusätzliche Komponenten und Leistungen beschafft werden.

Werden bei der Beschaffung von IoT-Geräten Fehler gemacht, so kann dies negative Folgen auf den sicheren Betrieb des übergeordneten Systems oder sogar des gesamten Informationsverbunds haben. Bevor ein IoT-Gerät beschafft wird, muss daher eine Anforderungsliste erstellt werden, anhand derer die in Frage kommenden Geräte bewertet werden. Aufgrund der Bewertung kann dann eine fundierte Kaufentscheidung erfolgen, die sicherstellt, dass das IoT-Gerät im praktischen Betrieb den Sicherheitsanforderungen genügt. Die Anforderungsliste sollte im Wesentlichen die im Folgenden dargestellten sicherheitsrelevanten Bereiche und Kriterien umfassen.

Organisatorische Randbedingungen

Die folgenden Aspekte sollten bei der Beschaffung berücksichtigt werden:

- Kann ein effektiver Prozess zur Versorgung mit sicherheitsrelevanten Firmware- bzw. Softwareupdates etabliert werden?
- Informiert der Hersteller die betroffenen Stellen, wenn Sicherheitslücken bekannt werden?
- Bietet der Hersteller einen technischen Kundendienst an, der in der Lage ist, in einer vertretbaren Zeit Auskunft zu geben bzw. Fehlfunktionen zu beheben?
- Bietet der Hersteller Schulungen oder Handbücher zur Sicherheit der IoT-Geräte an?

Vorgaben aus dem Anwendungsgebiet

Das IoT-Gerät muss im jeweiligen Anwendungsgebiet geltenden Standards und Normen entsprechen, sowie, falls zutreffend, die Kriterien für eine produktspezifische Zulassung erfüllen. Derartige Zulassungen sind z. B. in den Bereichen Luftverkehr, Straßenverkehr und Medizintechnik üblich.

Materielle Sicherheit

Wird das IoT-Gerät bei rauen Umweltbedingungen wie Feuchtigkeit, extremen Temperaturen, mechanischen Belastungen und Staub eingesetzt, muss es physikalisch robust sein. Es sollten keine oder nur wenige zuverlässige Steckverbindungen vorhanden sein. Empfindliche Komponenten sollten speziell gekapselt und mit Dämpfungsvorrichtungen versehen sein. Auf Bauteile mit beweglichen Komponenten sollte soweit wie möglich verzichtet werden.

Ausfall- und Betriebssicherheit

Abhängig von der geforderten Verfügbarkeit sind an das IoT-Gerät Anforderungen zur Ausfallsicherheit, zur elektromagnetischen Verträglichkeit, zu internen Überwachungs- und Selbsttestmechanismen und zum Wiederanlauf zu stellen.

Systemarchitektur

Die Bandbreite für Systemarchitekturen ist sehr groß. Neben Neuentwicklungen kommen, anders als im PC - oder Serverbereich, auch oftmals ältere Architekturen und Betriebssysteme zum Einsatz. Gründe dafür sind die niedrigeren Kosten für den Prozessor selbst und die Möglichkeit das Anwendungsdesign, Programmcode und Entwicklungswerkzeuge sowie Debugtools wiederverwenden zu können. Es ist darauf zu achten, dass die gewählte Systemarchitektur geeignet ist, die notwendigen Sicherheitsfunktionen zu realisieren.

Betriebssystem und Anwendungssoftware

Wird das IoT-Gerät zusammen mit einem Betriebssystemen und/oder Anwendungssoftware beschafft, muss festgelegt werden, welche sicherheitsrelevanten Merkmale diese aufweisen sollen, z. B. hinsichtlich

- Nutzung sicherer Kommunikationsprotokolle
- Sicherer Installation und Aktualisierung
- Absicherung von Zugang und Zugriff
- Benutzer- und Rechteverwaltung
- Protokollierung
- Alarmierung
- Integritätsschutz

SYS.4.4.M9 Regelung des Einsatzes von IoT-Geräten

Auch im laufenden Betrieb müssen eine Reihe von Sicherheitsanforderungen an den Einsatz von IoT-Geräten gestellt werden. Sie müssen adäquat in das technische und organisatorische Umfeld eingebunden sein, in dem sie eingesetzt werden. Dafür müssen die folgenden organisatorischen Regelungen getroffen werden.

Es müssen Verantwortliche für den Betrieb der IoT-Geräte benannt werden, die sich beispielsweise um Aktualisierungen, Wartungs- und Reparaturarbeiten, Protokollauswertung und für die Reaktion auf Sicherheitsvorfälle und Fehlfunktionen benannt werden. Bei Ausfällen, Fehlfunktionen und bei Sicherheitsvorfällen muss klar definiert sein, was zu unternehmen ist.

Es sind Regelungen festzulegen, um die Sicherheit und Funktionsfähigkeit der IoT-Geräte zu testen. Die Anforderungen an die physikalische Einsatzumgebung, wie z. B. der Luftfeuchtigkeits- und Temperaturbereich und die Energieversorgung, müssen festgelegt sein. Falls erforderlich sind dafür ergänzende Maßnahmen bei der Infrastruktur zu etablieren.

Die IoT-Geräte sollten so konfiguriert werden, dass eine angemessene Sicherheit und Funktionalität erreicht werden kann. Die Konfiguration der IoT-Geräte muss dokumentiert sein, damit sie nach einem Austausch, einer Aktualisierung oder um ein System wieder herzustellen entsprechend den Sicherheitsanforderungen wieder eingerichtet werden kann.

SYS.4.4.M10 Sichere Installation und Konfiguration von IoT-Geräten

Nachdem die Planung neuer IoT-Geräte abgeschlossen und eine Sicherheitsrichtlinie erstellt wurde, kann mit der Installation der IoT-Geräte begonnen werden.

Die Installation und Konfiguration der IoT-Geräte sollte nur von autorisierten Personen (Verantwortlich für IoT-Geräte, Administratoren oder vertraglich gebundene Dienstleister) durchgeführt werden. Administratoren für IoT-Geräte und deren Vertreter müssen sorgfältig ausgewählt werden. Sie müssen regelmäßig darüber belehrt werden, dass die Befugnisse nur für die erforderlichen Administrationsaufgaben verwendet werden dürfen. Da Administratoren hinsichtlich der Funktionsfähigkeit der eingesetzten Hard- und Software eine Schlüsselrolle inne haben, muss auch beim Ausfall von Administratoren die Weiterführung der Tätigkeiten gewährleistet sein. Hierzu müssen die benannten Vertreter über den aktuellen Stand der Systemkonfiguration verfügen sowie Zugriff auf die für die Administration benötigten Passwörter, Schlüssel und Sicherheitstoken haben.

Installation

Während der Installation und der späteren Konfiguration sollten zumindest die wichtigen Schritte so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können. Beispielsweise kann eine Checkliste für die Installation erstellt werden, auf der durchgeführte Schritte abgehakt und vorgenommene Einstellungen vermerkt werden können. Eine entsprechende Dokumentation ist für eine Fehleranalyse oder spätere Neuinstallation hilfreich. Dabei sollte beachtet werden, dass neben dem Autor auch weitere, auf diesem Gebiet eventuell weniger spezialisierte, Administratoren auf die Dokumentation zurückgreifen müssen. Daher ist es wichtig, dass die Dokumentation gut strukturiert und verständlich ist.

Es sollte verhindert werden, dass andere IT-Systeme während der Installation auf das zu installierende IoT-Geräte zugreifen können. Dies ist wichtig, weil während der Installation meist noch keine Passwörter vergeben und keine Schutzmechanismen aktiv sind, aber eventuell schon Zugriffe möglich sind. Falls die Installation der IoT-Geräte über das Netz erfolgen soll oder muss (beispielsweise Nachladen von Paketen), so wird empfohlen, einen Installationsserver im abgesicherten Administrationsnetz zu nutzen.

Sofern dies nicht bereits automatisch geschehen ist, sollte spätestens beim Abschluss der Grundinstallation auch die Protokollierung der Systemereignisse aktiviert werden. Die Protokolldaten können bei Problemen bei der weiteren Installation und Konfiguration wertvolle Informationen liefern.

Konfiguration

Die Grundeinstellungen, die vom Hersteller oder Distributor eines IoT-Geräts vorgenommen werden, sind meist nicht auf Sicherheit optimiert, sondern auf eine einfache Installation und Inbetriebnahme sowie oft darauf, dass jeder Anwender möglichst einfach auf möglichst viele Features des IoT-Geräts zugreifen kann. Beim Einsatz von IoT-Geräten in Behörden oder Unternehmen ist dies oft nicht wünschenswert.

Der erste Schritt bei der Grundkonfiguration muss daher sein, die Grundeinstellungen zu überprüfen und nötigenfalls entsprechend den Vorgaben der Sicherheitsrichtlinie anzupassen. Die Grundkonfiguration ist naturgemäß relativ stark vom eingesetzten Betriebssystem abhängig. Aus diesem Grund sind in den betriebssystemspezifischen Bausteinen entsprechende detailliertere Empfehlungen enthalten.

Ziele einer sicheren Grundkonfiguration sollten sein, dass

- die IoT-Geräte gegen "einfache" Angriffe über das Netz abgesichert sind,
- niemand durch reine Neugierde oder gar zufällig Zugriff auf sensitive Daten erlangen kann, die nicht für ihn bestimmt sind,
- niemand beim Arbeiten mit den IoT-Geräten durch reine Bedienungsfehler schwerwiegenden Schaden an den IoT-Geräten verursachen kann, und dass
- die Auswirkungen kleinerer Fehler so weit wie möglich begrenzt sind.

Die Einstellungen, die im Rahmen der Grundkonfiguration überprüft und angepasst werden sollten, betreffen insbesondere die folgenden Bereiche:

Einstellungen für Systemadministratoren

Nicht alle IoT-Geräte bieten ein dediziertes Rechte- und Rollenmodell. Wenn, dann sollten die Kennungen, unter denen Systemadministratoren arbeiten, besonders stark abgesichert werden. Diese Einstellungen sollten überprüft und gegebenenfalls angepasst werden.

Einstellungen für Benutzerkennungen und Benutzerverzeichnisse

Im Rahmen der Grundkonfiguration sollte überprüft werden, welche Standardeinstellungen für Benutzerkennungen gelten. Die Einstellungen müssen gegebenenfalls entsprechend der Sicherheitsrichtlinie angepasst werden. Dies betrifft im Wesentlichen dieselben Parameter wie für Systemadministrator-Kennungen, für normale Benutzer können aber unter Umständen andere Einstellungen sinnvoll sein.

Einstellungen für den Zugriff auf das Netz

Im Rahmen der Grundkonfiguration sollten auch die Einstellungen für den Zugriff auf das Netz sowie wichtige externe Dienste getroffen und dokumentiert werden.

Deaktivierung von "Call Home"-Funktionen

Einige IoT-Geräte senden Informationen, beispielsweise über aufgetretene Fehler oder über die Systemkonfiguration, direkt an den Hersteller, damit dieser zukünftig das Produkt an die Bedürfnisse der Anwender anpassen kann. Hierfür wird eine Datenverbindung über Datennetze, wie dem Internet, zu den Servern des Herstellers aufgebaut. Eine solche Form des Datenabflusses kann kritisch sein, vor allem, wenn die Anwender nicht über die Häufigkeit und Inhalte der Datenweitergabe informiert werden.

Generell sollte dieser oft unerwünschte Informationsaustausch unterbunden werden. Ob und wie Informationen versendet werden, kann in der Regel den Lizenzvereinbarungen der eingesetzten Software entnommen werden.

Viele Applikationen bieten die Möglichkeit, diese "Call Home"-Funktion zu deaktivieren. Nur in begründeten Ausnahmefällen sollte diese aktiviert bleiben. Nach Updates sollte überprüft werden, ob die "Call Home"-Funktion weiterhin deaktiviert ist.

Durch lokale Paketfilter oder dem zentralen Sicherheitsgateway (Firewall) kann ebenfalls der Verbindungsaufbau mit dem Hersteller unterbunden werden. Beispielsweise könnten auf Grundlage der Zieladressen oder der Portnummern die Datenverbindungen abgewiesen werden. Hierbei ist zu beachten, dass die Berücksichtigung aller Applikationen aufwändig ist und automatische Update-Funktionen, falls benötigt, dann oft nicht mehr zur Verfügung stehen.

SYS.4.4.M11 Verwendung sicherer Protokolle

Bereits bei der Beschaffung sollte darauf geachtet werden, dass IoT-Geräte ein auf Verschlüsselung basierendes Protokoll (z. B. SSL/TLS bzw. SSH) unterstützen (siehe SYS.4.4.A8 Beschaffungskriterien für IoT-Geräte). Bei der Inbetriebnahme muss darauf geachtet werden, dass vorhandene sichere Protokolle aktiviert und eventuell vorhandene unsichere (wie z. B. telnet) deaktiviert werden. Bietet das Produkt selbst keine Verschlüsselung, muss dies bei der Inbetriebnahme, z. B. über ein Virtual Private Network (VPN), flankierend umgesetzt werden.

Soweit möglich sollten auf den IoT-Geräten alle nicht benötigten Netzprotokolle deaktiviert werden (siehe SYS.4.4.M13 Deaktivierung und Deinstallation nicht benötigter Komponenten).

SYS.4.4.M12 Sichere Integration in übergeordnete Systeme [Informationssicherheitsbeauftragter (ISB)]

IoT-Geräte werden häufig in Zusammenhang mit übergeordneten Management-Systemen eingesetzt, z.B. Gebäudesteuerungssystemen.

IoT-Geräte wie Überwachungskameras, Raum- und Umgebungssensoren sollten ausschließlich mit dem zugehörigen Managementsystem kommunizieren. Eine Kommunikation dieser Systeme mit dem Internet ist in aller Regel nicht notwendig und sollte unterbunden werden.

SYS.4.4.M13 Deaktivierung und Deinstallation nicht benötigter Komponenten

Oft sind nach einer Standardinstallation eines IoT-Geräts eine größere Anzahl von Benutzerkennungen, Protokollen, Diensten, Funktionen, Schnittstellen und sonstigen Komponenten eingerichtet, die für den Betrieb nicht in jedem Fall notwendig sind und die deswegen eine Quelle von Sicherheitslücken sein können. Dies gilt insbesondere für Netzdienste. Daher sollte im Rahmen der Grundkonfiguration geprüft werden, welche Protokolle und Dienste wirklich gebraucht werden. Nicht benötigte Dienste der IoT-Geräte sollten deaktiviert oder ganz deinstalliert werden. Dies gilt insbesondere für chronisch unsichere Dienste, wie z. B. Telnet oder SNMPv1/v2.

Nicht benötigte Benutzerkennungen sollten entweder gelöscht oder zumindest so deaktiviert werden, so dass unter der betreffenden Kennung keine Anmeldung am IoT-Gerät möglich ist.

Einige Schnittstellen können potentielle Sicherheitsprobleme mit sich bringen, denen durch geeignete organisatorische oder technische Sicherheitsmaßnahmen entgegengewirkt werden muss. Schnittstellen, deren Nutzung kontrolliert werden sollte, sind beispielsweise Bluetooth, WLAN, Zigbee, Firewire, eSATA (externer SATA-Festplattenanschluss) und Thunderbolt. Die Verwendung von nicht benötigten Schnittstellen sollte unterbunden werden. An vielen Geräten lassen sich die Funk-Schnittstellen nicht deaktivieren, dann muss die Nutzung der Geräte geprüft werden (Schutzbedarf, Kontroll- und Einschränkungsmöglichkeiten gegeneinander abwägen).

Die Überprüfung auf laufende Dienste sollte von außen durch einen Portscan von einem anderen System aus erfolgen.

SYS.4.4.M14 Einsatzfreigabe

Bevor IoT-Geräte im produktiven Betrieb eingesetzt und bevor sie an ein produktives Netz angeschlossen werden, sollte der Einsatz freigegeben werden, dies ist zu dokumentieren. Die Einsatzfreigabe basiert auf einer Prüfung der Installations- und Konfigurationsdokumentation und der Funktionsfähigkeit der IoT-Geräte in einem Test. Sie erfolgt durch eine in der Institution dafür autorisierte Stelle. Vertiefende Informationen hierzu sind in OPS.1.1.7 Softwaretests- und Freigaben zu finden.

SYS.4.4.M15 Restriktive Rechtevergabe

Grundsätzlich sollten Berechtigungen immer restriktiv vergeben werden, so dass Benutzer genau auf die Dienste und Daten zugreifen können, die sie für ihre Aufgaben benötigen.

SYS.4.4.M16 Beseitigen von Schadprogrammen auf IoT-Geräten

Je nach Art und Einsatzgebiet von IoT-Geräten können diese von Schadprogrammen infiziert werden. Wie Infektionen mit Schadprogrammen vorgebeugt werden kann und wie sie beseitigt werden können, hängt von den verwendeten Betriebssystemen ab. Hierüber sollten regelmäßig aktuelle Sicherheitsinformationen eingeholt werden.

Aktuelle Schadsoftware auf Überwachungskameras und anderen IoT-Geräten befindet sich oftmals nur im flüchtigen Arbeitsspeicher, statt sich persistent im System einzunisten. Daher ist ein regelmäßiger Neustart solcher IoT-Geräte ratsam. Dies kann eine Infektion bereinigen, wenngleich es nicht vor einer Neuinfektion schützt.

Kann die Ursache für die Infektion nicht behoben bzw. eine Neuinfektion wirksam verhindert werden, sollten die betroffenen IoT-Geräte nicht mehr verwendet werden.

SYS.4.4.M17 Überwachung des Netzverkehrs von IoT-Geräten

Es empfiehlt sich, die Kommunikation (ein- und ausgehende Verbindungen) regelmäßig auf Auffälligkeiten zu kontrollieren. Hierbei können Logfiles von Firewalls genaue Informationen liefern, mit wem die IoT-Geräte über welchen Dienst kommunizieren möchten und ob diese Verbindungen erlaubt oder blockiert wurden. Weiterhin können auch die IoT-Geräte oder die dazugehörige Administrations- oder Managementsoftware Informationen liefern, ob die IoT-Geräte erwartungsgemäß verwendet werden.

Sollte eine präventive Unterdrückung ungewollter Kommunikation nicht möglich sein, können folgende Maßnahmen bei der Erkennung helfen:

- Aktivierung und nach Möglichkeit zentralisierte Sammlung und Auswertung von Logdaten von Systemen und Komponenten.
- Automatische Filter auf diese Logdaten, die einen Alarm auslösen, wenn Netzverkehr von den IoT-Geräten oder Sensor-Systemen zu Nicht-Managementsystemen beobachtet wird.
- Analyse der Netz-Statistik z.B. mit Netflow.

SYS.4.4.M18 Protokollierung sicherheitsrelevanter Ereignisse bei IoT-Geräten

Grundsätzlich sind sicherheitsrelevante Ereignisse im Betrieb von IoT-Geräten zu protokollieren. Die technischen Möglichkeiten dazu können bei unterschiedlichen Arten von IoT-Geräten und deren Umgebung stark variieren. Mögliche Ausprägungen, Funktionalitäten und Parameter sind:

- Protokollierung in einen nicht flüchtigen Speicher, kumulativ durch unterschiedliche Prozesse,
- Datenaufzeichnung in einfachen, formatierten Textdateien, CSV oder
- Aufzeichnung von Prozessdaten über Datenlogger, im Zeittakt, ereignisgesteuert oder bei Änderungen,
- Strukturierte Speicherung der Ereignisse in einem Datenbanksystem,
- Echtzeitüberwachung mit Information eines Anwenders und der Möglichkeit einer Interaktion zur Laufzeit,
- Protokollierung aller oder konfigurierbarer Zustands- und Transitionsänderungen,
- Variablenablaufverfolgung, Audit Trails,
- Statistische Auswertung in Berichtsform oder als grafische Darstellung und
- Korrelation, Bewertung.

Soweit möglich, sollten bei IoT-Geräten zumindest Sicherheitsverstöße protokolliert werden, wie versuchter und durchgeführter unautorisierter Zugang und Zugriff. Insbesondere sind die Aktivitäten von privilegierten Benutzern zu überwachen, wie Technikern und Administratoren. Dadurch kann zwar der Missbrauch von Rechten nicht verhindert werden, es ist aber die Voraussetzung, um gezielt Schwachstellen zu schließen.

Ist eine elektronische Protokollierung wegen technischer Einschränkungen durch die begrenzten Ressourcen nicht oder nur sehr begrenzt realisierbar, sollten organisatorische Regelungen geschaffen werden. Zum einen sollten alle Arbeiten an einem IoT-Gerät mit Angaben zu Ort, Zeit, Ausführendem sowie Art und Grund der Tätigkeit in einem Logbuch festgehalten werden. Zum anderen sollten alle Ausfälle, offensichtliche Zugangs- und Zugriffsverletzungen und sonstige Auffälligkeiten im Logbuch dokumentiert werden. Die Einträge sollten regelmäßig und anlassbezogen ausgewertet werden.

Sowohl automatisch erzeugte Protokolle als auch Aufzeichnungen durch das Personal sind gegen unerlaubte nachträgliche Veränderung zu schützen. Nur dediziert Berechtigte dürfen auf die Protokolle zugreifen können. Soweit technisch möglich, sind Vorkehrungen zu treffen, dass die Protokolldaten auch nicht von privilegierten Nutzern gelöscht oder geändert werden können, durch Speicherung auf nicht wiederbeschreibbaren Datenträgern oder mittels elektronischer Signatur. Datenträger mit Protokolldaten sind sicher zu verwahren und die beteiligten Personen sind über den korrekten Umgang zu belehren.

SYS.4.4.M19 Schutz der Administrationsschnittstellen

Abhängig davon, ob IoT-Geräte

- lokal, also am Gerät selber, direkt über das Netz, also an einem anderen IT-System über eine entsprechende vom IoT-Gerät selbst bereitgestellte Weboberfläche, oder über zentrale netzbasierte Tools, also über eine Managementsoftware auf einem Server,
- direkt über das Netz, also an einem anderen IT-System über eine entsprechende vom IoT-Gerät selbst bereitgestellte Weboberfläche, oder über zentrale netzbasierte Tools, also über eine Managementsoftware auf einem Server,
- über zentrale netzbasierte Tools, also über eine Managementsoftware auf einem Server,

administriert werden, sollten geeignete Sicherheitsvorkehrungen getroffen werden. Die zur Administration verwendeten Methoden sollten in der Sicherheitsrichtlinie festgelegt werden und die vereinbarten Sicherheitsvorkehrungen kurz beschrieben werden. Die Sicherheitsrichtlinie gibt auch vor, wie die IoT-Geräte zu administrieren sind. Für eine Administration über das Netz sollten sichere Protokolle verwendet werden.

SYS.4.4.M20 Geregelte Außerbetriebnahme von IoT-Geräten

Bei der Außerbetriebnahme von IoT-Geräten muss sichergestellt werden, dass

- keine wichtigen Daten, die eventuell auf diesen gespeichert sind, verloren gehen, und dass
- keine sensitiven Daten auf den Datenträgern von IoT-Geräten zurück bleiben.

Dazu ist es insbesondere wichtig, einen Überblick darüber zu haben, welche Daten wo auf den von IoT-Geräten gespeichert sind.

- Austragen des IT-Systems aus Verzeichnisdiensten und Datenbanken
  Etwaige Berechtigungen im Netz, die an ein IoT-Gerät gekoppelt sind, müssen gelöscht werden. Beispiele hierfür sind Einträge auf Proxyservern am Sicherheitsgateway oder Zugriffsrechte auf Netzdienste, die anhand der IP-Adresse gewährt werden. Ist ein IoT-Gerät in netzweiten Verzeichnisdiensten oder Datenbanken eingetragen, so müssen die zugehörigen Einträge gelöscht oder zumindest die entsprechenden Kennungen deaktiviert werden.
- Löschen der Daten auf den IoT-Geräten
  Es muss sichergestellt werden, dass keine schützenswerten Informationen mehr auf den Speicherbereichen von IoT-Geräten vorhanden sind. Alle auf Datenträgern vorhandenen bzw. permanent gespeicherten Daten sollten so gelöscht werden, dass sie nachträglich auch nicht durch spezielle Software lesbar wiederhergestellt und missbräuchlich verwendet werden können. Ist es nicht möglich, die Daten sicher zu löschen, sollten bei höherem Schutzbedarf die betreffenden Datenträger vernichtet werden.
- Entfernen sonstiger Informationen
  Sind von einem IoT-Gerät noch an anderen Stellen schützenswerte Daten gespeichert, etwa in einem nichtflüchtigen Speicher oder in der Cloud, so müssen auch diese bei der Außerbetriebnahme des Geräts gelöscht werden.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

SYS.4.4.M21 Einsatzumgebung und Stromversorgung [Haustechnik, Informationssicherheitsbeauftragter (ISB)] (I)

Bevor IoT-Geräte installiert werden, sollte geklärt werden, ob sie in der angedachten Einsatzumgebung betrieben werden dürfen. Der ISB sollte beispielsweise prüfen, ob IoT-Geräte wie Kameras mit dem Blickwinkel auf Eingabegeräte (Tastaturen, PIN-Pads) oder Monitore sinnvoll sind. Diese könnten somit auch vertrauliche Zugangsdaten aufzeichnen. Je nach Schutzbedarf der Umgebung sollten potentiell unsichere Geräte dort überhaupt nicht installiert werden. Bei IoT-Geräten wie Kameras müssen außerdem die entsprechenden Datenschutz-Vorgaben beachtet werden.

Es sollte geklärt sein, ob ein IoT-Gerät bestimmte Anforderungen an die physikalische Einsatzumgebung hat, wie z. B. Luftfeuchtigkeit, Temperatur oder Energieversorgung. Dies ist insbesondere bei IoT-Geräten, die in Außenbereichen betrieben werden, wichtig. Falls erforderlich, sollten dafür ergänzende Maßnahmen bei der Infrastruktur umgesetzt werden, beispielsweise passende Einhausungen.

IoT-Geräte sollten in der Einsatzumgebung vor Diebstahl, Zerstörung und Manipulation geschützt werden. Dies kann beispielsweise durch geeignete Anbringung oder zusätzliche Schutzmechanismen wie Einhausungen erreicht werden. Wichtig ist das vor allem bei an der externen Peripherie angebrachten Geräten, z. B. zur Videoüberwachung.

IoT-Geräte sind häufig nicht an Stromnetze angeschlossen, sondern werden mit Batterien betrieben. Dann sollte der regelmäßige Funktionstest und Austausch der Batterien geregelt werden.

IoT-Geräte sollten entsprechend ihrer vorgesehenen Einsatzart und des vorgesehenen Einsatzorts vor Staub und Verschmutzungen geschützt werden.

SYS.4.4.M22 Systemüberwachung (A)

Um auf kritische Systemereignisse reagieren zu können, sollte auch für IoT-Geräte ein geeignetes Systemüberwachungs- bzw. Monitoringkonzept erstellt werden. Dazu gehört, dass Systemzustand und Funktionsfähigkeit der IoT-Geräte laufend überwacht werden. Wenn Fehler auftreten oder definierte Grenzwerte über- oder unterschritten werden, sollte dies automatisch an das Betriebspersonal gemeldet werden. Dafür sollten die IoT-Geräte in ein geeignetes Systemüberwachungs- bzw. Monitoringkonzept eingebunden werden.

SYS.4.4.M23 Auditierung von IoT-Geräten (CIA)

Bei allen IoT-Geräten sollte regelmäßig überprüft werden, ob diese korrekt konfiguriert und ob alle festgelegten Sicherheitsmaßnahmen umgesetzt sind. Werden Abweichungen vom Soll-Zustand gefunden und sind Abhilfe-Maßnahmen bekannt, so sollten diese dokumentiert werden.

Außerdem sollten, zumindest in sicherheitskritischen Bereichen, alle zum Einsatz kommenden IoT-Geräte durch Experten vor dem Einsatz sicherheitstechnisch überprüft werden.

SYS.4.4.M24 Sichere Konfiguration und Nutzung eines eingebetteten Webservers (CIA)

Einige IoT-Geräte besitzen einen integrierten Webserver, mit dem Informationen abgerufen und eingesteuert werden können. Dabei handelt es sich für gewöhnlich um einen sogenannten Embedded-Webserver mit eingeschränkter Funktionalität, der für die meist knappen Ressourcen optimiert ist. Auf dem Markt sind zahlreiche eingebettete Webserver verfügbar, sie haben eine geringe Größe, belasten die CPU nur moderat und sind weitgehend plattformunabhängig. Als Hauptaufgabe können sie Webdokumente an den Client via HTTP(S) übertragen. Einige beherrschen zudem das dynamische Erstellen von Dokumenten, etwa per Server-Side Scripting.

Für einen eingebetteten Webserver sollten möglichst nur die benötigten Komponenten und Funktionen installiert bzw. aktiviert werden. Bei einigen IoT-Geräten sind hier wenige oder gar keine Konfigurationsmöglichkeiten vorhanden. Der Webserver sollte unter einem Konto mit möglichst geringen Rechten ablaufen. Falls zum Start höhere Privilegien benötigt werden, sollte anschließend in ein nicht privilegiertes Konto gewechselt werden. Es sollten alle für die Sicherheit und die Fehlerbehandlung relevanten Meldungen protokolliert werden, z. B. strukturiert nach erfolgreichen und nicht erfolgreichen Zugriffen, internen Fehlern, fehlerhaften oder unvollständigen HTTP-Anfragen und sonstigen relevanten Systemmeldungen. Diese Protokollierung sollte in der Sicherheitsdokumentation beschrieben sein (weitere Informationen hierzu finden sich in OPS.1.1.6 Protokollierung)Mit dem Webserver sollte möglichst nur über eine gesicherte SSL-Verbindung kommuniziert werden und der Zugang sollte nur nach einer starken Authentisierung möglich sein.

3 Weiterführende Informationen

3.1 Wissenswertes

Es gibt auch darüber hinaus Sicherheitsmaßnahmen, die zur Absicherung von IoT-Geräten umgesetzt werden könnten und die je nach Einsatzumgebung und Schutzbedarf sinnvoll sind. Dazu gehören:

- Penetrationstests bzw. Sicherheitsanalysen der IoT-Geräte oder deren Firmware
- Prüfen auf versteckte Links (vor allem im Bereich der Administrationsfunktionen)
- Ergänzung fehlender oder unzureichender Authentisierungsfunktionen
- verfügbare Funktionen auf Konsolenebene

Dies ist der Bereich, wo weitere Sicherheitsüberlegungen und Maßnahmen gesammelt werden können und daraus ergänzende Maßnahmen abgeleitet werden könnten. Ideen dazu bitte an mailen.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Allgemeines IoT-Gerät" finden sich unter anderem in folgenden Veröffentlichungen:

[27001] ISO/IEC 27001:2013

Information technology-Security techniques-Information security management systems-Requirements, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/SC 27, Oktober 2013

[ACS1] Sicherheit von IP-basierten Überwachungskameras

BSI-Veröffentlichungen zur Cyber-Sicherheit (BSI-CS 128), Version 1.1, November 2016, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_128.html, zuletzt abgerufen am 05.10.2018

[ACS2] Spionageangriffe mittels Hintertüren in Überwachungskameras und Raumsensoren

So schützen Sie Ihr Unternehmen, Expertenkreis Cyber-Sicherheit, Oktober 2016
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/partner/161010_expkr_statement01.pdf, zuletzt abgerufen am 05.10.2018

[DHS] Securing the Internet of Things

Department of Homeland Security (DHS), November 2016, https://www.dhs.gov/securingtheIoT, zuletzt abgerufen am 05.10.2018

[OWASP] Open Web Application Security Project (OWASP)

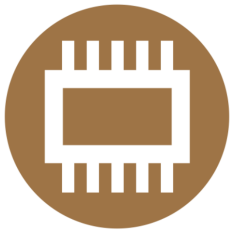
https://www.owasp.org, zuletzt abgerufen am 05.10.2018

Bundesamt
für Sicherheit in der
Informationstechnik

Umsetzungshinweise für die Bausteinschicht IND

IND.1 Betriebs- und Steuerungstechnik **815**

IT-Grundschutz



IND: Industrielle IT

Umsetzungshinweise zum Baustein IND.1 Betriebs- und Steuerungstechnik

1 Beschreibung

1.1 Einleitung

Betriebstechnik (englisch: Operational Technology (OT)) ist Hard- und Software, die Änderung durch die direkte Überwachung und / oder Steuerung von physikalischen Geräten, Prozessen und Ereignissen im Unternehmen erfasst und bewirkt [GART1].

In der Industrie, zu der unter anderem auch die Kritischen Infrastrukturen gehören, zählen dazu insbesondere industrielle Steuerungssystemen (Industrial Control Systems, ICS) und Automationslösungen, die dort die Steuerungs- und Regelfunktionen aller Art übernehmen. Weitere Beispiele sind Laborgeräte (z. B. automatisierte Mikroskop oder Analysewerkzeuge), Logistiksysteme (Barcodescanner mit Kleinrechner) oder Gebäudeleittechnik.

Die in der Vergangenheit übliche physische Trennung der OT von anderen IT-Systemen und Netzen in Büroanwendungen ist heute aufgrund zunehmender Integrationsanforderungen nur in Ausnahmefällen bei erhöhtem Schutzbedarf anwendbar. Mehrstufige Produktionsschritte und deren übergreifende Steuerung wie auch regulatorische Anforderungen erfordern eine zunehmende Öffnung auch über Organisationsgrenzen hinweg. Diese Entwicklung wird durch den Trend zur Optimierung von Fertigungsprozessen zur Steigerung der Wettbewerbsfähigkeit im Rahmen von Industrie 4.0 beschleunigt.

Da neben OT-spezifischen Komponenten zunehmend IT-Komponenten und Technologien aus der Office-IT in der OT eingesetzt werden, sind diese inzwischen vergleichbaren Gefährdungen ausgesetzt. Zugleich weisen die OT gegenüber der klassischen IT wesentliche Unterschiede auf, die das Anwenden dort etablierter Sicherheitsverfahren erschweren. So kann es Restriktionen aufgrund Herstellervorgaben oder gesetzlichen Anforderungen geben, die Veränderungen an Komponenten verhindern oder erschweren. Ein Beispiel hierfür sind die Anwendung von Sicherheitsupdates oder nachträgliche Härtungsmaßnahmen. Die OT unterliegt in der Regel auch deutlich längeren Lebenszyklen, auch über die Herstellerunterstützung hinaus, so dass auch die Verfügbarkeit von Sicherheitsupdates nicht durchgängig gewährleistet werden kann.

Diese Konvergenz der Technologien zwischen Office-IT und OT wird zukünftig eine vermehrte Zusammenarbeit zwischen den Knowhow-Trägern beider Funktionsbereiche fordern. Das technologische Know-how für IT, Kommunikation und Cyber-Defense liegt derzeit in den meisten Fällen bei den Office-IT Abteilungen. Eine erfolgreiche Lösung muss aber die Gegebenheiten der OT-Infrastruktur weitestgehend berücksichtigen. Dies kann jedoch nur mit der Unterstützung der OT-Verantwortlichen erfolgen.

1.2 Lebenszyklus

Der Lebenszyklus von ICS ergibt sich aus der Betriebsdauer der jeweiligen Produktionsanlage. Dieser ist immer deutlich länger als die in der Office-IT gewöhnlich anzutreffenden Zeiträume. Die typische Laufzeit beträgt zehn bis fünfzehn, mitunter auch 20 Jahre und länger. In der Office-IT sind es meist nur drei bis fünf Jahre.

Planung und Konzeption

Der Aufbau einer sicheren (im Sinne der Informationssicherheit) OT-Infrastruktur erfordert eine angemessene Planung. Bereits in der Konzeptionsphase sollten für die Informationssicherheit relevante Gesichtspunkte analysiert und in die Betrachtung einbezogen werden. Dies dient einer frühzeitigen Identifikation von Risiken im Entwicklungsprozess und kann in der Regel dann wirtschaftlicher behandelt werden. Im Rahmen der Planung sollte gleich das Bestandsverzeichnis und die initiale Dokumentation erstellt (siehe IND.1.M4 Dokumentation der OT-Infrastruktur) werden.

Die Entwicklung eines geeigneten Zonenkonzepts (siehe IND.1.M5 Entwicklung eines geeignete Zonenkonzeptes) bildet ein zentrales Element der Konzeptionsphase welches je nach Schutzbedarf einer mehr oder weniger ausgeprägten Abschottung bedürfen kann (siehe IND.1.M16 Stärkere Abschottung der Zonen). Bei der Konzeption ist auch der Umgang mit Wechseldatenträgern und mobilen Endgeräten (siehe IND.1.M9 Restriktiver Einsatz von Wechseldatenträgern und mobilen Endgeräten) und eine sichere (Fern-)Administration (siehe IND.1.M8 Sichere (Fern-)Administration) zu berücksichtigen. Dies sollte zusätzlich durch Konzepte für den Schutz vor Schadprogrammen (siehe IND.1.M3 Schutz vor Schadprogrammen) unterstützt werden.

Beschaffungsempfehlungen

Die Beschaffung einer sicheren ICS-Infrastruktur ist ein komplexer Prozess, im Rahmen dessen die notwendigen Anforderungen sinnvoll zwischen Betreiber, Integrator und Hersteller aufgeteilt und kommuniziert werden müssen (siehe IND.1.M11 Sichere Beschaffung und Systementwicklung).

Umsetzung

Damit die ICS-Infrastruktur sicher zu betreiben ist, muss sie in die Sicherheitsorganisation eingebunden werden (siehe IND.1.M1 Einbindung in die Sicherheitsorganisation). Mitarbeiter, die Aufgaben in ihrem Rahmen übernehmen, müssen in Bezug auf typische Gefährdungen sensibilisiert und geschult sein (siehe IND.1.M2 Sensibilisierung und Schulung des Personals). Um Maßnahmen entwerfen und bewerten zu können, ist schließlich eine gründliche Dokumentation der Infrastruktur unabdingbar (siehe IND.1.M4 Dokumentation der OT-Infrastruktur).

Darüber hinaus sind weitere Prozessbestandteile erforderlich, um den notwendigen Rahmen zu bilden, in dem ein sicherer Betrieb möglich ist: IND.1.M6 Änderungsmanagement in der OT und IND.1.M7 Etablieren einer Berechtigungsverwaltung, bei erhöhtem Schutzbedarf eventuell zusätzlich IND.1.M15 Prüfung und Überwachung von Berechtigungen und IND.1.M14 Starke Authentisierung an OT-Komponenten.

Betrieb

Der sichere Betrieb einer ICS-Infrastruktur umfasst ein Bündel von Prozessen und Maßnahmen, welche in IND.1.M6 Änderungsmanagement in der OT beschrieben sind. Grundlage des sicheren Betriebs ist die zuverlässige Erkennung von Störungen und Anomalien und wird mit IND.1.M19 Monitoring, Protokollierung und Detektion hervorgehoben.

Notfallvorsorge

Auch bezüglich der Notfallplanung gibt es einige Besonderheiten im Bereich ICS. Es müssen geeignete Konzepte für die Wiederherstellung der Infrastruktur nach einem Ausfall von Komponenten oder einer Kompromittierung der Infrastruktur beschrieben werden und vorliegen.

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Betriebs- und Steuerungstechnik" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

IND.1.M1 Einbindung in die Sicherheitsorganisation

Es muss ein Informationssicherheits-Managementsystem (ISMS) für die OT-Infrastruktur etabliert werden. Dieses OT-ISMS kann entweder als selbständiges ISMS oder als Teil eines Gesamt-ISMS existieren und sollte in seinem Geltungsbereich die Definition von Zielen und Werten, Prozessen, Rollen, Verantwortlichkeiten und Vorgaben für die OT-Infrastruktur explizit umfassen.

Insbesondere sollte auf die besonderen Anforderungen der OT eingegangen werden, die sich aus den besonderen Rahmenbedingungen wie z. B. Regelungen zur Gewährleistung ableiten lassen. Hierbei sollten die alternativen Vorgehensweisen zur Office-IT skizziert werden.

Aufbau einer Sicherheitsorganisation

Die Institution muss eine Sicherheitsorganisation aufbauen, welche die Rollen und Verantwortlichkeiten für die Informationssicherheit der OT-Infrastruktur und -Komponenten regelt. Dabei sollte die Sicherheitsorganisation alle an dem Betrieb von OT-Komponenten beteiligten Parteien berücksichtigen (z. B. Hersteller, Integrator/Maschinenbauer, Outsourcing-Partner, Drittanbieter, Spezialisten für die physische Sicherheit, Produktions- und Instandhaltungsleiter).

Es muss ein Gesamtverantwortlicher für die Informationssicherheit in der OT bestimmt und innerhalb der Organisation bekannt sein. Im folgenden wird dieser als ICS-Informationssicherheitsbeauftragter bezeichnet. In größeren Institutionen sollte zudem für jede Anlage, alternativ je Komponententyp/Schicht/Zone ein Verantwortlicher für die Informationssicherheit bestimmt werden.

Dabei kann sowohl eine Sicherheitsorganisation für die gesamte Institution aufgebaut und betrieben werden, welche die Bereiche Office-IT und OT umfasst, oder aber getrennte Sicherheitsorganisationen für die beiden Bereiche. Um Synergien zu nutzen und Fehlplanungen sowie Risiken zu vermeiden, muss eine enge Kooperation zwischen den OT- und Office-IT-Experten stattfinden. Welche Struktur für eine Organisation geeignet ist, hängt stark von den vorhandenen Strukturen und eingespielten Prozessen in einer Institution ab. Entscheidend ist, dass ein Informations- und Wissensfluss in beide Richtungen stattfindet und die jeweils Verantwortlichen in ihren Bereichen ernst genommen werden. Dafür müssen beide Seiten offen für die jeweiligen Besonderheiten des anderen Bereichs sein und zur Vermeidung von Missverständnissen die Kultur und Sprache der anderen Seite berücksichtigen. Eine Doppelspitze (Informationssicherheitsbeauftragter/ICS-Informationssicherheitsbeauftragter) kann in manchen Institutionen eine sinnvolle Lösung sein, wenn Aufgabenteilung und Schnittstellen eindeutig und schriftlich geklärt sind.

Beachtung gesetzliche Rahmenbedingungen

Gesetzliche, regulatorische und sonstige besonderen Vorgaben für die OT sowie die jeweilige Branche bzw. Sektor müssen bekannt sein und in ihren Auswirkungen für die Institution interpretiert werden. Dies gilt insbesondere für Institutionen, die kritische Infrastrukturen betreiben, aber auch zunehmend in anderen Bereichen. Neben den nationalen Vorgaben sind möglicherweise auch europäische und internationale Bestimmungen zu beachten. Es sollten Verantwortlichkeiten und Prozesse eingerichtet werden, um sicherzustellen, dass alle relevanten Anforderungen zeitnah den entscheidenden Stellen bekannt gegeben werden.

Festlegung und Einhaltung von Vorgaben

Es sollte ein Prozess existieren, wie konkrete Vorgaben für bestimmte Themenbereiche (Richtlinien/Policies) im ICS-Bereich verfasst, kommuniziert, fortgeschrieben, bewertet und zur Umsetzung gebracht werden. Diese können teilweise, wo angemessen und vorhanden, aus dem Bereich der Office-IT übernommen werden. Häufig sind jedoch Anpassungen notwendig, um die Besonderheiten der OT zu reflektieren.

Bei der Auswahl von Komponenten sollte eine Überprüfung von definierten (funktionalen und informationssicherheitsrelevanten) Anforderungen durchgeführt werden. Dabei können einzelne Komponenten bis hin zur gesamten OT Prüfgegenstand sein.

Weiterführende Informationen

Weiterführende Informationen zu Aufbau und Gestaltung des Sicherheitsorganisation sind im Baustein ISMS Sicherheitsmanagement dokumentiert.

IND.1.M2 Sensibilisierung und Schulung des Personals

Die Umsetzung der notwendigen Sensibilisierung und Wissensbildung des Personals kann auf unterschiedliche Art erfolgen. Es kann sich um spezielle Schulungsveranstaltungen handeln oder Online-Schulungen. Inhalte und Häufigkeit sollten sich an den Aufgaben der Mitarbeiter und den Bedrohungsszenarien orientieren. Eine einmalige Information ist mindestens für alle Mitarbeiter durchzuführen.

Betriebspersonal sollte auf die an einem OT-spezifischen Arbeitsplatz relevanten Bedrohungen oder Probleme hingewiesen werden. Dies kann z. B. der Umgang mit Wechseldatenträgern oder Smartphones sein.

OT-Verantwrotliche und ICS-Informationssicherheitsbeauftragter sollten spezifischer hinsichtlich der Bedrohungslage und notwendigen Handlungsbedarfen geschult werden.

Für KMUs bietet es sich in der Regel an, die Schulung durch Externe durchführen zu lassen, da diese stets aktuelles Praxiswissen mitbringen können. Bei größeren Institutionen lohnt sich eventuell. die Errichtung eines eigenen Kursprogramms.

Vorschläge für genauere Fortbildungspläne können z. B. dem Dokument „Empfehlungen für Fortbildungs- und Qualifizierungsmaßnahmen im ICS-Umfeld“ [BSI-CS 123] entnommen werden.

Zusätzlich ist zu empfehlen, die Sensibilisierung bezüglich Social Engineering regelmäßig und mit Nachdruck voranzutreiben, etwa durch Aufklärungskampagnen oder durch mit Datenschutz und Betriebsrat abgestimmte sorgsame Tests, welche niemanden persönlich bloßstellen dürfen.

IND.1.M3 Schutz vor Schadprogrammen

Ein Konzept zum Schutz vor Schadprogrammen muss die bedrohten OT-Komponenten sowie alle möglichen Infektionswege betrachten, Risiken bewerten und wo notwendig geeignete technische und organisatorische Schutzmaßnahmen festlegen.

Zu den möglichen Infektionswegen gehören unter Anderem:

- alle Außenschnittstellen inkl. Verbindungen zum Office-Netz, Internet und sonstigen Extranets
- Wechseldatenträger
- Service-Station und Programmiergeräte, auch von Dienstleistern
- sowie grundsätzlich auch neu beschaffte Komponenten (Festplatten, USB-Sticks, Software mit Trojanern etc.)

Virenscanner

Ist die Installation und der uneingeschränkte Betrieb von Virenschutzprogrammen auf OT-Komponenten möglich und durch den Hersteller/Integrator freigegeben, sollten diese Systeme automatisiert mit aktuellen Viren-Signaturen versorgt werden.

Sichere Konfiguration von Virenschutzprogrammen

Aufgrund der hohen Verfügbarkeitsanforderungen in der OT sollte bei kritischen Systemen unter Umständen eine angepasste Konfiguration für Virenschutzprogramme verwendet werden. Dabei sollten Einstellungen deaktiviert werden, die zu einer unbeabsichtigten Beeinträchtigung der Produktion führen können (z. B. aufgrund einer hohen Systemlast durch einen Virensuchlauf). Oftmals geben Hersteller nur solche eingeschränkten Konfigurationen zum Betrieb von Virenschutzprogrammen auf den OT-Komponenten frei.

Virenschutzprogramme können gewöhnlich in zwei unterschiedlichen Modi operieren. Zum einen kann vor dem Zugriff auf Anwendungen oder Dateien allgemein eine Überprüfung stattfinden oder der Scanvorgang wird manuell oder zeitgesteuert ausgelöst. Gewöhnlich sollte das Virenschutzprogramm automatisiert bei allen Zugriffen scannen.

Die Auswahl sollte dabei in Abhängigkeit von Empfehlung des Herstellers des Virenschutzprogramms und der OT-Komponente erfolgen. Sollte eine kontinuierliche Prüfung (z. B. aus Performancegründen) nicht möglich sein, sollten alternative Schutzmaßnahmen ergriffen werden.

Darüber hinaus sollte in regelmäßigen Abständen ein vollständiger Scan aller Daten durchgeführt werden. Ein zusätzlicher, vollständiger Scan mit aktuellen Signaturen sollte nach der Erstinstallation und nach Änderungen am System durchgeführt werden.

Grundsätzlich sollten folgende Einstellungen bei der Konfiguration der Virenschutzprogramme berücksichtigt werden:

- Manuelle Scans sollten ausschließlich bei Stillstand der Produktion durchgeführt und dokumentiert werden.
- Ausschließlich lokale Medien sollten geprüft werden. Netzlaufwerke sollten nicht gescannt werden, um parallele Scans durch mehrere Rechner zu vermeiden.
- Nur Administratoren dürfen die Befugnisse haben, das Virenschutzprogramm zu konfigurieren oder zu deaktivieren.
- Das Virenschutzprogramm sollte Funde an eine zentrale Stelle melden. Eine automatische Terminierung der Prozesse/Programme kann bei einen False Positive Fund zu einem Ausfall der OT-Komponente führen und ist daher kritisch zu prüfen.

Der Installationsprozess sowie die Konfiguration sollten für jede OT-Komponente dokumentiert werden.

Zentraler Viren

Das OT-Netz sollte soweit möglich autark betrieben werden und nur zwingend notwendige Verbindungen in andere Netze erlauben. Sind Verbindungen in andere Netze notwendig, so sollte diese nicht direkt erfolgen, sondern stets über einen Proxy-Server geführt werden.

Daher sollten die Signaturen für das Virenschutzprogramm nicht direkt aus dem Internet, sondern über einen zentralen Virensignaturverteildienst in der DMZ bezogen werden. Dieser lädt die aktuellen Signaturen stellvertretend aus dem Internet und stellt sie den OT-Komponenten zur Verfügung. Somit sind keine direkten Verbindungen dem OT in das Internet erforderlich.

Zeitnahe Aktualisierung der Viren-Signaturen

Oftmals sind zeitnahe Updates der Virensignaturen und der Virenschutzprogramme auf OT-Komponenten nicht möglich. Daher sind hierbei folgende Aspekte zu berücksichtigen.

Die OT-Komponenten sollten gemäß ihres möglichen Aktualisierungsintervalls in Gruppen unterteilt werden. Zusätzlich sollten redundant ausgelegte OT-Komponenten unterschiedlichen Gruppen zugeordnet werden, um beispielsweise auf die Verteilung von fehlerhaften Virensignaturen in der Produktionsumgebung (z. B. False Positives) umgehend reagieren zu können.

Die Verteilung der Virensignaturen in die Gruppen mit redundanten ICS sollte mit einer Zeitverzögerung durchgeführt werden (z. B. 12 Stunden), um bei Problemen weiterhin den Betrieb mit dem zweiten System aufrecht erhalten zu können.

Aufgrund der hohen Verfügbarkeitsanforderungen sollten nur vom Hersteller/Integrator der OT-Komponente freigegebene und als unkritisch klassifizierte Signaturen verteilt werden.

Virenschutzprogramm auf der Firewall (Virus-Wall)

Eine Virus-Wall untersucht den Datenverkehr zwischen zwei Netzen auf Schadprogramme. Auf diese Weise kann sie stellvertretend für OT-Komponenten mit keinem oder eingeschränktem Virenschutzprogramm übermittelte Daten prüfen. Dazu werden diese OT-Komponenten in ein separates Netzsegment platziert und der Datenverkehr zu und von diesem Netz durch ein Application Level Gateway (ALG) mit installiertem Virenschutzprogramm gefiltert und auf Schadprogramme untersucht. Siehe hierzu auch IND.1.M16 Stärkere Abschottung der Zonen.

Alternativen für Virenscanner

Virenschutzprogramme können jedoch in der Regel nicht auf allen Komponenten installiert werden. Mögliche Einschränkungen können sich aus einer fehlenden Herstellerfreigabe, nicht unterstützten Betriebsplattformen (z. B. Feldsysteme oder SPS), fehlenden Möglichkeiten zur Aktualisierung von Virensignaturen oder potentiellen Risiken in der Verfügbarkeit ergeben, so dass zumeist auch ergänzende oder alternative technische oder organisatorische Schutzmaßnahmen umgesetzt werden müssen. Alternative technische Schutzmaßnahmen können sein:

- Absicherung von Außenschnittstellen einer OT-Komponente (Standortanbindungen, Zugänge von Dienstleistern, Schnittstellen zum Office-Netz und dem Internet)
- Ausgliedern von bedrohten Systemen in abgesicherte Netzsegmente (mit einer Filterkomponente, falls eine Verbindung zu anderen Zonen notwendig ist (siehe Abschnitt Virenschutzprogramm auf der Firewall (Virus-Wall) oben)
- Einschränken von Wechseldatenträger (z. B. USB-Datenträger)
    - Deaktivieren von Systemschnittstellen
    - Einsatz einer Wechseldatenträgerschleuse
- Etablieren von netzbasierten Zugangskontrollen im Benutzerbereich (Vermeidung von Fremdgeräten)
- Einsatz netzbasierter Schutzsysteme
    - Application Layer Gateways (ALG)
- Application Whitelisting (Beschränkung von ausführbaren Programmen auf ICS)
- Falls möglich, regelmäßiges Scannen der OT-Komponenten von einem Boot-Medium oder USB-Device mit aktuellem Virenschutzprogramm und aktuellen Signaturen, beispielsweise während eines geplanten Wartungsfensters (auf diese Weise kann eine Infektion zumindest rückwirkend erkannt und dann beseitigt werden).

Alternative organisatorische Schutzmaßnahmen können sein:

- Regelungen zum Datenaustausch und Gebrauch von Wechseldatenträgern
- Verbot der Anbindung von Fremdgeräten
- Manuelle Virenprüfung mit speziellen offline-fähigen Antivirus-Lösungen in Wartungsfenstern

Um einen wirksamen Schutz der OT vor Schadprogrammen zu erreichen, sind daher abgestimmte und angemessene Sicherheitsmaßnahmen unter Berücksichtigung der umgebungsspezifischen Besonderheiten auszuwählen und umzusetzen. Auf dieser Basis ist ein Virenschutzkonzept zu erstellen, aus dem hervorgeht, wie der Schutz vor Schadprogrammen erreicht wird.

Application Whitelisting

Es besteht die Möglichkeit, mittels spezieller Sicherheitssoftware zur Applikationskontrolle, das Ausführen von Programmen zu überwachen und einzuschränken. Anders als bei gängigen Virenschutzprogrammen wird nicht versucht, unerwünschte Software zu blockieren, sondern es wird der Ansatz verfolgt, ausschließlich erwünschten Programmen die Ausführung zu erlauben.

Demzufolge können zwei unterschiedliche Ansätze unterschieden werden, um Anwendungen und unerwünschtes Verhalten eines Systems zu erkennen und zu verhindern (z. B. im Fall von Schadprogrammen). Bei dem Blacklist-Ansatz gewöhnlicher Virenschutzprogramme geschieht dies auf der Grundlage bekannter Signaturen und Heuristiken unerwünschter Anwendungen. Diese Herangehensweise weist einige Schwachstellen auf, wie z. B. dass sich neuartige Schadprogramme selbstständig bei jeder neuen Kopie verändern können und somit eine neue, noch unbekannte Signatur aufweisen. So ist der erfolgreiche Schutz von der Aktualität und Verfügbarkeit der Signaturen abhängig.

Beim Application Whitelisting werden nur solche Anwendungen und solches Verhalten erlaubt, welches explizit freigegeben wurde. Alles andere ist verboten. Auf diese Weise besteht keine Abhängigkeit zu aktuellen Signaturen. Insbesondere bei Systemen wie im OT-Umfeld, die nur geringfügigen Änderungen durch Softwareinstallationen unterliegen, eignet sich dieses Verfahren. Daher sollte, soweit möglich, eine Applikationskontrolle stets nach dem Whitelist-Ansatz erfolgen.

Um das Ausführen von unerlaubter Software zu verhindern, kann eine solche Schutzsoftware beispielsweise auf folgende unterschiedliche Attribute zurückgreifen:

- Zertifikate (Signieren von vertrauenswürdiger Software z. B. durch eine zentrale Stelle),
- Dateisystempfad (Bestimmte Bereiche werden als vertrauenswürdig deklariert),
- Hashes (Die Anwendungen und möglicherweise unbefugte Änderungen werden anhand eines Hashwertes der Dateien identifiziert),
- System- und Benutzerverhalten (z. B. Nutzung gewisser TCP-Ports, Bedienung nur zu bestimmten Zeiten).

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Betriebs- und Steuerungstechnik".

IND.1.M4 Dokumentation der OT-Infrastruktur

Eine vollständige, aktuelle und praktisch nutzbare Dokumentation der OT ist für einen ordnungsgemäßen Betrieb unabdingbar.

Erst recht gilt dies für die Informationssicherheit, da nur auf dieser Grundlage Notwendigkeit, Angemessenheit und Umsetzungsgrad vieler weiterer Maßnahmen festgestellt und mögliche Schwachstellen und Angriffsvektoren systematisch gefunden werden können.

Die Tiefe der Dokumentation kann sich unterscheiden. Beispielsweise kann man sich bei einem PLS, bei dem es sich um geschlossenes System handelt, auf die Außenschnittstelle beschränken. Das PLS selbst hat in der Regel eine interne Verwaltung bzw. einen einheitlichen Soft- / Hardware-Stand in Abhängigkeit der Systemversion. In anderen Fällen können sämtliche Komponenten dokumentiert werden.

Erstellen und Pflegen der Dokumentation

Die Form der Dokumentationsführung sollte sich an den Bedürfnissen der Zielgruppe orientieren und möglichst praktikabel gestaltet werden. Die Dokumentation kann in Form von einem oder mehreren Dokumenten, eingebettet in eine Website oder in spezifischen Dokumentationswerkzeugen (Tools) für IT-Umgebungen erfolgen. Zu beachten sind jedoch die bestehenden Anforderungen an die Verfügbarkeit der Dokumentation, welche insbesondere auch in Störungs- und Notfallsituationen zugänglich sein muss. Dies kann etwa durch Replikation auf Notsysteme oder als Ausdruck in Papierform am jeweiligen Arbeitsplatz und/oder am Notfallstandort erfolgen. Gleichzeitig sollte bei der Ablage auch die Sensibilität der Dokumentation berücksichtigt sein, um unbefugten Zugriffen vorzubeugen.

Der Betreiber muss sicherstellen, dass betriebsrelevante Änderungen in der Anlagendokumentation erfasst werden. Durch regelmäßig durchgeführte Prüfungen auf Aktualität können Versäumnisse im Tagesgeschäft identifiziert und nachgeholt werden.

Anforderungsaustausch mit Integrator und Hersteller

Dort, wo wesentliche Teile einer OT-Infrastruktur von Dienstleistern (Integratoren bzw. Maschinen-/Anlagenbauern) aufgebaut und gewartet werden, müssen Anforderungen, Nachweise und Dokumentationen in beide Richtungen weitergegeben werden: Sicherheitsanforderungen sollten möglichst schon im Rahmen der Ausschreibung, spätestens jedoch während der Umsetzung des Projekts an den Auftragnehmer kommuniziert werden.

Es sollte eine aktuelle und umfassende Dokumentation mitgeliefert oder erstellt werden, welche Informationen zu Sicherheitsfunktionen, Schwachstellen, Konfigurationen und notwendigen Schutzmaßnahmen enthalten.

Bestandsverzeichnis

Um Inkompatibilitäten und Inkonsistenzen von Software in spezifischen Versionen sowie von Konfigurationen (z. B. IP-Adressen-Konflikte) zu vermeiden, sollte in einer Liste die Konfiguration der einzelnen OT-Komponenten dokumentiert sein. Darüber hinaus können auf diese Weise OT-Komponenten schnell identifiziert werden, wenn neue Updates verfügbar oder Konfigurationsänderung nötig sind. Auch wenn Updates nicht möglich sind, so kann anhand einer solchen Liste die potentielle Betroffenheit zeitnah bewertet werden.

Die Liste kann beispielsweise folgende Eigenschaften dokumentieren:

- Funktionaler Name,
- Computername,
- Zuständiges Administrations-Personal mit hinterlegten Kontaktdaten (eventuell auch Servicezeiten),
- Physischer Aufstellungsort,
- MAC-Adresse(n),
- IP-Adresse(n),
- DNS-Bezeichnung,
- FQDN,
- Hersteller,
- Modell/Produkttyp
- Betriebssystem,
- installierte Anwendungen und Dienste unter Angabe von Ports und eingesetzten Protokollen,
- Patchstand jeder Software mit dem Datum der Einspielung des Patches (bei IT-Systemen wie SPSen und technsich verwandten Geräte ist es wichtig, Firmware-Stände jeder CUPU und jedes Moduls vorzuhalten),
- Datum der letzten Virenprüfung (bzw. Intervall bei automatischer Wiederholung) und
- Backup-Intervall (vollständig und inkrementell), Umfang der Datensicherung und die zuletzt durchgeführte Datensicherung.

Netzplan bzw. Netzstrukturplan

Die Struktur des Netzes sollte in einem physischen und einem logischen Netzplan dokumentiert werden. Soweit für die Umgebung sinnvoll darstellbar, soll der physische Plan die Orte und OT-Infrastruktur, z. B. Kabel, Gebäude und Funkverbindungen darstellen. Der Plan könnte hierzu enthalten:

- Name/Bezeichnung und Funktionalität der Systeme,
- mindestens ein technisches Merkmal, durch das das jeweilige System/Netzsegment identifizierbar ist, z. B.
  - IP-Netzadressen und Netzmasken z. B. 192.168.1.0/24,
  - IP-Adressen aller angeschlossenen Netzinterfaces z. B. 192.168.1.54
  - MAC-Adressen (mindestens dann, wenn und wo nicht primär IP-Kommunikation eine Rolle spielt),
- (falls vorhanden) DNS-Name, bzw.
- (falls vorhanden) FQDN (Fully Qualified Domain Name).

Der logische Netzplan stellt die physischen Gegebenheiten nicht dar und fokussiert auf die strukturelle Sicht und die Sicherheitszonen.

Neben den Kommunikationsmöglichkeiten, die der Netzplan darstellt, sollten auch die Kommunikationsbeziehungen zwischen den Komponenten erfasst werden. Dies bedeutet, welche Komponenten miteinander kommunizieren können müssen. Dies ist notwendig, um unbefugten Datenverkehr identifizieren und unterbinden zu können.

Redundanzen (gleichartige Systeme mit analoger Funktion, Konfiguration und gleichem Schutzbedarf) können im Netzstrukturplan zusammengefasst werden, da dies der Lesbarkeit dient. Bei hohem Verfügbarkeitsbedarf sollten die Redundanzen (Anzahl, Typ (etwa Hot-Standby, Failover, Load Balancing etc.)) jedoch aus dem Netzstrukturplan hervorgehen. Dies kann durch Annotierung der Objekte erfolgen, um den Plan selbst nicht aufzublähen.

Administrations- und Benutzerhandbücher

Für den sicheren und unterbrechungsfreien Betrieb ist es notwendig, dass das Service- und Wartungspersonal sowie Administratoren alle Funktionen der OT kennen und diese bedienen können. Kommt es zu Ausfällen beim Personal (z. B. krankheitsbedingt oder aufgrund einer Kündigung), sollte sichergestellt sein, dass die benötigten Informationen weiterhin in der Institution verfügbar und für die Vertreter zugänglich sind.

Daher sollte für die OT und jede Anwendungen ein Administrations- und ein Benutzerhandbuch verfügbar sein (möglicherweise auch ein Dokument, welches beide Themen abdeckt). Neben betrieblichen Regeltätigkeiten und Abläufen sollten die Dokumente auch Aspekte der Informationssicherheit abdecken, darunter:

- Notwendiges Firewall-Regelwerk (mit Dienst, Protokoll und Port),
- Anweisungen zur Härtung spezifischer Anwendungen,
- Anweisungen zur sicheren Konfiguration,
- Spezifische Risiken (z. B. bei der Aktivierung einer bestimmten Konfiguration),
- Systemwiederherstellung (zur Notfallvorsorge).

Die Dokumentationslage sollte die Fortführung des Betriebs durch Dritte ermöglichen.

Energiewirtschaft und andere KRITIS-Sektoren

Für die Energiewirtschaft gelten aufgrund des IT-Sicherheitsgesetzes zusätzliche Anforderungen. Hier verlangt der IT-Sicherheitskatalog der Bundesnetzagentur gemäß §11 Absatz 1a des Energiewirtschaftsgesetzes (EnWG) neben der Errichtung eines ISMS, das den Anforderungen der DIN ISO/IEC 27001 in der jeweils geltenden Fassung genügt und bei dessen Implementierung die Normen DIN ISO/IEC 27002 und DIN ISO/IEC TR 27019 (DIN SPEC 27019) in der jeweils geltenden Fassung zu berücksichtigen sind, auch die Erstellung einer bestimmten Form des Netzstrukturplans. Der Netzbetreiber hat eine Übersicht über die vom Geltungsbereich des IT-Sicherheitskatalogs betroffenen Anwendungen, Systeme und Komponenten mit den anzutreffenden Haupttechnologien und deren Verbindungen zu erstellen. Die Übersicht ist nach den Technologiekategorien „Leitsystem/Systembetrieb“, „Übertragungstechnik/Kommunikation“ und „Sekundär-, Automatisierungs- und Fernwirktechnik“ zu unterscheiden. Kapitel E.IV Tabelle 2 des IT-Sicherheitskatalogs enthält eine kurze Beschreibung zu den Technologiekategorien sowie einige Beispiele, welche in der Regel jedoch an die konkrete OT angepasst werden müssen. Im Geltungsbereich des ISMS wie im Netzstrukturplan müssen mindestens die Telekommunikations- und EDV-Systeme enthalten sein, die „für einen sicheren Netzbetrieb notwendig“ sind. Die Definition der letztgenannten Kategorie ist von der Institution vorzunehmen und zu begründen.

Auf andere KRITIS-Sektoren kommen zukünftig ebenfalls Sonderanforderungen zu. Hier muss die jeweilige Regulierung und Umsetzungspraxis beobachtet werden.

Wichtig ist, eine begründete Abgrenzung vorzunehmen, welche Systeme für den sicheren Betrieb der industriellen bzw. KRITIS-Funktionen notwendig sind. Dies kann z. B. im Netzplan geschehen und sollte mit dem Zonenmodell (siehe IND.1.M5 Entwicklung eines geeigneten Zonenkonzepts) kompatibel sein.

IND.1.M5 Entwicklung eines geeigneten Zonenkonzepts [IT-Betrieb]

Das OT-Netz sollte aus mehreren Netzsegmenten mit individuellen Schutzbedarfen bestehen. Der Datenverkehr zwischen den verschiedenen Ebenen (vgl. Abbildung: Ebenen der Automatisierungspyramide) sollte durch eine Datenflusskontrolle(z. B. mittels Firewall) auf das betriebliche notwendige Maß reglementiert werden.

Abbildung: Ebenen der Automatisierungspyramide

Neben der Trennung von Netzen mit unterschiedlichen Funktionalitäten auf derselben Ebene sollten auch standortübergreifende Netze oder allgemein organisatorisch unabhängige Maschinen/Anlagen untereinander segmentiert werden (horizontale Segmentierung). So wird z. B. verhindert, dass sich Schadprogramme ungehindert auf alle Maschinen ausbreitet.

Der Verbindungsaufbau sollte grundsätzlich aus dem Netzsegment mit dem höheren Schutzbedarf in das Netzsegment mit dem niedrigeren Schutzbedarf aufgebaut werden.

Eine Umgehung der Netztrennung durch undokumentierte Verbindungen darf nicht stattfinden. Insbesondere sollten keine unkontrollierten Verbindungen zu Netzsegmenten mit unterschiedlichem Schutzbedarf zugelassen werden.

Berücksichtigung

Bei der Konzeption und Umsetzung des Zonenmodells müssen betriebliche Abhängigkeiten ermittelt und in ihren Auswirkungen untersucht werden. Damit wird die Betriebsstabilität im Rahmen der bestehenden Anforderungen gewährleistet und unter Berücksichtigung der Anforderungen der OT-Umgebung angemessen ausgestaltet. Für die Bewertung sind die Verfügbarkeitsanforderungen jeder Zone gemäß den Anforderungen der technischen Prozesse nach dem Maximalprinzip über alle Systeme der Zone zu bestimmen.

IND.1.M6 Änderungsmanagement im OT-Betrieb

Über die Lebenszeit der OT gilt es die Veränderungen an der Anlage und der möglichen neuen Gefährdungen laufend zu berücksichtigen und entsprechend Rechnung zu tragen.

Dokumentation

Beim Betrieb der Anlage gilt es, in die bestehende Dokumentation Änderungen und Anpassungen zu übernehmen. Ziel ist, stets über eine aktuelle Dokumentation zu verfügen, die den tatsächlichen Zustand der Systeme abbildet. Durch die kontinuierliche Fortschreibung entfallen aufwändige Bestandsanalysen.

Änderungsverwaltung

Administrative Änderungen an der bestehenden Infrastruktur oder OT-Komponenten können die Informationssicherheit der Umgebung beeinflussen und sollten über einen verbindlichen Änderungsprozess geplant, geprüft, im Rahmen der Möglichkeiten angemessen getestet, durchgeführt und dokumentiert werden. Die Ausprägung des Prozesses ist dabei stark von der jeweiligen Organisation bzw. OT abhängig und sollte nachvollziehbar dokumentiert sein. In weniger komplexen Umgebungen mit einem kleinen Administrationsteam kann der Änderungsprozess im Wesentlichen aus Ablaufvorgaben (Planung, Informationspflichten bei Wartungsarbeiten, Bezug von Software- und Updates, Ablauf von Tests (Testkonzept), Regelungen zum Einsatz von Dienstleistern) sowie aus Dokumentationsverpflichtungen (z. B. übergreifendes oder systemgebundenes Administrationsjournal) bestehen. In größeren Organisationen kann ein komplexerer Änderungsprozess bestehend aus Antrags-, Prüfungs-, Test- und Genehmigungsverfahren bestehen und den Einsatz unterstützender Tools (Formulare, technisch gestützte Arbeitsabläufe, CMDB, etc.) erforderlich machen.

Zeitsynchronisation

Eine Vielzahl an Prozessen, aber auch administrative Tätigkeiten, beruhen in der OT auf einer genauen und abgestimmten Zeit (z. B. die Nachvollziehbarkeit verteilter Protokolldaten, Beigabe von Zusatzstoffen in der Produktion zum richtigen Zeitpunkt etc.). Es muss aufgrund der Applikationsanforderungen abgewogen werden, wie die Zeitsynchronisation erfolgt.

Für die Synchronisation kann das Network Time Protocol (NTP) oder IEEE 1588 genutzt werden.

Das Zeitsignal für die Systeme sollte aus einer vertrauenswürdigen Quelle stammen. Zonen hoher Kritikalität etwa sollten ihre Zeit nicht aus einer weniger geschützten Zone beziehen, wenn das Signal möglicherweise manipuliert werden könnte. Die Clients auf den OT-Komponenten sollten die Zeit in einem einheitlichen, standardisierten Format interpretieren (z. B. unter Berücksichtigung von Zeitzonen, Winter- und Sommerzeit).

IND.1.M7 Etablieren einer Berechtigungsverwaltung

Unter Berechtigungen sind Privilegien von Personen zum

- Zutritt (physikalischer Zugriff zu IT-Systemen),
- Zugang (Erreichbarkeit eines Systems über Netzwerk) oder
- Zugriff (Ausführbarkeit von Programmen und Funktionen sowie Nutzbarkeit von Daten)

zu verstehen.

Falsch gesetzte Berechtigungen können die Sicherheit einer IT-Umgebung wesentlich beeinträchtigen. Zu umfangreich oder zu Unrecht vergebene Rechte können durch Missbrauch oder Fehlhandlungen Störungen begünstigen, während zu gering gesetzte Rechte Regelabläufe erschweren und in kritischen Situationen die effektive Störungsbearbeitung behindern können.

Berechtigungen müssen daher bedarfsorientiert nach dem Minimalprinzip vergeben und in Bezug auf Änderungen aktiv gepflegt werden. Hierzu wird ein durchgängiger Prozess (Berechtigungsverwaltung) benötigt.

Die Berechtigungsverwaltung muss die folgenden grundlegenden Anforderungen erfüllen:

Bereitstellen eines Beantragungs-, Prüf- und Freigabeprozesses

Berechtigungen müssen formal beantragt und erfolgreich geprüft werden, bevor sie vergeben werden dürfen. Ein Berechtigungsantrag sollte von zumindest zwei Personen geprüft werden. Die Prüfung könnte durch den jeweilig Vorgesetzten und durch den jeweiligen Anwendungs- oder Systemverantwortlichen erfolgen.

Revisionssichere Pflege einer Bestandsübersicht und Historie

Das Berechtigungsmanagement muss eine vollständige Übersicht über die an eine Person vergebenen Berechtigungen besitzen. Diese Übersicht muss auch die Berechtigungshistorie einer Person sowie Informationen über den jeweils gestellten Berechtigungsantrag und durchgeführten Prüf- und Freigabeprozess umfassen.

Die Bestandsführung von Benutzerkonten und Berechtigungen muss in nutzbarer Form dargestellt und als Grundlage für ein Soll-/Ist-Vergleich genutzt werden können.

Verifikation bestehender Zugänge

Die Berechtigungsverwaltung benötigt eine Schnittstelle zum Personalprozess, damit Statusänderungen in Beschäftigungsverhältnissen von Mitarbeitern zeitnah berücksichtigt werden können. Zugänge und Berechtigungen von befristeten und externen Mitarbeitern sollten stets zeitlich befristet für die Dauer des Arbeits- bzw. Beauftragungsverhältnis angelegt werden.

Ergänzend sollte in einem festgelegten Zyklus (z. B. jährlich) eine manuelle Verifikation der eingerichteten Benutzerzugänge durchgeführt werden.

Bei IT-Berechtigungen sind zudem spezielle Vorgaben zur Berechtigungsverwaltung zu berücksichtigen.

Nutzung persönlicher Benutzerzugänge

Sofern vom System unterstützt, sollten Benutzerzugänge für die interaktive Systemnutzung durch Anwender und Administratoren als persönliche Konten erstellt und dem Besitzer fest zugeordnet werden. Ist die Nutzung persönlicher Zugänge technisch nicht möglich oder im bestehenden Umfeld nicht sinnvoll umsetzbar, muss die Vergabe von Gruppenzugängen nachvollziehbar bleiben.

Rollenbasierte Berechtigungsvergabe an persönliche Zugänge

Berechtigungen sollten persönlichen Benutzerzugängen grundsätzlich über Gruppen zugeordnet werden. Zur Wahrnehmung einer Benutzerrolle kann ein Benutzerzugang Mitglied einer oder mehrerer Gruppen sein. Die für ein System zur Verfügung stehenden Berechtigungsgruppen werden durch die jeweiligen Systeme und Anwendungen vorgegeben.

Vergabe spezieller Zugriffsberechtigungen

Besondere netzwerkseitige Zugangsberechtigungen, wie diese etwa durch Firewall-Freischaltungen oder Access Control Lists (ACL) auf Screening-Routern eingerichtet werden, werden typischerweise für die Arbeitsplatzrechner bestimmter Personen eingerichtet. Eine solche Zugriffsregel ist somit als Benutzerberechtigung zu verstehen und sollte in der Berechtigungsverwaltung geführt und im Rahmen der regelmäßigen Verifikation überprüft werden.

Die Verwaltung von Berechtigungen kann eigenständig für die OT durch die Institution erfolgen, oder in eine institutionsweite Berechtigungsverwaltung eingebunden sein.

Gruppen

Grundsätzlich ist die Nutzung persönlicher Benutzerzugänge aufgrund der höheren Nachvollziehbarkeit und Anwenderverantwortung zu bevorzugen. In bestimmten Fällen kann jedoch auch die Verwendung funktionaler Gruppenzugänge vertreten werden, wenn sich hierdurch betriebliche Vorteile oder eine verbesserte Verfügbarkeit erreichen lassen, welche mit anderen Mitteln nur aufwändig herzustellen wären. Jeder Gruppenzugang muss separat dokumentiert werden. Die Personen, die Zugriff auf den Personenzugang erhalten, müssen organisatorisch z. B. über Schichtpläne nachvollziehbar dokumentiert sein. Ein Beispiel könnte sein die Verwendung eines Zugangs „Bediener“ in einer Warte, welche rund um die Uhr besetzt ist und in der sich alle Personen mit Zutritt gegenseitig kennen. Die funktionalen Zugänge müssen ebenso wie andere Zugänge in den ordnungsgemäßen Prozess des Managements von Berechtigungen integriert sein. Es ist insbesondere darauf zu achten, dass jeweils nur die minimal benötigten Rechte erteilt werden. Im Zweifel können verschiedene Aufgaben auf verschiedene Zugänge verteilt werden, sodass idealerweise ein möglichst großer Teil des Personals nur lesenden Zugriff benötigt. Jeder Zugang muss einem Verantwortlichen zugeteilt sein.

Verantwortung für funktionale und technische Benutzerzugänge

Funktionale Zugänge sollten dem für die Anwendung Verantwortlichen zugeordnet sein. Technische Benutzer- und Dienstezugänge (etwa für Maschine- zu Maschine-Kommunikation bzw. die Integration mit anderen Anwendungen) sollten den für eine Komponente jeweilig Betriebsverantwortlichen zugeordnet sein.

Passwortverteilung und -management, Passwort

Es sollte eine Passwortrichtlinie umgesetzt sein, welche die folgenden Punkte berücksichtigt. Dabei können technische Lösungen als auch organisatorische Maßnahmen festgelegt werden.

- Der Benutzer sollte durch Komplexitätsanforderungen daran gehindert werden, schwache Passwörter zu wählen (z. B. Länge, Alphabet mit Zahlen und Sonderzeichen).
- Das Passwort sollte nur für einen vordefinierten Zeitraum gültig sein. Der Benutzer sollte daraufhin aufgefordert werden, ein neues, vom alten abweichendes Passwort zu wählen.
- Die Anzahl fehlgeschlagener Anmeldeversuche sollte begrenzt werden (z. B. temporäre Sperrung des Benutzerzugangs).

Bei der Auswahl der Maßnahmen ist sicherzustellen, dass die Anlage stets bedienbar bleibt und gefährliche Zustände ausgeschlossen bleiben.

Eine mögliche Alternative zu Passwörten stellen Smart-Cards dar.

Vermeidung von Missbrauch

Ein unbefugter Zugriff auf Systeme sollte verhindert werden. Es sollte erkennbar und dokumentierbar sein, welcher Benutzer aktiv war (vgl. IND.1.M10 Monitoring, Protokollierung und Detektion).

Es gibt bestimmte Betriebssituationen, die einen unmittelbaren Bedienzugriff in die OT benötigen. Dabei ist eine Abmeldung oder Bildschirmsperre nicht akzeptabel. In diesen Fällen sollten die Systeme durch kompensierende Schutzmaßnahmen vor dem unbefugten Zugriff geschützt werden (z. B. besetzter Leitstand).

In weniger kritischen Bereichen sollte die Bedienung gesperrt werden und lediglich eine Anzeige der aktuellen Informationen erfolgen. Auf diese Weise ist eine Beobachtung weiterhin möglich, der ungehinderte Zugriff jedoch verhindert.

Zur Authentisierung können Lösungen unter Nutzung von Chip- oder RFID-Karten mit Benutzer-PIN genutzt werden, um die Eingabe von komplexen Passworten zu vermeiden.

IND.1.M8 Sichere Administration [IT-Betrieb]

Die Verwaltung von aktiven Systemkomponenten wie Serversystemen, Netz- oder OT-Komponenten erfolgt entweder an der lokalen Konsole, über eine serielle Schnittstelle oder bei vernetzten Komponenten nach der Ersteinrichtung typischerweise per netzbasiertem Fernzugriff.

Inbetriebnahme

Für die Erstkonfiguration einer Komponente sollte eine Anleitung bzw. Prüfliste erstellt werden, die gewährleistet, dass sicherheitsrelevante Einstellungen personenunabhängig durchgesetzt werden. Die jeweilig vorzunehmenden Einstellungen sind komponentenabhängig. Sie können beispielsweise umfassen (Aufzählung nicht vollständig):

- Deaktivieren von
  - nicht erforderlichen oder unsicheren administrativen Schnittstellen (SNMP, HTTP, Service-Ports, usw.)
  - entbehrlichen Standardbenutzerkonten
  - bzw. Deinstallation nicht erforderlicher Funktionen
- Aktivieren von Sicherheitsfunktionen:
  - Konfiguration sicherer Fernadministrationsschnittstellen (SSH, HTTPS)
  - Logon-Banner
  - Session-Timeouts oder Sitzungszeitbeschränkungen
  - Mindestanforderungen an die Passwortsicherheit
  - Beschränkung administrativer Zugriffe auf Administrationsnetze (Access Control Lists)
  - Verschlüsselte Speicherung von Passwörtern
  - Zeitsynchronisierung
  - Aktivieren der Systemprotokollierung / Konfiguration von Protokollierungsservern
  - Prüfen auf und Ändern von potentiell vorhandenen Standardpasswörtern
  - Einbindung in zentrale Verwaltungs- oder Authentisierungssysteme
  - Sicheres Hinterlegen von Administrationspasswörtern
  - eventuell lokale Firewall oder Integritätsprüfungen

Die Erstkonfiguration kann auch auf Basis einer initial erstellen Referenzkonfiguration durchgeführt werden. Die Erstkonfiguration sollte möglichst in einer sicheren Umgebung erfolgen und auch stets das Einspielen der verfügbaren Sicherheitsaktualisierungen (Patches) umfassen, bevor eine Komponente in Betrieb genommen wird. Vor der Integration in das OT-Netz wird empfohlen, die Echtheit der Komponente zu prüfen und auf kompromitierendes Verhalten zu testen.

Konfigurationen an der lokalen Konsole

Konfiguration von OT-Komponenten an der lokalen Konsole beschränkt sich bei vielen Komponenten auf die Erstkonfiguration bei der Inbetriebnahme, sodass die Verwaltung im Betrieb über netzbasierte Fernzugriffe erfolgen kann. Die Konfiguration nicht vernetzter Komponenten erfolgt auch weiterhin über die lokale Konsole. Die lokale Konsole wird zudem oftmals als alternative Konfigurationsmöglichkeit im Störungsfall der Netzwerkinfrastruktur beibehalten und nicht deaktiviert.

Der physische Zugang zu aktivierten Systemkonsolen muss daher auf geeignete Weise beschränkt werden, etwa durch gesicherte Räumlichkeiten oder abschließbare Serverschränke. Des Weiteren sollte der Zugriff auf die Konsole durch ein Passwort gesichert und auf autorisierte Zugänge beschränkt sein.

Fernwartung

Die Fernwartung sollte grundsätzlich durch sichere Protokolle wie zum Beispiel TLS-gesicherte Verbindungen, SSH oder SNMPv3 erfolgen. Klartextprotokolle sind zu vermeiden. Falls möglich, sollte die Einrichtung eines dedizierten Administrationsnetzes bzw. Zugriffsbeschränkungen (ACLs) vor unbefugtem Zugriff schützen.

Die Sicherheit der Wartungsrechner ist für den sicheren Betrieb der Anlage unverzichtbar. Diese müssen daher angemessen vor Kompromittierung oder Missbrauch geschützt werden. Als Grundlage hierfür sollten die einschlägigen Bausteine des IT-Grundschutzes für die Wartungssrechner angewendet werden. Besonderes Augenmerk sollte in diesem Zusammenhang auf die Aspekte Zutritt, netzbasierter Zugang, Nutzung des Systems und Außenschnittstellen wie Internet, Email oder die Nutzung von Wechseldatenträgern gelegt werden. Der Betrieb eines aktuellen Virenscanners kann in Abhängigkeit von der Bedrohungslage erforderlich bzw. vermeidbar sein.

Support-Zugriffe

Extern erreichbare Fernwartungszugänge müssen angemessen geplant und wirksam vor Missbrauch gesichert werden. Geeignete Maßnahmen hierzu sind:

- ZugangsbeschränkungenDer Zugang zu Fernwartungszugängen sollte nach Möglichkeit auf bekannte, vordefinierte Netzbereiche beschränkt werden.
- Sichere AuthentisierungDer externe Verbindungsaufbau sollte sicher authentisiert werden. Dies kann beispielsweise mittels eines zusätzlichen Tokens oder Client-Zertifikats erreicht werden. Bei Einwahlverbindungen kann ein Call-Back-Verfahren an eine hinterlegte Rufnummer eingerichtet werden.
- Einsatz sicherer ProtokolleDer externe Zugriff auf OT-Umgebungen darf ausschließliche über verschlüsselte und integritätsgesicherte Protokolle erfolgen.
- Nutzung von SprungservernDer externe Fernwartungszugriff auf OT-Komponenten sollte nicht direkt, sondern über gehärtete Sprungserver in einer DMZ-Infrastruktur erfolgen (vgl. IND.1.M16 Stärkere Abschottung der Zonen). Der Sprungsserver kann bestmöglichst gegen Angriffe geschützt werden und auf dem aktuellsten Patch-Stand sein, während die OT-Komponente wegen Verfügbarkeitsanfoderungen oder fehlender Updates noch auf einem veralteten Stand ist. Auf diese Weise kann die Komponente vor unberechtigten oder schadhaften Zugriffen geschützt werden, Datentransfers unterbunden, Prüfungen auf Schadprogramme erzwungen und Sitzungszeitbeschränkungen oder Verbindungsabbrüche bei Inaktivität durchgesetzt werden.
- Bedarfsabhängige AktivierungWenn Fernzugänge nur unregelmäßig benötigt werden, sollten die externen Zugänge standardmäßig deaktiviert sein und nur im Bedarfsfall aktiviert werden.
- Protokollierung von ZugriffenFernzugriffe sollten durch eine geeignete Protokollierung nachvollziehbar bleiben. Bei sehr hohem Schutzbedarf sollte erwogen werden, die Administrationssitzung mittels geeigneter Verfahren aufzuzeichnen.

Bei der Konzeption des Fernzugangs sollte darauf geachtet werden, die Nutzung unerwünschter Tunnel (TLS, SSH, IPsec) zur Umgehung von Sicherheitsmaßnahmen zu unterbinden. Durch solche Tunnel könnten Komponenten und Dienste der OT-Komponenten unerwünscht zugänglich werden.

IND.1.M9 Restriktiver Einsatz von Wechseldatenträgern und mobilen Endgeräten

Wechselmedien einerseits (z. B. USB-Stick) und mobile Endgeräte anderseits (z. B. Service-Laptop) haben sich zu Haupteinfallstoren für Angriffe entwickelt, da diese Komponenten häufig die sorgsam konstruierten Zonengrenzen überqueren und so missbraucht werden können, um Schadsoftware oder Befehle hinein oder sensible Informationen hinaus zu transportieren.

Regelungen zum Thema Wechselmedien und mobile Endgeräte

Die Regelung sollte auf den Anwendungsbereich eingehen und mögliche definierte Ausnahmen und abweichende Regelungen dokumentieren. Es sollten Vorgänge dokumentiert werden, in denen Wechseldatenträger genutzt werden.

Eine Nutzung von privaten Wechseldatenträgern oder anderen mobilen Endgeräten zum Datentransport oder Anschluss an OT-Komponenten sollte generell ausgeschlossen werden.

Einschränkung der Nutzung

Auf den OT-Komponenten sollte die Nutzung auf bestimmte Geräte eingeschränkt werden (Device Control). Dies ist meist mit Funktionen des Betriebssystems oder über zusätzliche Software möglich.

Ist der Transport von Medien oder Geräten zwischen verschiedenen Zonen notwendig, so muss ein Prozess existieren, mit dem die Medien bzw. Geräte abgesichert und geprüft werden. Für Dienstleister sollte ein gleichwertiger Prozess gelten.

Bei der Neuplanung von Anlagen und Systemen sollte auf die Nutzung verzichtet werden oder ein restriktiver Umgang und eine sichere Nutzung von Wechselmedien forciert werden.

Wechseldatenträgerschleuse (Quarantäne-PC)

Ein Quarantäne-PC kann stellvertretend für OT-Speichermedien auf Schadprogramme prüfen. Hierzu müssen die Mitarbeiter angewiesen werden, Speichermedien aus einer nicht vertrauenswürdigen Quelle (z. B. USB-Sticks) mittels des Quarantäne-PCs auf Schadprogramme zu überprüfen, bevor solche Datenträger in das OT-Netz eingebracht oder an OT-Komponenten mit keinem oder eingeschränktem Virenschutzprogramm angeschlossen werden.

Der Quarantäne-PC sollte einen aktuellen Patchstand der Virenschutzprogramme aufweisen und mit aktuellen Schadsoftware-Signaturen bespielt sein. Daher müssen die Signaturen von Quarantäne-PCs immer auf dem aktuellsten Stand sein.

Zusätzlich zu einer möglicherweise automatisierten Überprüfung der Speichermedien durch den Quarantäne-PC sollte immer auch ein manueller Prüfung für den Datenträger durchgeführt werden.

Nutzung mobiler Endgeräte

Auf Service-Laptops, Programmiergeräte und ähnliche Endgeräte, welche speziell im Bereich der OT eingesetzt werden, kann in der Regel nicht verzichtet werden. Hier sind daher besondere Überlegungen notwendig, damit die Sicherheit der OT-Infrastruktur nicht durch Schwachstellen in diesen Clients oder in deren Nutzung gefährdet wird.

Smartphones, Tablets und andere Mobilgeräte, welche nicht ausschließlich im OT-Netz verwaltet werden, sollten in der Regel nicht mit dem OT-Netz verbunden werden. Ist dies doch erwünscht, so sind diese angemessen abzusichern. Zur Absicherung dieser Geräte sollten zudem die einschlägigen IT-Grundschutz-Bausteine angewendet werden.

Einsatz von Notebooks zu Wartungszwecken

In Anwendungen kommen häufig Notebooks als mobile Wartungsgeräte zum Einsatz. Grundsätzlich ist vor jedem Einsatz zu definieren, welche Arbeiten auszuführen sind und der Mitarbeiter muss aufgrund seiner Ausbildung und Kenntnisse dazu in der Lage sein. Bei Arbeiten an Anlagen mit hohem Schutzbedarf (SIL, GMP etc.) ist durch Zusatzmaßnahmen sicherzustellen, dass keine unbeabsichtigten Änderungen vorgenommen werden.

Es sind technische Sicherungsmaßnahmen (z. B. Schutz der Konfigurationsdaten des Feldgerätes mittels entsprechender Brücke) oder alternativ organisatorische Maßnahmen (Vier-Augen-Prinzip) anzuwenden.

Interne Geräte

Über organisatorische Maßnahmen ist sicherzustellen, dass auf diesen Wartungsgeräten ausschließlich Software installiert ist, die für Wartungszwecke erforderlich ist. Es sollte eine Systemhärtung durchgeführt werden. Darüber hinaus sollten diese Geräte regelmäßig gepatcht und auf Malware (Schadprogramme) untersucht werden.

Externe Geräte

Für den Einsatz externer Wartungsgeräte empfiehlt sich zunächst der Abschluss eines entsprechenden Vertrages mit dem externen Anbieter, in welchem die informationssicherheitsrelevanten Themen (speziell Verhaltensregeln für die externen Mitarbeiter) vertraglich geregelt werden.

Vor dem Einsatz eines externen Wartungsgerätes ist eine Bestandsaufnahme erforderlich. Zu klären ist in diesem Zusammenhang:

- Welche Software ist installiert (inkl. Betriebssystem und Patches)
- Welche Schnittstellen sind vorhanden und aktiv (z. B. UMTS/GPRS/GSM)
- Welcher Schutz für Schadprogramme ist installiert (sind aktuelle Signaturen vorhanden?)

Ist diese Inventarisierung abgeschlossen und hat keine negativen Erkenntnisse geliefert, ist im nächsten Schritt eine Untersuchung auf Schadprogramme unter Nutzung eines den institutionsseitigen Festlegungen genügenden Antivirenschutz durchzuführen.Ist dieser Test erfolgreich abgeschlossen, so kann Zugang zur OT gewährt werden.

In diesem Zusammenhang hat sich bei verschiedenen Anwendern die Nutzung individueller Firewalls (USB betriebene Kompaktgeräte) bewährt. Diese werden zwischen die jeweilige OT-Komponente und das Wartungsgerät geschaltet und sollen ungewollte Aktivitäten unterbinden.

IND.1.M10 Monitoring, Protokollierung und Detektion [Bereichssicherheitsbeauftragter]

Durch das frühzeitige Erkennen von sicherheitsrelevanten Ereignissen kann zeitnah auf diese reagiert und somit ein möglicher Schaden begrenzt werden. Daher sollte im Vorfeld in einem Security Incident Response Plan eine Strategie entwickelt werden, wie sicherheitsrelevante Ereignisse erfasst und erkannt werden, welche Reaktionen erforderlich sind und wie ein sicherer Zustand wiederhergestellt werden kann. Der Security Incident Response Plan sollte die Phasen Planung, Reaktion und Wiederherstellung berücksichtigen und hierfür Prozesse z. B. zur Klassifizierung der Ereignisse, Benachrichtigung, Dokumentation, Untersuchung des Ereignisses und den daraus abgeleiteten Aktionen definieren.

Insbesondere sollten die Verantwortlichkeiten und Rollen sowie das weitere Vorgehen (z. B. Meldung an Behörden oder Veröffentlichung) festgelegt werden. Hier ist auch der Datenschutzbeauftragte einzubinden.

Der Plan sollte in regelmäßigen Abständen und mindestens jährlich erprobt, auf Aktualität geprüft und bei Bedarf überarbeitet werden.

Protokollierung

Logging dient dem frühen Erkennen von Fehlern und sicherheitsrelevanten Vorfällen wie beispielsweise unbefugte Zugriffsversuche auf Daten oder Identifikation von Übertragungsengpässen.

Die Protokollierungsdaten sollten auf einem zentralen Server gespeichert werden. So können die Protokollierungsdaten von verteilten Systemen und Komponenten zentral gesammelt, analysiert und in Zusammenhang gebracht werden.

In einem OT sollten mindestens die folgenden Ereignisse protokolliert und zentral gesammelt werden, soweit diese verfügbar sind:

- lokale Ereignisse, z. B. der Betriebssysteme,
  - Neustart von Diensten,
  - Systemstarts und Reboots,
  - Erfolgreiche und erfolglose Anmeldungen am System (Betriebssystem und Anwendungssoftware),
  - Fehlgeschlagene Berechtigungsprüfungen,
- Ereignisse von Domänen-Controllern, etwa
  - Einrichtung oder Änderungen von Benutzern, Gruppen und Berechtigungen,
- Firewall-/Router-/Switch-/Server-Ereignisse, vor allem
  - Blockierte Datenströme (Verstöße gegen ACLs oder Firewall-Regeln),
- Ereignisse der Virenschutzprogramme,
- sonstige sicherheitsrelevante Fehlermeldungen (z. B. Hardwaredefekte, Überschreitung von Kapazitätsgrenzen),
- Ereignisse des IDS/IPS.

Zusätzlich sollten zu den vorher genannten Ereignissen folgende Daten aufgezeichnet werden:

- Datum und Zeit (Es ist für alle Systeme eine gemeinsame Zeitquelle zu nutzen vgl. IND.1.M6 Änderungsmanagement in der OT - Zeitsynchronisation),
- Beschreibung des Ereignisses,
- Kritikalität,
- Quelle des Ereignisses, z. B. Anwendung, Betriebssystem.

Außerdem ist auf die geltenden Datenschutzbestimmungen zu achten.

Monitoring und Auswertung

Zur Gewährleistung des sicheren Wirkbetriebs sollte eine geeignete Infrastruktur für die betriebliche Überwachung des Systembetriebs konzipiert, implementiert und betrieben werden. Die Überwachung sollte neben der betrieblichen Verfügbarkeits- und Auslastungsüberwachung von Diensten, Systemen und Netzen auch die Auswertung sicherheitsrelevanter Ereignisse umfassen.

Dies wird in der Regel nicht erfolgen, wenn die Logs auf eine Vielzahl von Systemen verteilt sind. Daher sollte ein zentraler Protokollserver eingerichtet werden. Dieser muss geeignet in das Zonenkonzept eingebettet werden (siehe IND.1.M5 Entwicklung eines geeignete Zonenkonzepts). Gegebenenfalls sind mehrere Protokollserver notwendig, um die Trennung der Zonen aufrechterhalten zu können.

Die auflaufenden Protokolle müssen systematisch ausgewertet werden, damit nötigenfalls die geeignete Reaktion ausgelöst werden kann. Bei einer überschaubaren Anzahl von Systemen kann dies stichprobenartig erfolgen, hierfür ist mindestens eine (Rollen-)Verantwortung und eine Frequenz (je nach Schutzbedarf, z. B. wöchentlich) festzulegen. Bei einer größeren OT-Infrastruktur wird ausschließlich eine zumindest teilautomatisierte Auswertung erlauben, kritische Ereignisse zu erkennen.

Auf Grundlage von auftretenden Ereignissen und Grenzüberschreitungen bei überwachten Werten sollte ein Alarm ausgelöst werden, der den IT-Betrieb der Komponente über das Ereignis informiert.

Die folgende Liste veranschaulicht mögliche Beispiele für solche Ereignisse und Muster:

- Auffälliges Verhalten, welches typisch für Schadprogramme ist (z. B. erhöhter Netzverkehr, Abnahme der Performance, zunehmende Fehler in Anwendungen und Integritätsverletzungen),
- Hardware-Defekte wie fehlerhafte Sektoren bei Datenspeichern (z. B. Festplatte) oder ausfallende Komponenten aufgrund von Hardware-Fehlern,
- Verlust der Netzverbindung,
- ungewöhnlicher Anstieg der CPU-Last und des Speicherverbrauchs.

Implementierung von Intrusion-Detection- bzw. Intrusion-Prevention-Systemen

Mithilfe von Intrusion-Detection Systemen (IDS) und Intrusion-Prevention Systemen (IPS) lassen sich Angriffsversuche in einer frühen Phase erkennen, sodass der IT-Betrieb frühzeitig alarmiert wird (IDS) oder bereits eine automatisierte Reaktion auf den Angriff eingeleitet wird (IPS).

Hierzu arbeiten IDS/IPS auf der Grundlage von Heuristiken, um Angriffsversuche von gewöhnlichen, gewünschten Verhalten und Daten zu unterscheiden. Demgemäß müssen diese Heuristiken regelmäßig aktualisiert werden. Bei der Aktualisierung der Heurisitiken sollten die Hinweise zur Aktualisierung von Virensignaturen berücksichtigt werden. Darüber hinaus müssen die Heuristiken auf die OT und seine individuelle Gegebenheiten angepasst werden. Typische Vorfälle und Ereignisse, die durch ein solches System erkannt werden können, sind z. B. unbefugte Zugriffe auf Systeme und die unbefugte Installation von Software oder Manipulationen von Daten. Zudem können hierdurch auch unbeabsichtigte und versehentliche Änderungen (z. B. in Konfigurationsdateien) bemerkt werden.

Ein IDS/IPS kann einzelne Server überwachen (Hostbasierte IDS/IPS; HIDS/HIPS) oder durch Sensoren im Netz den Datenverkehr prüfen (netzbasiertes IDS/IPS; NIDS/NIPS).

Wird ein NIDS/NIPS verwendet, so sollten die Sensoren im Netz zur Überwachung des Datenverkehrs insbesondere bei externen Schnittstellen platziert werden (z. B. DMZ). Von externen Schnittstellen geht gewöhnlich eine höhere Bedrohung durch Angriffe aus (z. B. Internet). Ebenso sollte ein HIDS auf allen OT-Komponenten installiert werden. Die Protokolldaten des HIDS sollten in ein zentrales Logging integriert werden.

IDS/IPS sollten als zusätzliche Schutzmaßnahme angesehen werden und ersetzen kein Monitoring der Systeme und des Netzes (z. B. mittels eines Security Information Event Management (SIEM) Systems).

Der Einsatz und der Betrieb eines IDS können nur größeren Institutionen empfohlen werden, da die Einrichtung, die Pflege und die Sichtung der Meldungen (insbesondere in der Anfangsphase) mit einem nicht unerheblichen Aufwand verbunden sind. In kleineren Anlagen ist der Aufwand und der Nutzen vorab zu prüfen und es sind eventuell alternative Härtungs- und Schutzmaßnahmen umzusetzen.

Bei der Umsetzung eines IPS ist zudem zu beachten, dass bei der Planung auch sehr spezielle Situationen berücksichtigt werden, damit diese legitimen Übertragungen nicht verhindert werden. Vor einer Aktivierung dieser Funktionen ist daher eine sehr sorgfältige Probephase zu absolvieren.

Die Effektivität eines IDS/IPS ist stark abhängig von einer angepassten und individuellen Konfiguration. So kann die Effektivität beispielsweise durch eine hohe Anzahl an immer wiederkehrenden False Positives beeinträchtigt werden. Insbesondere IPS sollten mit Bedacht eingesetzt werden. Vorrangig ist hier der laufende Betrieb, der durch ein fehlerhaftes Eingreifen des IPS gestört werden könnte.

Daher erfordert nicht nur die initiale Konfiguration des IDS/IPS ein geschultes Fachpersonal, sondern auch im Betrieb muss mindestens eine Person im Notfall einen gemeldeten Angriffsversuch von einem False Positive unterscheiden können. Diese Person sollte ständig erreichbar sein, sodass nach der Klassifizierung der Meldung entsprechende Gegenmaßnahmen eingeleitet werden können.

IND.1.M11 Sichere Beschaffung und Systementwicklung

Entwicklung und Integration

OT-Komponenten werden als Verbund von Hard- und Software ausgeliefert. Die Anpassung auf die individuellen Gegebenheiten und Bedürfnisse wird durch die Konfiguration realisiert. In vereinzelten Fällen kann es notwendig sein, eigene Software zu entwickeln (z. B. Skripte, Batch-Dateien zur Stapelverarbeitung), um gewisse Automatismen oder Funktionen nachträglich zu integrieren. Werden eigene Programme oder auch Skripte entwickelt, so sollte sowohl die sichere Erstellung (Secure-Coding-Guidelines) der Programme als auch die sichere Integration in die bestehende Umgebung durch eine interne Softwareentwicklungsrichtlinie geregelt werden.

Vertraulichkeitsvereinbarung mit den Herstellern, Lieferanten und externen Betreibern

Die Institution sollte mit Vertragspartnern (Hersteller, Lieferanten oder externe Betreiber) Vertraulichkeitsvereinbarungen treffen. Diese sollten insbesondere Mitarbeiter des Vertragspartners mit relevanten Informationen und Kenntnissen der Informationssicherheit über die OT der Institution berücksichtigen (z. B. für den Fall, dass Mitarbeiter des Vertragspartners die Position oder Firma wechseln).

Darüber hinaus sollte geregelt werden, wie die Verfügbarkeit der OT erhalten werden kann, falls der Vertragspartner keine Wartungsdienste oder Dienstleistungen mehr anbietet (z. B. wegen Insolvenz des Vertragspartners). So sollte der Institution beispielsweise der notwendige Zugriff auf diese Systeme auch weiterhin möglich und ausreichend Dokumentation zur Wartung und zum Betrieb der OT verfügbar sein.

Im Fall der Geschäftsaufgabe eines Vertragspartners sollte vertraglich geregelt sein, dass ausgehändigte, vertrauliche Informationen an die Institution zurückzugeben sind.

Langfristige Gewährleistung der Informationssicherheit

Die Institution, Systemintegratoren und Hersteller sollten bereits bei der Planung eine Strategie erarbeiten, wie langfristig die Informationssicherheit der Anlage gewährleistet werden kann. Dies gilt für die gesamte Laufzeit der Anlage. Dies umfasst auch die weitere Nutzung von abgekündigter Software. Es sollten daher bereits frühzeitig alternative Schutzmaßnahmen berücksichtigt werden.

Kompatibilität

Das zu beschaffende OT und deren Komponenten sollten gängige Standards der jeweiligen Technologie umsetzen und gemäß dieser Standards kompatibel zu anderen Systemen sein. Dazu sollten diese nach Möglichkeit etablierte, marktübliche Informationssicherheitsmechanismen unterstützen.

Verzicht auf überflüssige Produktfunktionen

Falls OT-Komponenten Dienste oder Schnittstellen besitzen, die nicht für den Betrieb benötigt werden, sollten nach Möglichkeit entfernt oder zumindest deaktiviert werden. Die durchgeführten Änderungen an der OT sollten nachvollziehbar dokumentiert werden.

Mitteilung der Informationssicherheitsanforderungen an den Systemintegrator und Hersteller

Die Informationssicherheitsanforderungen der Institution für die OT, die sich aus der Risikoanalyse ergeben, sollten dem Hersteller und Systemintegrator, der die Anlage realisiert, mitgeteilt werden. Dieses sollte als Bestandteil des Lastenhefts erfolgen.

Die Anforderungen sollten auf Basis der konkreten Anwendungen formuliert werden. So können sie sich auf geforderte Eigenschaften oder Informationen beziehen. Es sollten keine Lösungen, sondern Anforderungen beschrieben werden. Der Erfüllungsgrad der Anforderungen sollte bei der Wahl der Lösung und des Integrators berücksichtigt werden.

Berücksichtigung der Informationssicherheitsspezifikationen des Herstellers und Systemintegrators

Die Institution muss die Informationssicherheitsspezifikation, die der Hersteller und der Systemintegrator bereitstellt, im Zyklus der Risikoanalyse berücksichtigen. Aufbauend auf den Informationen des Herstellers und Systemintegrators können weitere Maßnahmen durch die Institution definiert werden.

Robustheit der Produkte

Neben der Hardware (z. B. Industrie-Rechner) sollte auch die Software (z. B. Protokollstack, OT-Anwendungen) robust auf ungültige Eingaben reagieren. So sollten beispielsweise ungültige Netzpakete nicht zum Absturz oder zu Fehlern der Software führen, sondern von dem Protokollstack ignoriert und bei Bedarf protokolliert werden.

Die Robustheit der Komponenten sollte bereits durch die Hersteller sichergestellt werden. Diese Anforderung sollte bereits bei der Anschaffung neuer Komponenten durch die Institution gefordert werden.

Unterstützung von Virenschutz-Lösungen

Falls notwendig sollten die zu beschaffenden OT-Komponenten mit einem Schadsoftwareschutzprogramm ausgestattet sein oder zumindest den Betrieb von Schadsoftwareprogrammen unterstützen. In der Regel unterstützt der Hersteller ausgewählte Produkte (siehe auch IND.1.M3 Schutz vor Schadprogrammen).

Abnahme- und Integrationstests

Im Rahmen der Abnahme- und Integrationstests sollte die Umsetzung der Sicherheitsanforderungen sowie die Interoperabilität geprüft und verifiziert werden.

Im besonderen Fokus sollte die Handhabung und Wirksamkeit von Backup- und Recovery-Maßnahmen stehen.

IND.1.M12 Etablieren eines Schwachstellen-Managements

Fehler in der Software stellen ein Problem. Durch die hierdurch verursachten Schwachstellen kann ein Angreifer Zugriff auf das System erlangen oder den Ablauf der Software stören. Daher gilt grundsätzlich, dass diese Fehler behoben werden sollten oder aber ihre negativen Auswirkungen anderweitig begrenzt werden müssen.

Schwachstellen

Wie bei allen IT-Systemen enthalten OT-Komponenten, -Systeme, -Anwendungen und -Protokolle Schwachstellen. Da diese die Sicherheit grundsätzlich bedrohen, ist ein Prozess zum Umgang mit ihnen notwendig.

Dabei ist zwischen verschiedenen Fällen zu unterscheiden: Für eine Komponente (Produkt, System, Anwendung) sind

- keine Schwachstellen öffentlich bekannt. Dies kann sich jederzeit ändern.
    - Außerdem können Schwachstellen nur bestimmten Parteien bekannt sein, die diese aus unterschiedlichen Gründen nicht veröffentlichen möchten.1Die Ausnutzung einer Schwachstelle, bevor die Schwachstelle öffentlich bekannt gegeben wurde, ist ein sogenannter „Zero?Day(?Exploit)“.
- Schwachstellen bekannt und der Hersteller hat
    - Patches bereitgestellt. Diese wurden vom Integrator/Maschinen-/Anlagenbauer für die OT
        - freigegeben
        - nicht freigegeben
    - noch keine Patches bereitgestellt. Der Hersteller plant:
        - Patches bereitzustellen
        - keine Patches bereitzustellen. In diesem Fall muss das Risiko des Weiterbetriebs betrachtet und entsprechende technische oder organisatorische Maßnahmen getroffen werden. Ansonsten müssen solche Komponenten (Hardware wie Software) ausgetauscht werden.

Ziel des Schwachstellen-

Für alle zutreffenden Fällen sollte das Schwachstellen-Management Vorgehensweisen liefern können. Dieses sollte grundsätzlich in die sonstigen Vorgehensweisen zum sicheren Betrieb der Betriebs- und Steuerungstechnik integriert werden (siehe IND.1.M16 Änderungsmanagement in der OT).

Das Schwachstellen-Management muss Lücken in Software, Komponenten, Protokollen und Außenschnittstellen der Umgebung identifizieren und mögliche Handlungsbedarfe und -möglichkeiten (z. B. ein Patchmanagement) ableiten, bewerten und umsetzen.

Bestandsanalyse

Bei der Ersteinführung des Schwachstellen-Managements muss einmal eine Schwachstellenanalyse der Ausgangslage zum Ableiten von Handlungsbedarfen durchgeführt werden. Auf Grundlage der Bestandsinfrastruktur muss die Institution dafür alle bestehenden Schwachstellen aller verbauten Komponenten (Produkte, Anwendungen, Systeme, Protokolle, Außenschnittstellen) identifizieren. Grundlage hierfür sollten Schwachstellenmeldungen (Advisories) von Herstellern und öffentlich verfügbare CERT-Meldungen sein. Ergänzend hierzu können organisatorische und technische Audits zur Schwachstellenanalyse durchgeführt werden. Dies ist insbesondere bei höherem Schutzbedarf und bei besonderer Exponiertheit (z. B. Schnittstellen zum Internet) zu empfehlen.

Ein Einspielen sicherheitsrelevanter Updates im Rahmen eines systematischen Patchmanagements kann eine Möglichkeit sein, bestimmte Schwachstellen zu schließen. Hierfür muss ein geeignetes Verfahren für die jeweilige Umgebung bestimmt werden, ob, wie und wann Patches ausgebracht werden können.

Bewertung von Schwachstellen

Um relevante Schwachstellen zeitnah, systematisch, fachlich angemessen und wirtschaftlich bewerten und die richtigen Schlussfolgerungen ziehen zu können, ist die Festlegung eines Verfahrens zur Bewertung von Schwachstellen notwendig. Hierbei sollte definiert werden, wer (welche Rolle(n)) wann (in welcher Frequenz) welche Informationsquellen (Nachrichten, Advisories, E-Mail-Verteiler, Datenbanken etc.) abonniert, sichtet und auswertet. In kleineren Organisationen bietet es sich an, diese Aufgaben beim ICS-Informationssicherheitsbeauftragter zu bündeln. In größeren Strukturen mit vielen System- und Anwendungstypen wird eine Aufgabenteilung notwendig sein. Aus den möglichen Auswirkungen einer Schwachstelle (gefolgert aus dem Schutzbedarf) und der Exponiertheit (Einfachheit der Ausnutzbarkeit) sollte eine Kritikalität abgeleitet werden, welche die Priorität für das weitere Vorgehen vorgibt. Es kann ein standardisierter Bewertungsmaßstab wie CVSS verwendet werden. Für kleinere Organisationen reicht in der Regel eine zwei- oder dreistufige qualitative Skala:

- unkritisch (geringe Auswirkungen oder vernachlässigbare Exponiertheit): Weiter zu beobachten.
- mittel (maximal mittlere Auswirkungen oder Exponiertheit): Behandlung im Rahmen der nächsten regulären Softwarepflege
- kritisch (kritische Auswirkung oder hohe Exponiertheit): Prioritäre außerplanmäßige Behandlung (Informationssicherheitsbeauftragter entscheidet über das weitere Vorgehen)

An den Bewertungsprozess angeschlossen sein sollte ein Vorgehen zur Software-Pflege: Je nach Bereich (z. B. nach Zone) können unterschiedliche Vorgaben definiert sein, wann, wie oft und wie Schwachstellen ab einer bestimmten Kritikalität gepatcht werden bzw. welche alternativen Maßnahmen in Kraft sein müssen, damit auf das Patchen verzichtet werden kann. Bei jeder neuen Art von Schwachstelle und jeder Fortentwicklung von Angriffstechniken ist zu prüfen, ob die etablierten Ersatzmaßnahmen weiterhin ausreichen oder ob diese ergänzt werden müssen.

Patchen

Wo Patchen möglich ist, dessen Risiken abgeschätzt sind und tragbar erscheinen, sollte ein Patchprozess mit rollenspezifischen Verantwortlichkeiten definiert werden, welcher neben den vom Hersteller freigegebenen Patches und Updates ebenso zusätzliche Drittanbieter-Software berücksichtigt (z. B. Büroanwendungen, PDF-Reader). Der Prozess sollte mindestens folgende Elemente beinhalten:

- Regelmäßige Prüfung auf neue Schwachstellenmeldungen bei den Herstellern der OT-Komponenten oder Drittanbieter-Software
- Bewertung der Kritikalität von Patches, beispielsweise mit Common Vulnerability Scoring System (CVSS),
- Beziehen der Patches und Updates,
- Testen (dies sollte auf einer Testumgebung (baugleiche Komponente) erfolgen),
- Freigabeprozess,
- Umgang mit Hersteller-Freigaben von Patches und
- Umgang mit dem Patchen von zusätzlicher Software.

Bezugsquellen für die Meldung von Schwachstellen sind die Hersteller oder auch CERTs.

CVSS ist eine Methodik zur Bewertung und Klassifizierung von Schwachstellen in Abhängigkeit des individuellen Risikos des einzelnen Betriebs. In die Basis-Bewertung (Base-Score) fließt unter Anderem ein, wie die Schwachstelle ausgenutzt werden kann (z. B. lokal oder entfernt) und welche Konsequenzen drohen (z. B. Denial of Service oder Code-Ausführung). Ein zweiter Wert (temporal-score) bewertet über die Zeit veränderbare Rahmenbedingungen. Dazu zählt z. B. die Verfügbarkeit von Exploit-Code. Eine dritte Komponente stellt den Bezug zur lokalen Umgebung des Anwenders her. Dieser muss anhand seiner Umgebung einschätzen, was dies Schwachstelle für ihn bedeutet. Die ersten beiden Informationen werden auf verschiedenen Webseiten zu Schwachstellen zur Verfügung gestellt (z. B. CVE MITRE).

Das Einspielen von Patches und Updates erfordert gewöhnlich die Freigabe durch den Hersteller der OT-Komponente. Daher können in der Regel z. B. bereits im Internet verfügbare Patches und Updates durch die Institution nicht eingespielt werden, da ein Funktionsverlust möglich wäre und durch den Hersteller keine Garantie übernommen würde.

Aus diesem Grund sollte die Institution mit dem Hersteller vertraglich Zeiträume zur Freigabe und Bereitstellung von Patches und Updates oder alternativen Workarounds für Schwachstellen festlegen, insbesondere dann, wenn solche Eingriffe Auswirkungen auf die Zulassung eines Systems haben können. Die Zeiträume sollten möglichst kurz gewählt werden, da in diesem Zeitfenster das betroffene System durch die Schwachstelle einem erhöhten Risiko ausgesetzt ist.

Sofern die Möglichkeit besteht, kann die Institution vor der Installation eigenständig Tests durchführen. Alternativ sollten die Updates sequenziell installiert und getestet werden. Hierbei sollten zuerst redundante Systeme bespielt werden. Vor dem Einspielen von Patches und Updates wird empfohlen, für jedes System eine Datensicherung durchzuführen. Dies betrifft insbesondere OT-Systeme, die notwendig für die Produktion sind. OT mit keiner oder geringer Bedeutung für die Produktion können auch ohne vorherige Datensicherung und umfangreiche Tests gepatcht werden.

Zudem sollte geprüft werden, ob ein Neustart nach dem Patch durchgeführt wird oder erforderlich ist. Dies muss bei der Planung berücksichtigt werden.

Insgesamt sollte das Einspielen von Patches in die Betriebszyklen der Anlage integriert werden. So können Wartungsfenster an der Anlage genutzt werden, um Patches zu installieren. Bei redundant ausgelegten Komponenten kann ein schrittweises Vorgehen gewählt werden, um den Zeitpunkt der Installation nicht zu lange aufzuschieben.

Alternativen zum Patchen

Steht kein Patch zur Verfügung, sollten in einer Sicherheitsbetrachtung alternative Maßnahmen betrachtet und ergriffen werden, um die Ausnutzung der Schwachstelle zu verhindern. Lösungen können zum Beispiel zusätzliche Tools sein, die eine Ausnutzung von Schwachstellen verhindern oder Änderungen verhindern. Als alternative Maßnahme ist es beispielsweise möglich, die betroffene OT in ein separates Netzsegment zu platzieren und den Datenverkehr zu diesem Netzsegment mittels einer Firewall zu filtern (siehe IND.1.M5 Entwicklung eines geeigneten Zonenkonzepts).

Umgang mit End-Of-Support / End-Of-Life (EOS/EOL)

Falls für OT-Komponenten oder darin verwendeter Software der End-of-Support erreicht wird, führen diese Komponenten zu einem erhöhten Betriebsrisiko. Dies gilt im Speziellen für Software aus dem IT-Umfeld (z. B. Betriebssysteme). In diesem Fällen ist es möglich, dass weiterhin Schwachstellen entdeckt werden, diese jedoch nicht mehr geschlossen werden. In diesem Fall sind möglicherweise zusätzliche Schutzmaßnahmen notwendig, z. B. die Migration auf eine neue Soft- oder Firmware-Version oder Hardware-Revision.

Hierfür sollte eine Sicherheitsbetrachtung durchgeführt werden und darauf aufbauend sollten in Abhängigkeit der Funktion der OT und Bedeutung für die Produktion angemessene Informationssicherheitsmaßnahmen identifiziert werden. So kann beispielsweise eine Separierung der OT mit ungepatchten Schwachstellen in ein eigenes Netzsegment und einer restriktiven Firewall zur Filterung des Datenverkehrs die Systeme schützen.

Langfristiges Ziel sollte der Austausch der betroffenen OT-Komponenten durch vom Hersteller unterstützte Komponenten sein. Ohne Support durch den Hersteller können zukünftig auftretende Fehler und Ausfälle die Produktion stark beeinträchtigen, da die Erarbeitung von Lösungen ohne Hilfe durch den Hersteller aufwendiger ist.

Es sollte insbesondere bei der Anschaffung darauf geachtet werden, dass keine Komponenten zum Einsatz kommen, die bereits durch den Hersteller abgekündigt wurden.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

IND.1.M13 Notfallplanung für OT (A)

Notfallmanagement

Viele Organisationen verfügen aufgrund unterschiedlicher Anforderungen bereits über ein Notfallmanagement, welches bestimmte Szenarien abdeckt. Im Bereich der OT sollten diese um Notfallpläne mindestens für folgende Szenarien ergänzt werden:

- Komplettausfall der Internetanbindung inklusie Fernwartung für längere Zeit (> 1 Woche)
- Komplettausfall der Office-IT für eine bestimmte Zeit (z. B. 2 Tage)
- Temporärer Ausfall kritischer IT-Komponenten im OT-Bereich für einen Zeitraum, der mit Standardbetriebsprozessen nicht auffangbar ist
- Kompromittierung kritischer IT-Komponenten im OT-Bereich durch einen unbekannten Angreifer bzw. durch Schadprogramme

Falls bereits ein Business Continuity Management (BCM) besteht, kann das Notfallmanagement für die OT-Infrastruktur in dieses integriert werden. Andernfalls sollte ein BCM eingerichtet werden, etwa nach IT-Grundschutz (Baustein DER.4 Notfallmanagement bzw. BSI-Standard 100-4), welches die OT-Infrastruktur umfasst.

Systemsicherung und -wiederherstellun

Für die OT sollte ein Sicherungs- und Wiederherstellungskonzept erstellt werden. Grundlage hierfür können die bewährten Verfahren der Office-IT (siehe Baustein OPS.1.1.5 Datensicherung) sein. Darüber hinaus können ergänzende system- bzw. komponentenspezifische Sicherungsverfahren für Systeme erforderlich werden, die nicht in klassische Sicherungslösungen eingebunden werden können.

Die Sicherungsinfrastruktur der OT sollte möglichst unabhängig von der Infrastruktur der Office-IT-Lösung betrieben werden. Bei der Nutzung einer gemeinsamen Infrastruktur sollten die durch die Abhängigkeiten entstehenden Risiken betrachtet und angemessen berücksichtigt werden. Dies gilt insbesondere auch für die Ablage von Systemsicherungen oder Projektdaten auf Dateiservern der Office-IT.

Wiederherstellungsplan

In einem Wiederherstellungsplan sollte festgelegt werden, wie grundlegende Funktionen in der OT nach einer signifikanten Störung wieder aufgenommen werden können. Es sollten im Vorfeld Aktionen abgeleitet werden, die nach Eintritt einer Produktionsstörung oder eines Sicherheitsvorfalls den Wiederanlauf der Produktion in einer angemessenen Zeit sicherstellen. Dazu zählen beispielsweise Prozesse zur Datensicherung, Wiederherstellung und dem regelmäßigen Testen von Backups, Prozeduren zur Systemwiederherstellung, Reparatur defekter Komponenten und Vorhalten von Ersatzteilen als auch alternative Kommunikations- und Steuerungsmöglichkeiten bei Ausfällen.

Der Plan sollte in regelmäßigen Abständen und mindestens jährlich auf Aktualität geprüft und bei Bedarf überarbeitet werden.

Notfallplan und -vorgehensweisen müssen mit geltenden Gesetzen und anderen regulatorischen Anforderungen kompatibel sein. Die Notfallplanung für die OT-Infrastruktur lässt sich entweder in ein bestehendes Notfallmanagement integrieren oder aber als eigenständiges Notfallmanagement für die OT etablieren. In letzterem Fall kann das OT-Notfallmanagement auch Teil eines bereits bestehenden OT-Krisenmanagements sein.

Die Organisation muss Notfallpläne für zu definierende Kategorien von Ausfällen und anderen Krisen entwickeln. Für den Fall des Ausfalls der gesamten oder Teile der OT oder wichtiger Kommunikationsverbindungen müssen vordefinierte Maßnahmen ausgeführt werden (z. B. den gesteuerten Prozess sicher herunterfahren oder letzten Betriebszustand vor dem Ereignis aufrechterhalten).

Wiederherstellung der OT-Infrastruktur in einen sicheren Zustand bedeutet, dass alle Systemparameter (Standardparameter wie organisationsspezifische) auf sichere Werte gesetzt sind, sicherheitskritische Updates (wieder) installiert sind, sicherheitsrelevante Einstelllungen wiederhergestellt sind, Systemdokumentationen und Bedienungsanleitungen verfügbar sind, aktuelle, verifizierte Backups wiederhergestellt sind und das Gesamtsystem voll getestet und funktional ist.

Evaluierung des Notfallmanagements

Das OT-Notfallmanagement muss regelmäßig (z. B. einmal jährlich) evaluiert werden. Dafür sollte die Organisation ein Testverfahren auswählen (z. B. vollumfängliche Simulation oder Table-Top-Excercise), dessen Testtiefe und -abdeckung der Kritikalität der OT-Infrastruktur angemessen ist.

Redundanz

Bezüglich Redundanzen als wichtige Maßnahme der Business Continuity gilt im OT-Bereich grundsätzlich dasselbe wie für Office-IT. Die Ausgestaltung und Dimensionierung der Redundanzen hat dabei immer den Schutzbedarf zu beachten und muss alle betriebskritischen Elemente der OT-Umgebung abdecken, also auch Stromeinspeisung, Versorgungsleitungen, Datenkabel, aktive Netzkomponenten etc.

Wenn sehr hohe Verfügbarkeitsbedarf besteht, so sollte eine alternatives Kontrollzentrum (Warte, Leitstand etc.) aufgebaut werden, welches bei Ausfall des Hauptkontrollzentrums in einem gewissen Zeitrahmen, welcher von der Organisation mithilfe des Schutzbedarfs zu definieren ist, einsatzbereit ist (sogenannter Notfallstandort). Dieser Notfallstandort sollte

- geographisch getrennt sein, sodass ein Einwirken einer Naturkatastrophe auf beide Standorte unwahrscheinlich ist,
- im Notfall erreichbar sein (auch bei regionalen Ausfällen von Strom und anderen Diensten),
- über notwendige Dienstleisterverträge mit der angemessenen Priorität abgedeckt sein und
- ständig so weit konfiguriert sein, dass er im gesetzten Zeitrahmen einsatzfähig ist.

IND.1.M14 Starke Authentisierung an OT-Komponenten (CIA)

Soweit möglich sollte die Nutzung aller OT-Komponenten eine Authentisierung der Benutzer und Dienste erfordern, sodass eine Bedienung der Systeme nur im authentisierten Zustand möglich ist. Dazu zählen neben gewöhnlichen Rechnern auch Router, Switches und SPS.

Zur Authentisierung können unterschiedliche Verfahren und Merkmale eingesetzt werden. Es wird zwischen den Authentisierungsmerkmalen Wissen (z. B. Passwort, PIN), Besitz (z. B. Token, Smartcard, Zertifikat) und körperliche Merkmale (z. B. Fingerabdruck, Iriserkennung) unterschieden. Auch der Aufenthaltsort des Zugreifenden kann indirekt als Merkmal betrachtet werden, wenn sichergestellt ist, dass dieser nur mittels eines oder mehrerer weiterer Merkmale an diesen Ort gelangen konnte. Ein Beispiel ist eine Warte, die nur mit einem Schlüssel oder nach einer (beiläufigen) Gesichtskontrolle durch Kollegen betreten werden kann.

Mehrfaktorauthenti

Bei erhöhtem Schutzbedarf sollten mehrere Merkmale zur Authentisierung herangezogen werden und so ein höheres Informationssicherheitsniveau etablieren (z. B. Zwei-Faktor-Authentisierung mittels Token und Passwort). Hierbei sollten Merkmale aus unterschiedlichen Klassen (Wissen, Besitz, Biometrie, Ort) kombiniert werden.

Bei der Auswahl der Authentisierungsmethoden ist eine Sicherheitsbetrachtung durchzuführen. Diese muss mit weiteren Anforderungen (z. B. Störfallverordnung) und organisatorischen Rahmenbedingungen (z. B. Zugangsrestriktionen) abgeglichen werden, um zu einer geeigneten Auswahl zu kommen.

Zentrale Verwaltung von Authenti

Die Verwaltung der genannten Anforderungen sollte vorzugsweise über eine zentrale Management-Lösung realisiert werden (z. B. in einem Verzeichnisdienst). Dabei sollte keine zusätzliche Abhängigkeit von anderen Zonen eingeführt werden. Dies kann dadurch erreicht werden, dass der Verzeichnisdienst innerhalb der Zone betrieben wird, für die er benötigt wird. Informationen aus einem Verzeichnisdienst in einer anderen Zone können bei Bedarf repliziert werden.

Nicht alle hier genannten Maßnahmen sind voll umfassend auf alle OT-Komponenten sinnvoll anwendbar. So kann beispielsweise ein Angreifer durch provozierte, fehlgeschlagene Anmeldeversuche den Benutzerzugang sperren. Somit wäre ein Zugriff auf das betroffene System durch den legitimen Benutzer nicht mehr möglich. Daher muss der Sicherheitszugewinn durch die jeweilige Maßnahme und mögliche Einschränkungen sonstiger Anforderungen an die OT-Komponenten (z. B. erforderlicher, unmittelbarer Zugriff) gegeneinander abgewogen werden. Es sollte immer ein Notfallprozess existieren, durch den im Fall der Störung der Authentisierung der Betrieb aufrechterhalten werden kann. In diesem Zusammenhang sollten die für den automatisierten Betrieb erforderlichen technischen Benutzer- und Dienstezugänge möglichst nicht von einem Verzeichnisdienst abhängig sein.

IND.1.M15 Prüfung und Überwachung von Berechtigungen (CIA)

Notwendig Grundlage für diese Maßnahme ist, dass IND.1.M7 Etablieren einer Berechtigungsverwaltung ordnungsgemäß umgesetzt wurde. Im Fall des erhöhten Schutzbedarfs werden die Anforderungen an die Berechtigungsverwaltung folgendermaßen erhöht. Ziel ist, dass ein Missbrauch einfacher und schneller verhindert oder zumindest erkannt werden kann.

Revisionssichere Pflege einer Bestandsübersicht und Historie

Nach IND.1.M7 Etablieren einer Berechtigungsverwaltung gilt: Das Berechtigungsmanagement muss eine vollständige Übersicht über die an eine Person vergebenen Berechtigungen besitzen. Diese Übersicht muss auch die Berechtigungshistorie einer Person sowie Informationen über den jeweils gestellten Berechtigungsantrag und durchgeführten Prüf- und Freigabeprozess umfassen.

Dies stellt also eine Zuordnung von Benutzern zu (Mengen von) Rechten dar. Zusätzlich soll die Bestandsübersicht jedoch umgekehrt darüber Auskunft geben können, welche Zugriffsrechte auf bestimmten Systeme und Anwendungen gelten, also die Zuordnung Anwendung bzw. System zu Anwendern und Rechten. Zumindest für alle kritischen Systeme sollte dies vorliegen und aktuell sein. Idealerweise werden hier die effektiven Berechtigungen dargestellt – also die tatsächlich im System technisch gesetzten anstelle der aus der historischen Setzung und Löschung ableitbaren. Dies hat den Vorteil, dass eine Chance besteht, illegitim am Berechtigungsprozess vorbei hinzugefügte Berechtigungen zu erkennen.

Automatisierte Auswertung

Es bietet sich an, die Zusammenstellung der effektiven Berechtigungen automatisiert vorzunehmen und dabei gleichzeitig eine Auswertung durchzuführen. So könnten Änderungen (Deltas) gemeldet werden oder Abweichungen von einem Standard- oder Sollzustand besonders dargestellt werden.

Protokollierung kritischer Tätigkeiten

Kritische Berechtigungen können auf unterschiedliche Arten missbraucht werden:

1 durch Innentäter
2 durch Social Engineering
3 unabsichtlich durch Fehlhandlungen
4 unbewusst durch einen kompromittierten Client oder Kommunikationskanal

Zum ersten Fall lässt sich die Wahrscheinlichkeit mindern, zu den anderen zumindest die Nachvollziehbarkeit und Aufklärung verbessern, wenn kritische administrative Tätigkeiten protokolliert werden. Dies sollte zentral erfolgen und Bedarf einer systematischen Auswertung (vgl. IND.1.M10 Monitoring, Protokollierung und Detektion). Um in den Fällen 1 und eventuell auch 4 effektiv sein zu können, dürfen die Protokolle nicht einfach durch dieselbe Rolle gelöscht oder manipuliert werden können, deren Handlung protokolliert wurde. Zumindest sollte eine Löschung oder Manipulation an eine weitere, unabhängige Rolle gemeldet werden. Noch besser ist, die Löschung oder Manipulation technisch zu verhindern und Versuche der Löschung oder Manipulation automatisch an eine unabhängige Rolle zu melden.

IND.1.M16 Stärkere Abschottung der Zonen (IA)

Schnittstellen zu Zonen mit hohem oder sehr hohem Schutzbedarf können eine stärkere Abschottung erfordern, als dies durch Layer-4 Firewall-Systeme oder durch die oft eingeschränkten Absicherungsmöglichkeiten von OT-Komponenten möglich ist. Insbesondere bei Außenschnittstellen der OT und Office-Netz sollten die Schnittstellen einer Sicherheitsbewertung unterzogen werden.

Die Sicherheitsbewertung sollte unter Berücksichtigung der Ausgestaltung der jeweiligen Schnittstelle auf Basis der Elementaren Gefährdungen erfolgen. Bei dieser Vorgehensweise sind zunächst die relevanten Elementaren Gefährdungen zu bestimmen und die jeweilige Schnittstelle auf angemessenen Schutz zu untersuchen. Aus dieser Betrachtung heraus kann es erforderlich werden, Schnittstellen zu verwerfen oder diese gegen die ermittelten Bedrohungen zusätzlich abzusichern, wenn die etablierten Sicherheitsmaßnahmen die ermittelten Gefährdungen nicht hinreichend abdecken.

Die jeweils erforderlichen Schutzmaßnahmen ergeben sich aus der Risikobetrachtung und können auch Anpassungen an den kommunizierenden OT-Komponenten wie Härtung, Antivirenschutz, Patch-Management oder Vergabe minimaler Recht erfordern. Aufgrund der dort häufig eingeschränkten Handlungsmöglichkeiten können solche Schutzmaßnahmen auch auf einem Schnittstellensystem realisiert werden. Zu diesem Zweck kann der Aufbau einer DMZ in Betracht gezogen werden.

Die Kommunikation zwischen den betrachteten Sicherheitsbereichen (etwa externer Zugriff in die OT) wird in dieser DMZ durch Application-Layer-Gateways (ALG) wie etwa Proxy oder Datentransferserver terminiert. Dabei können auf dem Gateway spezifische Inhaltsprüfungen wie etwa Prüfung auf Schadprogramme oder Datenformatprüfungen (z. B. XML-Prüfung durch eine Web Application Firewall oder Protokollprüfungen durch Industrie-Firewalls) vorgenommen werden Die Firewall-Systeme gewährleisten, dass lediglich vordefinierten Kommunikationswege möglich sind und die erwünschte Kommunikationsrichtung des Verbindungsaufbaus beachtet wird. Die ALGs können speziell gehärtet werden und die für die Zone erforderlichen Sicherheitsanforderungen durchsetzen, ohne dass Anpassungen an den OT-Komponenten notwendig sind. Eine solche DMZ-Infrastruktur kann je nach Umgebungsanforderungen pro Schnittstelle oder für mehrere Schnittstellen genutzt werden.

IND.1.M17 Regelmäßige Sicherheitsüberprüfung (I)

Revision

OT-Infrastrukturen werden oftmals noch seltener auditiert als Systeme der Office-IT. Neben mangelndem Sicherheitsbewusstsein ist dies häufig den hohen Verfügbarkeitsanforderungen solcher Umgebungen geschuldet.

Vor diesem Hintergrund sollte ein geeigneter Überprüfungsprozess für die Umgebung entwickelt werden, der unter Berücksichtigung der Gegebenheiten geeignete Überprüfungsverfahren auf Basis manuell oder automatisiert durchgeführter Richtlinienkonformitätsprüfungen (Konfigurations- und Richtlinienprüfungen) umfasst. Besonderes Augenmerk sollte hierbei auf exponierte Systeme mit Außenschnittstellen sowie auf Systeme mit direktem Benutzerzugriff gelegt werden, da diese einer erhöhten Bedrohungslage ausgesetzt sind.

Bei der Planung sollte zudem berücksichtigt werden, dass sich bestimmte Schwachstellen prinzipbedingt nur durch praktische Schwachstellenprüfungen (Vulnerability Assessment, häufig auch als Penetrationstest bezeichnet) wirtschaftlich aufdecken lassen. Durch eine solche Maßnahme kann grundsätzlich die Verfügbarkeit der Umgebung zeitweise vermindert werden.

Audits sollten stets in Abstimmung mit den zuständigen Administratoren während der Betriebszeiten durchgeführt werden.

Für die Tests werden umfangreiche Fähigkeiten und Erfahrungen benötigt, welche bei Bedarf von extern bezogen werden können. In größeren Institutionen lohnt eventuell auch der Aufbau eigener Kompetenz. Je nach Schutzbedarf empfiehlt sich ein Audit pro System und Jahr bis hinunter zu einem Audit vor Produktivsetzung sowie bei größeren Änderungen in der Umgebung. Dies kann umfassen, bleibt aber nicht beschränkt auf:

- Erweiterungen der Anlagen (Hard- und Software)

- Einrichtung neuer Außenanbindungen

- Ersatzinstallationen

- Substanzielle Upgrade-Vorgänge und System- bzw. Software-Migrationen

3 Weiterführende Informationen

3.1 Wissenswertes

Für verschiedene Branchen existieren unterschiedliche nationale und internationale Spezialstandards und -vorgaben, welche ergänzend zu diesem Baustein herangezogen werden können, um die Maßnahmen weiter zu schärfen und zu ergänzen. Einige sind in der Literaturliste genannt; für weitere Verweise siehe das ICS-Security-Kompendium.

Begriffsbestimmungen

Für eine ausführliche Beschreibung typischer OT-Infrastrukturen wird auf Kapitel 2.3 *Hierarchische Gliederung von ICS* und Kapitel 2.5 *Kommunikationsvorgänge* des ICS-Security-Kompendiums verwiesen. Dort werden insbesondere auch die Level (Zonen) 1-5 (vgl. IND.1.M5 Entwicklung eines geeignete Zonenkonzepts) genauer dargestellt.

- OT (Operational Technologie): Betriebstechnik (englisch: Operational Technology (OT)) ist Hard- und Software, die Änderung durch die direkte Überwachung und / oder Steuerung von physikalischen Geräten, Prozessen und Ereignissen im Unternehmen erfasst und bewirkt [GART1].
- ICS (Industrial Control System): ICS ist ein Oberbegriff für Automatisierungslösungen zur Steuerung technischer Prozesse im industriellen Umfeld und ein Teil der OT.

- PLC (Programmable Logic Controller), SPS (Speicherprogrammierbare Steuerung), PNK (Prozessnahe Komponente); MTU (Main Terminal Unit), Controller: Diese Begriffe bezeichnen (abhängig von der sie einsetzenden Branche) eine Automatisierungskomponente mit Verarbeitungsfunktion. Diese werden zur Steuerung oder Regelung in einer Maschine oder Anlage eingesetzt und auf digitaler Basis programmiert wird.

- Sensor Messwertaufnehmer, Endschalter, Taster/Schalter, Initiator, Grenztaster: Dies sind Komponenten zur Erfassung physikalischer Größen und deren Wandlung in ein Einheitssignal. Als Interfaces kommen dabei analoge Standardschnittstellen wie 4...20 mA Stromschnittstelle, 0-10V, 24V-Gleichspannung usw. aber auch digitale Kommunikationsprotokolle wie Feldbusse (z. B. PROFIBUS PA) oder digitale Punkt-zu-Punkt-Verbindungen (z. B. IO-Link) zum Einsatz

- Aktuator, Aktor: Ein Aktor wandelt eine Steuergröße (z. B. elektrisches, hydraulisches oder pneumatisches Signal) in die Stellgröße zum Beeinflussen des Prozessgeschehens um. Bezüglich der Anbindung kommen die gleichen Techniken zum Einsatz, wie bei Sensoren.

- HMI (Human Machine Interface); BUB (Bedien- und Beobachtungskomponenten), ABK (Anzeige- und Bedienkomponente): Diese Komponenten dienen der Verwirklichung von Anzeige- und Bedienfunktionen. Typische Anwendungen sind z. B. die Darstellung und Bedienung des Prozesses über Prozessfließbilder, Standard-Bedienbilder (Faceplates), Trendbilder, Ablaufsprachenbilder, Gruppenbilder. Darüber hinaus stehen Funktionen für die Alarmverwaltung, die Datenarchivierung und Auswertung sowie die Systemdiagnose und Dokumentation.

- Programmier- und Testgerät, Service Rechner, Engineering Workstation: Diese Komponenten ermöglichen die Konfiguration und Inbetriebnahme von Automatisierungskomponenten.
- DCS (Digital Control System), PLS (Prozessleitsystem): DCS werden meist für größere verfahrenstechnische Anlagen eingesetzt. Sie können eine Vielzahl von Merkmalen, wie Alarmsysteme, Anlagenvisualisierung (Kurvenaufzeichnung von Messwerten), Benutzerverwaltung, zentrale Datenhaltung sowie Wartungs- und Entwicklungs- werkzeuge aufweisen.
- IS-Management (Informationssicherheitsmanagement): Die Planungs-, Lenkungs- und Kontrollaufgabe, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen, wird als Informationssicherheitsmanagement bezeichnet. Dabei handelt es sich um einen kontinuierlichen Prozess, dessen Strategien und Konzepte ständig auf ihre Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf fortzuschreiben sind. Das Ziel des IS-Management sind nicht nur der Schutz der Informationen, sondern auch der Systeme selbst. Cyber-Sicherheit ist im Sinne des Dokuments synonym zu verstehen.

Grundcharakteristika der OT

Die OT umfasst alle Technik, die für Produktionsprozesse und der Interaktion mit der physischen Welt umfassen. Ein Teil sind ICS. Diese werden überall dort eingesetzt, wo technische Prozesse automatisiert werden. Sie werden für das Messen, Steuern, Regeln und Bedienen von industriellen Abläufen benutzt. Beispiele hierfür sind die Verfahrens- und Prozesstechnik, die Fertigungsautomatisierung, die Ver- und Entsorgungsnetze (z. B. Strom, Wasser, Abwasser, Gas, Fernwärme), die Betriebstechnik (z. B. Schienen- und Straßenverkehr) und die Gebäudeautomation. Zur OT gehören auch Labor- und Analysegeräte.

Die individuellen Anforderungen werden unmittelbar durch die betrieblichen Anforderungen der Produktionsprozesse bestimmt.

Garantierte Antwortzeiten

Regelkreise gewährleisten im Hinblick auf ihr Zeitverhalten definierte Reaktionszeiten. Kommt es aufgrund von (temporären) Modifikationen im Bereich der Software zu Änderungen am Zeitverhalten der OT, kann dies zu Störungen im Produktionsprozess führen und etwa eine erhöhte Ausschussquote zur Folge haben.

Gesetzliche Auflagen/Beschränkungen

Es gibt viele Anwendungen, in welchen der Betrieb der Anlagen an behördliche Auflagen gebunden ist (z. B. CE-Zertifizierung von Geräten, Safety-Richtlinien, Richtlinien bei der Produktion von pharmazeutischen Produkten). In diesen Fällen bedürfen wesentliche Änderungen, worunter auch Softwareänderungen an den eingesetzten OT-Komponenten fallen können, eines dedizierten Genehmigungsprozesses. Aufgrund des vorgeschriebenen Prüfprozesses sind hier beispielsweise die Möglichkeiten zum zeitnahen Einspielen von Sicherheitsupdates begrenzt bzw. nicht gegeben.

Software

Bei OT-Komponenten ist zwischen Firmware, Anwendungssoftware und Parametrierung zu unterscheiden.

Die Firmware wird von den Herstellern nur bei auftretenden Fehlfunktionen aktualisiert; Änderungen bei den Anwenderprogrammen erfolgen nur, wenn die Anlagen geändert oder erweitert werden; Parametrierungen erfolgen im normalen Betrieb.

Änderungen und Updates

Das Ändern von Systemkonfigurationen oder das Einspielen von Updates bereiten, im Gegensatz zur Office-IT, häufig größere Probleme. Vor der Maßnahme sind mögliche Auswirkungen auf das Zeitverhalten oder andere Auswirkungen auf die Systeme zu prüfen. Bei der Durchführung kann es zu Einschränkungen der Verfügbarkeit (z. B. durch einen notwendigen Neustart) kommen. Nach Abschluss der Maßnahme ist eine Abnahme (etwa bzgl. Safety-Aspekten) zu erneuern. Dies führt dazu, dass Änderungen und Updates in der Regel nur im Rahmen von geplanten Anlagenstillständen eingebracht werden.

Hardware

Im Gegensatz zur Office-IT wird in der OT über längere Zeiträume mit gleicher Hardware (Gerätetypen) betrieben. Dies führt dazu, dass möglicherweise aktuelle Software, Firmware oder Protokolle nicht unterstützt werden.

Normen

Im Bereich der OT gibt es eine Vielzahl von Normen, Standards und Guidelines, welche stringente Anforderungen beinhalten (z. B. IEC 61508-3 im Bereich der Softwareentwicklung). Weitere Quellen führt das ICS-Security-Kompendium in Kapitel 4 Organisationen, Verbände und deren Standards auf.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Betriebs- und Steuerungstechnik" finden sich unter anderem in folgenden Veröffentlichungen:

[27019] ISO/IEC 27019:2017

Information technology - Security techniques - Information security controls for the energy utility industry, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/SC, Oktober 2017

[AHWAST] Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme

Bundesverband der Energie- und Wasserwirtschaft e.V. (BDEW) und Oesterreichs E-Wirtschaft, Version 2, Mai 2018, https://www.bdew.de/media/documents/Awh_20180507_OE-BDEW-Whitepaper-Secure-Systems.pdf, zuletzt abgerufen am 05.10.2018

[CSE] Empfehlungen für Fortbildungs-und Qualifizierungsmaßnahmen im ICS-Umfeld

BSI-Veröffentlichungen zur Cyber-Sicherheit (BSI-CS 123), November 2015, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_123.pdf, zuletzt abgerufen am 05.10.2018

[GART1] Gartner IT Glossary

Operational Technology (OT), http://www.gartner.com/it-glossary/operational-technology-ot/, zuletzt abgerufen am 05.10.2018

[ICSSK] ICS-Security-Kompendium

Testempfehlungen und Anforderungen für Hersteller von Komponenten, Bundesamt für Sicherheit in der Informationstechnik (BSI), November 2014 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security-Kompendium-Hersteller.html, zuletzt abgerufen am 05.10.2018

[ICSSKfH] ICS-Security-Kompendium

Testempfehlungen und Anforderungen für Hersteller von Komponenten, Bundesamt für Sicherheit in der Informationstechnik (BSI), November 2014
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security-Kompendium-Hersteller.html, zuletzt abgerufen am 05.10.2018

[IEC62443-2.1] IEC 62443-2-1:2010 Industrial communication networks - Network and system security

Part 2-1: Establishing an industrial automation and control system security program, International Electrotechnical Commission (IEC), 2010, https://webstore.iec.ch/publication/7030, zuletzt abergerufen am 05.10.2018

[NIST80082] Guide to Industrial Control Systems (ICS) Security

NIST Special Publication 800-81, Revision 2, September 2013,
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf,
zuletzt abgerufen am 05.10.2018

[VDI2182.1] Richtlinie VDI/VDE 2182

Blatt 1, Informationssicherheit in der industriellen Automatisierung - Allgemeines Vorgehensmodell, Januar 2011

[VDI2182.2.1] Richtlinie VDI/VDE 2182

Blatt 2.1, Informationssicherheit in der industriellen Automatisierung - Anwendungsbeispiel des Vorgehensmodells in der Fabrikautomation für Hersteller - Speicherprogrammierbare Steuerung (SPS), Februar 2013

[VDI2182.3.1] Richtlinie VDI/VDE 2182

Blatt 3.1, Informationssicherheit in der industriellen Automatisierung - Anwenderbeispiel des Vorgehensmodells in der Prozessautomation für Hersteller - Prozessleitsystem einer LDPE-Anlage, September 2013

[WAST] Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme

Bundesverband der Energie- und Wasserwirtschaft e.V (BDEW), Version 2.0, Mai 2018,
https://www.bdew.de/
service/anwendungshilfen/whitepaper-anforderungen-sichere-steuerungs-telekommunikationssysteme/, zuletzt abgerufen am 05.10.2018

Bundesamt
für Sicherheit in der
Informationstechnik

Umsetzungshinweise für die Bausteinschicht NET

IT-Grundschutz

Umsetzungshinweise zum Baustein NET.2.1 WLAN-Betrieb

1 Beschreibung

1.1 Einleitung

WLANs können entsprechend den Bedürfnissen eines Betreibers und der Hardware-Ausstattung, die zur Verfügung steht, in zwei verschiedenen Modi betrieben werden. Im Ad-hoc-Modus kommunizieren zwei oder mehr mobile Endgeräte, die mit einer WLAN-Karte ausgestattet sind, direkt miteinander. Da sich WLANs im Ad-hoc-Modus selbstständig, ohne feste Infrastruktur aufbauen und konfigurieren können und somit eine vollvermaschte parallele Netz-Infrastruktur etablieren können, wird davon abgeraten, WLANs im Ad-hoc-Modus in einer zu schützenden Umgebung zu betreiben. Dieser wird im Folgenden nicht weiter betrachtet. In den vorliegenden Umsetzungshinweisen wird davon ausgegangen, dass alle Access Points (Zugangspunkte) zentral administriert und nicht im Ad-hoc-Modus betrieben werden.

Für die Umsetzungshinweise wird auf die folgenden drei fiktiven Szenarien zurückgegriffen.

1. Szenario

- Die Informationen sind nicht als vertraulich klassifiziert.
- Access Points dürfen über eine Cloud-Infrastruktur administriert werden.
- Die Benutzer nutzen die zur Verfügung gestellte WLAN-Infrastruktur für die Telefonie.

2. Szenario

- Die Informationen sind teilweise als vertraulich klassifiziert.
- Access Points dürfen nicht über eine Cloud-Infrastruktur administriert werden.
- Die Benutzer nutzen die zur Verfügung gestellte WLAN-Infrastruktur für die Telefonie.
- Die Benutzer können über die WLAN-Infrastruktur außerdem auf interne Kollaborations- und Dokumentenmanagementsysteme zugreifen.

3. Szenario

- Die Informationen sind teilweise als streng vertraulich klassifiziert.
- Access Points dürfen nicht über eine Cloud-Infrastruktur administriert werden.
- Die Benutzer nutzen die zur Verfügung gestellte WLAN-Infrastruktur für die Telefonie.
- Die Benutzer können über die WLAN-Infrastruktur außerdem auf interne Kollaborations- und Dokumentenmanagementsysteme, Finanzdaten oder kritische Systeme der Institution zugreifen.

1.2 Lebenszyklus

Planung und Konzeption

Alle gewünschten Nutzungsszenarien und Funktionen sowie die damit einhergehenden regulatorischen Anforderungen sollten in der Planungs- und Konzeptionsphase in das Design der zukünftigen WLAN-Infrastruktur einfließen. Grundlage hierfür ist eine durchdachte WLAN-Strategie (siehe NET.2.1.M1 *Festlegung einer Strategie für den Einsatz von WLANs*). Die bestehenden Prozesse sollten darauf hin analysiert werden, ob sie mögliche Schnittstellen zu den Prozessen der zukünftigen WLAN-Infrastruktur aufweisen und bei Bedarf sollten sie aktualisiert werden. Zudem sollte geprüft werden, ob die Funktionen, die die WLAN-Infrastruktur mit sich bringt mit den geschäftlichen, sicherheitstechnischen und datenschutzrechtlichen Regelungen vereinbar sind.

Neben der Strategie sind die Auswahl des richtigen WLAN-Standards und den damit verbundenen Kryptoverfahren (siehe NET.2.1.M2 *Auswahl eines geeigneten WLAN-Standards* und NET.2.1.M3 *Auswahl geeigneter Kryptoverfahren für WLAN*) wichtige Themen, die bereits in der Planungsphase adressiert werden müssen.

Alle getroffenen Entscheidungen über Sicherheitseinstellungen, ausgewählte WLAN-Standards, sowie die Regelungen für die Administration des WLANs, sollten in einer WLAN-Sicherheitsrichtlinie niederzuschreiben (siehe NET.2.1.M10 *Erstellung einer Sicherheitsrichtlinie für den Betrieb von WLANs*). Wissenswertes zu WLANs ist unter "Wissenswertes" im Kapitel 3.1.1 *Einführung in WLAN-Grundbegriffe* zu finden.

Beschaffung

Bei der Auswahl der WLAN-Komponenten ist die Maßnahme NET.2.1.M11 *Geeignete Auswahl von WLAN-Komponenten* anzuwenden. Da sich Standards, Protokolle und integrierte Sicherheitsmechanismen stetig fortentwickeln, unterliegen WLANs einem schnellen Wandel. Dies bedeutet, dass die WLAN-Infrastruktur an sich oder einzelne Komponenten häufiger migriert werden müssen. Für Migrationsphasen einzelner WLAN-Komponenten oder gar ganzer WLAN-Bereiche müssen notwendige WLAN-Migrationsschritte sorgfältig geplant und idealerweise in einem Proof of Concept (Machbarkeitsnachweis) vor der eigentlichen Migration verifiziert werden.

Umsetzung

Um die maximal möglichen Übertragungsraten zu erreichen, ist es nicht unerheblich, an welcher Stelle die Access Points im Raum positioniert sind (siehe NET.2.1.M4 *Geeignete Aufstellung von Access Points*). Die WLAN-Komponenten oder die WLAN-Managementlösung müssen bei der Installation stets gemäß den internen Sicherheitsrichtlinien konfiguriert werden (siehe NET.2.1.M5 *Sichere Basis-Konfiguration der Access Points* und NET.2.1.M6 *Sichere Konfiguration der WLAN-Clients*). Werden WLANs mit der eventuell bereits vorhandenen kabelgebundenen Infrastruktur verbunden, muss der Übergang zwischen WLANs und LAN entsprechend des höheren Schutzbedarfs abgesichert werden (siehe NET.2.1.M7 *Aufbau eines Distribution Systems* und NET.2.1.M9 *Sichere Anbindung von WLANs an ein LAN*).

Um Fehlkonfigurationen oder Fehlbedienungen zu vermeiden und auf mögliche Gefahren hinzuweisen, die entstehen können, wenn WLANs unsachgemäß betrieben werden, sind Verantwortliche ausreichend zu schulen und zu sensibilisieren. Weitere Informationen hierzu sind im Baustein ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit* zu finden.

Betrieb

Ist das WLAN in Betrieb genommen und wurden alle WLAN-Verantwortlichen ausreichend geschult, so ist durch regelmäßige Audits (siehe NET.2.1.M14 *Regelmäßige Audits der WLAN-Komponenten*) sicherzustellen, dass alle getroffenen Sicherheitseinstellungen stets aktuell sind und diese Einstellungen auch greifen. Unumgänglich ist ein Schlüsselmanagement für die eingesetzten kryptographischen Schlüssel, um die Kommunikation in WLANs abzusichern (siehe CON.1 *Kryptokonzept*). Wird eine WLAN-Managementlösung (siehe NET.2.1.M12 *Einsatz einer geeigneten WLAN-Management-Lösung*) eingesetzt, können die Schlüssel, Einstellungen sowie die WLAN-Komponenten selbst zentral von einer Stelle aus verwaltet werden.

Aussonderung

Werden WLAN-Komponenten außer Betrieb genommen, sind Konfigurationseinstellungen zu entfernen und wieder auf Standardwerte zurückzusetzen. Weitere Informationen hierzu sind im Baustein CON.6 *Löschen und Vernichten* zu finden.

Notfallvorsorge

Wurden Angriffe auf WLANs erkannt, so müssen die Verantwortlichen der WLANs wissen, wie sie sich zu verhalten haben (siehe NET.2.1.M8 *Verhaltensregeln bei WLAN-Sicherheitsvorfällen*). Hieraus ergibt sich ein Notfallplan, welche Schritte notwendig und welche Personen zu informieren sind, wenn ein Sicherheitsvorfall eintritt.

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "WLAN-Betrieb" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

NET.2.1.M1 Festlegung einer Strategie für den Einsatz von WLANs [Leiter IT]

Wenn die folgenden Fragen beantwortet werden, kann hieraus die WLAN-Strategie in ihren Grundzügen hergeleitet werden.

- In welchen Bereichen (organisatorisch sowie räumlich) soll eine WLAN-Infrastruktur genutzt werden?
- Welche Potenziale erschließt die Nutzung einer WLAN-Infrastruktur?
  - Welche Aspekte der Mobilität werden durch WLANs ermöglicht?
  - Welche Funktionen bzw. Anwendungen sollen durch die WLAN-Nutzung bereitgestellt bzw. unterstützt werden (z. B. Voice over WLAN, Media Broadcasting, Kollaboration, Videokonferenzen, Gastzugang/Hotspot, Einbindung von mobilen Endgeräten, Client-Netz-Segmentierung)?
  - Welche Geschäftsprozesse lassen sich durch die Nutzung von WLANs optimieren?
- Welches Sicherheitsrisiko entsteht dadurch, dass eine WLAN-Infrastruktur genutzt wird bzw. welches Risiko stellt der Verlust von Daten/Informationen über WLANs dar?
- Welche gesetzlichen Regelungen müssen eingehalten werden?
- Welche klassifizierten Daten/Informationen dürfen nicht ohne zusätzliche kryptographische Schutzmechanismen übertragen werden?
- Wer ist für den Betrieb der WLAN-Infrastruktur verantwortlich?
  - Wird die WLAN-Infrastruktur extern administriert?
  - Darf die WLAN-Infrastruktur cloudbasiert administriert werden?
- Welche Anforderungen werden an die Verfügbarkeit der WLAN-Infrastruktur gestellt?

NET.2.1.M2 Auswahl eines geeigneten WLAN-Standards [Planer]

Im Rahmen des WLAN-Designs, das den dokumentierten strategischen Anforderungen folgt, müssen potenziell störende Systeme in der Nähe des späteren Aufstellungsorts von Access Points ermittelt und evaluiert werden. Werden Mikrowellen in der Nähe von Access Points oder anderen IT-Systemen betrieben, können Störungen auftreten. Mögliche weitere Störquellen können Bluetooth-Sender, Hochspannungsleitungen, schnurlose Telefone (DECT) oder LCD-Monitore sowie das Baumaterial selbst sein.

Wenn die Anforderungen an die Beschaffung von Hard- und Software zusammengestellt werden, muss darauf geachtet werden, dass die Authentisierung nach dem Standard IEEE 802.11i-2004 oder neuer realisiert wird.

Um Brute-Force-Angriffe auf WLAN-Passwörter zu vermeiden, sollte die WLAN-Infrastruktur den Standard IEEE 802.11s unterstützen. Dieser Standard definiert mittels Simultaneous Authentication of Equals (SAE), dass das eigentliche Passwort nicht mehr über den Funkkanal übertragen wird. Hierdurch kann den bisher üblichen Angriffen durch Mitschneiden eines Verbindungsaufbaus mit anschließendem Brute-Force-Angriff auf das WLAN-Passwort effektiv begegnet werden. Der Standard IEEE 802.11ac definiert, wie Management-Frames mittels Protected Management Frames (PMF) gegen gefälschte Deassoziierungspakete eines Angreifers abzusichern sind. Um PMF effektiv nutzen zu können, muss jedoch auch das Endgerät den Standard IEEE 802.11ac unterstützen.

In Tabelle 1 sind diverse Authentisierungsmöglichkeiten für die drei fiktiven Szenarien abgebildet.

Authentisierungsoption	Szenario 1	Szenario 2	Szenario 3
Offen (keine Authentisierung)	nein	nein	nein
Wired Equivalent Privacy (WEP)	nein	nein	nein
Message Authentication Code (MAC)	nein	nein	nein
Pre-Shared Key	ja	nein	nein
Standard IEEE 802.1X / Extensible Authentication Protocol (EAP)	ja	ja	ja
Captive Portal (empfohlene Methode für Gast-Netze)	ja	ja	ja

Tabelle : WLAN-Authentisierungsmethoden

Tabelle 2 gibt einen Überblick über die unterstützten IEEE-802.1X-EAP-Lösungen auf Basis der aufgeführten Endgeräte bzw. deren Betriebssysteme. Sie listet nicht alle Varianten auf und zeigt nicht die Wertigkeit der einzelnen Systeme. Es sollte EAP-TLS oder EAP-AKA anstelle von EAP-PEAP, EAP-TTLS oder EAP-SIM verwendet werden. Da EAP-PEAP und EAP-TTLS derzeit jedoch noch häufig eingesetzt werden, werden sie in der Tabelle dennoch aufgeführt.

Betriebssystem	Authentisierungs-option	Authentisierungs-option	Authentisierungs-option
	EAP-PEAP	EAP-TTLS	EAP-TLS
Windows 10	ja	ja	ja
Windows 8.1	ja	ja	ja
Windows 7	ja	ja	ja (nach Update, siehe Kapitel Fehler: Referenz nicht gefunden)
Mac OS X	ja	ja	ja
Linux	ja	ja	ja
iOS	ja	ja	ja
Android	ja	ja	ja
BlackBerry 10	ja	ja	ja
Windows Phone 10	ja	ja	ja
Windows Phone 8.1	ja	Ja	ja

Tabelle : WLAN-EAP-Authentisierungsvarianten je nach Art des Betriebssystems

Wenn EAP-TTLS verwendet wird, müssen kryptographisch abgesicherte Authentisierungsverfahren eingesetzt werden. Für die IEEE-802.1X-basierte Authentisierung von Smartphones und Tablets an der WLAN-Infrastruktur bietet sich zusätzlich EAP-SIM/EAP-AKA an.

NET.2.1.M3 Auswahl geeigneter Kryptoverfahren für WLAN [Planer]

Um WLANs sicher zu betreiben, muss die Kommunikation hierüber kryptographisch über Wi-Fi Protected Access 2 (WPA2) abgesichert sein. Leicht zu kompromittierende kryptographische Verfahren dürfen nicht mehr eingesetzt werden. Falls WEP oder WPA noch benutzt werden, sollte durch eine hierfür geplante Migration auf WPA2 aktualisiert werden.

Wird WPA2 mit Pre-Shared Keys (WPA2-PSK) verwendet, muss ein komplexer Schlüssel mit einer Mindestlänge von 20 Zeichen konfiguriert sein. Da der Schlüssel regelmäßig ausgetauscht werden muss, ist diese Methode nur für kleine WLAN-Installationen wirtschaftlich tragbar. Zudem muss bei WPA2-PSK darauf geachtet werden, dass die deutschen Umlaute und spezielle Steuerzeichen nicht eingesetzt werden können.

NET.2.1.M4 Geeignete Aufstellung von Access Points [Haustechnik]

Um Manipulationen an den Access Points vorzubeugen, müssen diese in stabilen Gehäusen untergebracht sein, die im Inneren eines Gebäudes an der Wand montiert werden können. Zusätzlich kann ein Access Point gegen zu einfachen Diebstahl z. B. durch ein Kensington Lock am Gehäuse selbst abgesichert werden. Aus WLAN-versorgungstechnischen Gründen sollten Access Points nicht in Zwischendecken oder abgehängten Decken untergebracht werden, wenn keine externen Antennen genutzt werden. Dies gilt auch für die Anbringung von Metallkäfigen zum Schutz von Access Points, da auch sie die Übertragungsqualität und den Durchsatz eines WLANs essentiell beeinflussen, insbesondere wenn Beamforming-Technik entsprechend dem Standard IEEE 802.11ac eingesetzt wird.

Die optimalen Aufstellungsorte der Access Points sollten durch eine Ausleuchtungsmessung ermittelt werden.

Werden Außenbereiche versorgt, müssen Außeninstallationen (Antennen und gegebenenfalls Access Points) vor Witterungseinflüssen, elektrischen Entladungen und unberechtigtem Zugriff geeignet geschützt werden. Außerhalb von Gebäuden sollten Access Points möglichst nicht angebracht werden.

NET.2.1.M5 Sichere Basis-Konfiguration der Access Points

Voreingestellte SSIDs, Zugangskennwörter oder kryptographische Schlüssel müssen direkt nach Inbetriebnahme geändert werden, um den späteren sicheren Betrieb nicht zu gefährden. Die Access Points dürfen nicht im Auslieferungszustand produktiv in Betrieb genommen werden. Beispielsweise sollte der Name des Service Set Identifiers (SSID) keine Rückschlüsse auf die Hardware, die Institution, eventuelle Dienstleister und den Einsatzzweck ermöglichen.

Durch die Verantwortlichen muss regelmäßig überprüft werden, ob alle sicherheitsrelevanten Updates und Patches für die etablierte WLAN-Infrastruktur eingespielt sind. Damit Empfänger und Sender optimal und sicher zusammenspielen, ist dies auch für die zugehörigen WLAN-Gerätetreiber auf den WLAN-Clients zu berücksichtigen. Eine neue Software-Version oder ein Patch sollten erst nach einem angemessenen Test eingespielt werden. Die spezifizierten Melde- und Informationsprozeduren im Änderungsmanagement sollen beschreiben, wer und wie bei derartigen Änderungen zu informieren ist. Ebenso ist die Dokumentation der WLAN-Infrastruktur anzupassen.

Im Folgenden wird aufgezeigt, mit welchen Einstellungsempfehlungen die WLAN-Infrastruktur weiter abgesichert werden kann.

Schließen aller nicht benötigten offenen Ports

Port-Nummer	Beschreibung	Hinweise
21/TCP	Wird meist genutzt, um ein Image des Access Points vom WLAN-Controller herunterzuladen	Müssen erhöhte Sicherheitsanforderungen erfüllt werden (Szenario 3), sollten Images kryptographisch abgesichert heruntergeladen werden.
23/TCP	Teletype Network (Telnet)	Der Zugang via Telnet darf nicht ermöglicht werden.
67/UDP	DHCP-Server-Funktionen	Ist kein DHCP-Service verfügbar, müssen die DHCP-Server-Funktionen deaktiviert werden.
80/TCP	Hypertext Transfer Protocol (HTTP)	Ist kein HTTP-Service verfügbar, muss dieser Dienst deaktiviert werden.
123/UDP	Network Time Protocol (NTP) – Zeitdienst für die Access Points	Müssen erhöhte Sicherheitsanforderungen (Szenario 3) erfüllt werden, sollte die Zeitsynchronisation kryptographisch abgesichert erfolgen.
161/UDP	SNMP-Management-Zugang	Der Zugang mittels SNMP sollte auf Basis der Version 3 realisiert sein.
514/UDP	Syslog für den Empfang von Meldungen von den Access Points	Müssen erhöhte Sicherheitsanforderungen (Szenario 3) erfüllt werden, sollten Meldungen der Access Points nur kryptographisch abgesichert empfangen werden können.

Tabelle 3: Schließen aller nicht benötigten offenen Ports

Sperren nicht benötigter Services

Für alle drei fiktiven Szenarien wird empfohlen, die Verschlüsselungsmethode WPA2-AES-CCM (128 Bit) anstelle von WPA2-TKIP zu nutzen.

Das Dokument Technische Richtlinie TR-02102 (siehe [TR02102]) des BSI enthält Empfehlungen für die Verwendung von SSL/TLS. Diese Empfehlungen sollten die Basis für die spätere Aktivierung der genutzten Cipher-Suiten sein. Mit welcher TLS-Version für welches der drei fiktiven Szenarien die Informationen ausreichend abgesichert werden können, zeigt die folgende Tabelle.

	Szenario 1	Szenario 2	Szenario 3
TLS v1.0	ja	nein	nein
TLS v1.1	ja	ja	nein
TLS v1.2	ja	ja	ja

Tabelle 4: Empfohlene TLS-Versionen je Szenario

Sperren nicht benötigter Management-Zugänge

Um potentielle Angriffsvektoren zu reduzieren, sollte die Administration der WLAN-Komponenten z. B. via Secure Shell (SSH), HyperText Transfer Protocol Secure (HTTPS) oder SNMP aus einem dedizierten Management-Netz heraus erfolgen. Die WLAN-Infrastruktur sollte nicht über einen per WLAN angebundenen Client administriert werden.

Um Innentäter-Angriffe vorzubeugen, sollte eine zentrale Authentisierung auf Basis von personalisierten Benutzerkonten etabliert werden. Die für das Benutzerkonto des Administrators hinterlegten Berechtigungen müssen nach dem Minimalprinzip erfolgen.

Im Rahmen der Notfallvorsorge ist es empfehlenswert, ein lokales Benutzerkonto (Notfallbenutzerkonto) zu hinterlegen. Das Passwort des Notfallbenutzerkontos muss der etablierten Passwortrichtlinie der Institution genügen. Nach jeder Verwendung des Notfallbenutzerkontos muss dessen Passwort geändert werden. Verwendung und Einsatzgrund müssen anschließend nachvollziehbar dokumentiert werden.

Erkennen und Sperren unberechtigter Benutzer-Zugänge

ARP-Spoofing-Angriffe sollten erkannt und abgewehrt werden, wenn IP-Adressen via DHCP-Server vergeben werden. Hierfür können DHCP Snooping und Dynamic ARP Inspection (DAI) eingesetzt werden.

NET.2.1.M6 Sichere Konfiguration der WLAN-Clients

Für einen sicheren WLAN-Betrieb ist es wichtig, dass auch alle mit den WLANs gekoppelten Clients sicher konfiguriert sind. Geeignete Anforderungen für eine sichere Konfiguration von Clients sind im Baustein SYS 2.1 *Allgemeiner Client* und NET.2.2 *WLAN-Nutzung* definiert. Zusätzlich muss die WLAN-Schnittstelle deaktiviert werden, wenn sie über einen längeren Zeitraum nicht genutzt wird. Durch den Betrieb von WLANs dürfen etablierte Sicherheitsinfrastrukturen (und insbesondere Firewalls) nicht umgangen werden können.

Sollen WLAN-Clients (z. B. Smartphones) selbst Hotspot-ähnliche Funktionen zur Verfügung stellen, müssen die Benutzer sicherstellen, dass voreingestellte SSIDs, kryptographische Schlüssel und Passwörter durch sie geändert wurden, bevor die Hotspot-Funktionen aktiviert werden. Das Passwort (WPA2-Schlüssel) sollte so gewählt sein, dass es nur schwer erraten werden kann.

NET.2.1.M7 Aufbau eines Distribution Systems [Planer]

Ein Distribution System verbindet die Access Points untereinander und bindet die weitere Infrastruktur ein. Es gibt zwei Arten von Distribution Systemen:

- kabelgebundene Distribution Systeme (alle Access Points werden untereinander und mit der weiteren Infrastruktur verkabelt)
- Wireless Distribution Systeme (eine direkte Verkabelung zwischen den Access Points ist nicht notwendig)

Sind hohe Verfügbarkeitsanforderungen zu erfüllen, sollte kein Wireless Distribution System eingerichtet werden. In einem Wireless Distribution System müssen Repeater sowohl mit den WLAN-Clients als auch mit dem Access Point kommunizieren. Hierdurch reduziert sich die Übertragungsrate um die Hälfte. Diese drastische Reduzierung der Übertragungsrate lässt sich nur umgehen, indem Clients und Repeater auf einer anderen Frequenz miteinander kommunizieren als Repeater und Access Point/WLAN-Router. Theoretisch lässt sich ein Wireless Distribution System mit bis zu 254 Repeatern in einem Netz betreiben, wenn die Repeater nicht in Reihe, sondern im Stern angebunden sind, um Signalüberschneidungen zu vermeiden.

Bevor ein kabelgebundenes Distribution System aufgebaut wird, sollte entschieden werden, ob eine eigenständige physische Switch-Infrastruktur für die WLANs aufgebaut werden soll, eine virtualisierte Switch-Infrastruktur oder ob alternativ eine logische Segmentierung durch Virtual Local Area Networks (VLANs) ausreichend ist. Hierbei sind insbesondere Sicherheitsaspekte zu beachten.

NET.2.1.M8 Verhaltensregeln bei WLAN-Sicherheitsvorfällen

Falls sich das WLAN in nicht vorgesehener Weise verhält (z. B. WLAN ist längere Zeit nicht verfügbar, Zugriff auf Netzressourcen ist nicht möglich, Netzperformance bricht dauerhaft ein), kann dies durch einen Sicherheitsvorfall verursacht worden sein. Dieser kann durch einen Angreifer, Fehlkonfigurationen oder Systemfehler herbeigeführt worden sein.

Der IT-Betrieb sollte die folgenden Maßnahmen umsetzen:

- Die Benutzer müssen den IT-Betrieb über geeignete Eskalationsstufen erreichen können.
- Am Übergabepunkt der WLAN-Kommunikation ins interne LAN sollte bei einem Angriff auf das WLAN die Kommunikation selektiv pro SSID, Access Point oder sogar für die komplette WLAN-Infrastruktur gesperrt werden.
- Bei einem Sicherheitsvorfall oder einem Diebstahl sollte der IT-Betrieb passende Sicherheitsmaßnahmen einleiten können. Idealerweise greifen sie auf abgestimmte und dokumentierte Prozeduren zurück. Mögliche Aktionen sind z. B.:
  - Abschaltung von Access Points
  - Herunterfahren von Servern
  - Überprüfung der Konfigurationen der Access Points
  - Sicherung aller Dateien, die Aufschluss über die Art und Ursache des aufgetretenen Problems geben könnten (z. B. ob tatsächlich ein Angriff erfolgt ist und auf welche Weise der Angreifer eindringen konnte), d. h. insbesondere Sicherung aller relevanten Protokolldateien.
  - Gegebenenfalls Wiedereinspielen der Original-Konfigurationsdaten
  - Benachrichtigung der Benutzer mit der Bitte, ihre Arbeitsbereiche auf Unregelmäßigkeiten zu prüfen.

Falls Access Points gestohlen worden sind, müssen gezielte Sicherheitsmaßnahmen ergriffen werden, wie z. B.:

- Änderung aller eingesetzten kryptographischen Schlüssel, also z. B. der PSKs im Falle der Verwendung von WPA2-PSK
- Konfigurationsänderung auf RADIUS-Servern, um den entwendeten Access Point (IP, Name, RADIUS-Client, Shared Secret, IPSec) zu sperren.

Sind WLAN-Clients entwendet worden und wird eine zertifikatsbasierte Authentisierung verwendet, müssen auch die Client-Zertifikate gesperrt werden.

Die möglichen Konsequenzen sicherheitskritischer Ereignisse müssen untersucht werden. Letztlich sind alle erforderlichen Maßnahmen zu ergreifen, um eine missbräuchliche Verwendung von entwendeten Geräten zum Zugriff auf das Netz der Institution auszuschließen.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "WLAN-Betrieb".

NET.2.1.M9 Sichere Anbindung von WLANs an ein LAN [Planer]

Die WLAN-Komponenten müssen an den Übergängen zwischen WLANs und LAN abgesichert werden, beispielsweise durch einen Paketfilter. Um unnötigen Broadcast und Multicast Traffic zu vermeiden, sollte für jede vergebene SSID ein korrespondierendes VLAN etabliert sein. Weitere Anforderungen, die zu beachten sind, finden sich im Baustein NET.1.1 *Netz-Architektur und -design*.

Sollen WLANs sicher an ein LAN angebunden werden, kann zwischen einer Controller-basierten und einer Controller-losen Administration von Access Points unterschieden werden. Angemessene Absicherungsmaßnahmen für die jeweilige Variante werden nachfolgend aufgezeigt.

Controller-basierte Verwaltung der Access Points

Für eine Controller-basierte Verwaltung der WLAN-Infrastruktur werden in der folgenden Tabelle angemessene Absicherungsmaßnahmen für die Anbindung des Access Points an das LAN benannt.

Gewünschte Access-Point-Funktionen	Szenario 1	Szenario 2	Szenario 3
Zentrale Authentisierung der Benutzer	ja	ja	ja

Gewünschte Access-Point-Funktionen	Szenario 1	Szenario 2	Szenario 3
Zentrale Auskopplung der Nutzdaten (Central Switching) am WLAN-Controller	nein	nein	ja
Lokale Auskopplung der Nutzdaten (Local Switching) direkt an dem Switch, der die Anbindung zum Access Point realisiert	ja	ja	nein
Roaming-Funktionen	nein	ja	ja
Gast-/Hotspot-Zugänge	ja	ja	nein

Tabelle 5: Empfohlene Access-Point-Funktionen je Szenario

Ein pragmatischer Ansatz für eine lokale Auskopplung der Nutzdaten kann in Teilen für Szenario 3 gewählt werden, sofern der berechtigte Zugang zum WLAN mittels IEEE 802.1X und EAP-TLS überprüft wird und die Access Points und Endgeräte den Standard IEEE 802.11ac vollumfänglich unterstützen. Die Kommunikation zwischen den Access Points und den WLAN-Controllern muss auch kryptographisch abgesichert sein. Um mögliche Risiken des Verlusts der Vertraulichkeit und Integrität der über Funk übertragenen Informationen zu kompensieren, wird eine zusätzliche Overlay-Verschlüsselung empfohlen.

Bei den Szenarien 1 und 2 geht die Benutzerkommunikation direkt vom Access Point über den Switch in die internen Netze über. Ein pragmatischer Ansatz ist deshalb nicht möglich. Lediglich freigegebene und in die etablierten Prozesse aufgenommene Access Points der Institution dürfen an das Netz angebunden sein. Dies sollte mittels IEEE 802.1X sichergestellt werden.

Alle Access Points beziehen ihre Betriebssoftware direkt vom zugeordneten WLAN-Controller. Die Betriebssoftware eines Access Points wird über einen kryptographisch abgesicherten Kanal aktualisiert. Wird die Betriebssoftware auf Basis von Klartext-Protokollen ausgetauscht, sollte im Anschluss die Integrität der Software anhand von Signaturen verifiziert werden.

Die WLAN-typischen Kommunikationsenden für bereitgestellte Gastzugänge müssen in einer Demilitarized Zone (DMZ) enden. Zugriffe aus dem Gast-WLAN sind wie Zugriffe aus dem Internet zu behandeln. Sie dürfen nur über ein Sicherheitsgateway zugelassen werden.

Controller-lose Verwaltung der Access Points

Ein pragmatischer Ansatz ist bei einer Controller-losen Verwaltung der Access Points meist nicht möglich, da die Benutzerkommunikation direkt vom Access Point über den Switch in die internen Netze übergeht.

Um Roaming-Funktionen bereitzustellen, werden zwischen den einzelnen Access Points autarke Netze aufgespannt, meist im Default-VLAN. Ob die Anforderungen für den Betrieb der Access Points mit den Sicherheitsanforderungen vereinbar sind, kann mit den folgenden Fragen überprüft werden:

- Ist die Kommunikation der Access Points untereinander ausreichend kryptographisch abgesichert?
- Ist die Gruppe der Mitarbeiter mit Zugang zu Spiegelports an den Switches bekannt und begrenzt?
- Ist ein nicht genutzter Switch-Port aus dem Default-VLAN entbunden?
- Ist eine Hardware-Authentisierung am Switch-Port eingerichtet?
- Sind die Roaming-Funktionen durch Bridging- und Tunneling-Methoden realisiert?
- Endet die Gast-Zugangskommunikation über einen kryptographischen Tunnel in der DMZ?

Auch für Access Points, die ohne Controller administriert werden, gilt, dass lediglich freigegebene und in die etablierten Prozesse aufgenommene Access Points der Institution an das Netz angebunden sein dürfen. Mittels IEEE 802.1X sollte sichergestellt werden, dass diese Anforderung erfüllt ist. Der berechtigte Zugang von Endgeräten zum WLAN sollte ebenfalls mittels IEEE 802.1X und EAP-TLS überprüft werden.

Alle Access Points beziehen ihre Betriebssoftware direkt vom zugeordneten WLAN-Managementsystem (WNMS). Die Betriebssoftware eines Access Points sollte über einen kryptographisch abgesicherten Kanal aktualisiert werden. Wird die Betriebssoftware auf Basis von Klartext-Protokollen ausgetauscht, sollte im Anschluss die Integrität der Software anhand von Signaturen verifiziert werden.

Die eingesetzten Access Points und eingebundenen WLAN-Clients sollten den Standard IEEE 802.11ac vollumfänglich unterstützen. Die Access-Point-zu-Access-Point-Kommunikation muss auf Basis von Internet Protocol Security (IPsec) oder TLS in einem gekapselten Tunnel stattfinden.

NET.2.1.M10 Erstellung einer Sicherheitsrichtlinie für den Betrieb von WLANs

Für den Einsatz von WLAN-Komponenten in Institutionen sollte eine geeignete Sicherheitsrichtlinie erstellt werden. Diese WLAN-spezifische Sicherheitsrichtlinie sollte konform zum generellen Sicherheitskonzept und den allgemeinen Sicherheitsrichtlinien der Institution sein. Sie sollte regelmäßig auf Aktualität überprüft und gegebenenfalls angepasst werden.

Eine WLAN-Sicherheitsrichtlinie sollte unter anderem folgende Punkte umfassen:

- Es sollte beschrieben sein, wer in der Institution WLAN-Komponenten installieren, konfigurieren und benutzen darf.
- Für alle WLAN-Komponenten sollten Sicherheitsmaßnahmen und eine Standard-Konfiguration festgelegt werden.
- Bei einem Verdacht auf Sicherheitsprobleme muss ein Sicherheitsverantwortlicher hierüber informiert werden, damit dieser weitere Schritte unternehmen kann (siehe auch DER.2.1 Behandlung von Sicherheitsvorfällen).

Der IT-Betrieb sollte über die Gefährdungen, denen WLAN-Komponenten ausgesetzt sind und die zu beachtenden Sicherheitsmaßnahmen informiert bzw. geschult werden.

Die korrekte Umsetzung der in der WLAN-Sicherheitsrichtlinie beschriebenen Sicherheitsmaßnahmen sollte regelmäßig kontrolliert werden.

NET.2.1.M11 Geeignete Auswahl von WLAN-Komponenten

Wichtige Kriterien für die Auswahl von WLAN-Komponenten sind Sicherheit, Datenschutz und Kompatibilität. Kompatibilitätsprobleme können bei der Vielzahl verschiedener WLAN-Komponenten nicht ausgeschlossen werden. Um Kompatibilitätsprobleme zu vermeiden, müssen alle Komponenten von der Wi-Fi Alliance zertifiziert sein und die IEEE 802.11 Standards unterstützen. Alle WLAN-Komponenten dürfen nur von den Regulierungsgremien des Landes freigegebene Frequenzbänder verwenden. Jeder Anbieter von WLAN-Komponenten muss hierüber in den Datenblättern zu seinem Produkt kostenfrei Auskunft erteilen.

Im Rahmen der Beschaffung von Access Points und korrespondierenden Managementsystemen sollte Folgendes geprüft werden:

- Wie viele WLAN-Kanäle können verwaltet werden?
- Ist die SSID einstellbar?
- Welche kryptographischen Verfahren sind implementiert?
- Können für die Authentisierung die gewünschten Modi eingestellt werden?
- Welche EAP-Methoden werden unterstützt?
- Kann die Administration auf kryptographisch abgesicherte Kommunikationswege beschränkt werden? Können Klartextprotokolle abgeschaltet werden?
- Ist Netflow in Version 9 (RFC 3954) zur Informationsflusskontrolle nutzbar?
- Sind Mechanismen zur Zugriffssteuerung vorhanden?
- Sind Mechanismen für eine applikationsbasierte Umsetzung von Quality of Service integriert?

Einige WLAN-Komponenten können drahtlos direkt über das WLAN konfiguriert werden. Ist diese Funktion integraler Bestandteil der Komponenten, sollte sie abschaltbar sein, um Risiken zu minimieren. Um in der Institution etablierte Rollen- und Berechtigungskonzepte umzusetzen, darf ein Administrationszugriff auf WLAN-Komponenten nur für autorisierte Personen möglich sein.

Im Rahmen der Beschaffung sollte auch geprüft werden, ob alle WLAN-Komponenten mit den etablierten Netz-, Sicherheits-, Authentisierungs-, Monitoring- und Protokollierungsinfrastrukturen korrekt zusammenarbeiten. Hierzu zählt z. B. Folgendes:

- Die im WLAN genutzten Authentisierungsmethoden müssen von den Betriebssystemen und der Hardware der Clients, den Access Points, den Netzmanagementsystemen und den Authentisierungsservern unterstützt werden.
- Falls im WLAN die Authentisierung nach IEEE 802.1X erfolgt, müssen die Access Points die Authentisierungsmethoden der EAP-Familie unterstützen und die mitgeteilten Informationen innerhalb von IEEE 802.1X korrekt verarbeiten.
- Zusätzlich ist zu prüfen, ob die Authentisierungsanfragen mittels sicherer Abfragemethoden an eine zentrale Benutzerdatenbank durchgereicht werden können.

Ist geplant, eine größere WLAN-Infrastruktur zu etablieren, sollte durch eine entsprechende Teststellung geprüft werden, ob die definierten und dokumentierten Anforderungen eingehalten werden, bevor die Infrastruktur endgültig beschafft wird.

NET.2.1.M12 Einsatz einer geeigneten WLAN-Management-Lösung

Der Leistungsumfang der eingesetzten WLAN-Managementlösung sollte mindestens die folgenden Aspekte erfüllen:

- Dokumentation der Firmware-Stände der Access Points und der WLAN-Clients,
- Dokumentation der Konfigurationen,
- Historienverwaltung von Konfigurationsänderungen,
- Auswertung und Bewertung von Alarmen,
- Auswertung von Statistiken zur Fehlersuche,
- Auslösung von Maßnahmen bei einem vermuteten Sicherheitsvorfall,
- Anpassung von Schwellwerten zur Alarmauslösung an eine geänderte WLAN-Nutzung,
- Protokollierung und deren sinnvollen Aufbereitung für die Auswertung und
- versenden der Protokolldaten an ein zentrales Logging-System zur nachgelagerten Auswertung.

Beim WLAN-Konfigurationsmanagement sind im Hinblick auf die Sicherheit einer Installation die zentrale Administration der Sicherheitseinstellungen und die Bereitstellung abgesicherter Installations- und Managementwege von entscheidender Bedeutung. Unter Sicherheitsaspekten ist darüber hinaus dringend zu empfehlen, dass WLAN-Managementsysteme dabei unterstützen, die Luftschnittstelle zu überwachen und die dabei gewonnenen Messergebnisse und Funktionen zu interpretieren. Zu diesen Messergebnissen und Funktionen gehören Rogue Access Point Detection, Wireless Intrusion Detection System (WIDS) sowie Wireless Intrusion Prevention System (WIPS). Die beiden nachfolgenden Tabellen benennen für die drei fiktiven Szenarien die Mindestparameter zur Erkennung von Manipulationen und Angriffen.

Mindestparameter zur Erkennung von Manipulationen und Angriffen	Szenario 1	Szenario 2	Szenario 3
Erkennen von Clients mit ungültigem MAC OUI			ja
Erkennen von Deauthentication Broadcast	ja	ja	ja

Mindestparameter zur Erkennung von Manipulationen und Angriffen	Szenario 1	Szenario 2	Szenario 3
Erkennen von Deassociation Broadcast	ja	ja	ja
Erkennen der missbräuchlichen Nutzung gültiger SSIDs für Ad-hoc-Netze		ja	ja
Erkennen eines Malformed Frame (Large Duration)		ja	ja
Erkennen eines Malformed Frame (HT-IE)			ja
Erkennen eines Malformed Frame (Association Request)			ja
Erkennen eines Malformed Frame (Authentisierung)			ja
Erkennen von Access-Point-Identitätswechseln			ja
Erkennen des Missbrauchs von gültigen SSIDs			ja
Erkennen von Wireless Bridges			ja
Erkennen von 802.11 40MHz-Intoleranzeinstellungen			ja
Erkennen des aktiven 802.11n Greenfield-Modus			ja
Erkennen von Access-Point-Flood-Attacken			ja
Erkennen von Client-Flood-Attacken			ja
Erkennen von CTS-Rate-Anomalien			ja
Erkennen von RTS-Rate-Anomalien			ja
Erkennen von ungültigen Adress-Kombinationen			ja
Erkennen eines Overflow IE			ja

Mindestparameter zur Erkennung von Manipulationen und Angriffen	Szenario 1	Szenario 2	Szenario 3
Erkennen eines Overflow EAPOL Key			ja
Erkennen eines falschen Beacon-Channel			ja

Tabelle 6: Erkennung von Manipulationen und Angriffen durch ein WIDS an der Infrastruktur

	Szenario 1	Szenario 2	Szenario 3
Erkennen von fälschlicherweise akzeptierten Verbindungen an gültigen WLAN-Stationen	ja	ja	ja
Erkennen von Disconnect-Angriffen		ja	ja
Erkennen von Omerta-Angriffen		ja	ja
Erkennen von FATA-Jack-Angriffen		ja	ja
Erkennen eines Block-ACK-DOS		ja	ja
Erkennen von Hotspot-Angriffen		ja	ja
Erkennen von Power-Save-DOS-Angriffen		ja	ja
Erkennen von nicht verschlüsselnden, jedoch von der Institution freigegebenen Clients		ja	ja
Erkennen von EAP-Rate-Anomalien			ja
Erkennen von Rate-Anomalien			ja
Erkennen von TKIP-Replay-Angriffen			ja
Erkennen von AS-LEAP-Angriffen			ja
Erkennen von Wireless Packet Injections mittels Air Jack			ja

Tabelle 7: Erkennung von Manipulationen und Angriffen durch ein WIDS auf dem Client

Mittels einer Controller-basierten Lösung können Richtlinien zentral verwaltet und der WLAN-Traffic kann auf dem WLAN-Controller terminiert werden. Hierdurch kann z. B. der eventuell vorhandene Gästeverkehr zur DMZ oder Firewall weitergeleitet werden. Bei einer Controller-losen Umgebung müssen die Access Points und nachgelagerte Systeme mittels VPN diese Funktion übernehmen.

Ein weiterer Aspekt der Controller-basierten Lösung ist, dass das Failover- sowie das Failback-Verhalten einfach koordiniert werden können. Der IT-Betrieb muss sicherstellen, dass bei Ausfall eines Access Points der Netzverkehr nicht zu stark beeinträchtigt wird. In einem Controller-basierten Modell dient der Controller als Single Point of Coordination für alle Access Points. Fällt einer der Access Points aus, reagiert der Controller, um so die Latenzen so kurz wie möglich zu halten. Dies wird erreicht, indem er die zentral gespeicherten Session-Informationen eines WLAN-Benutzers sofort an einen verfügbaren Access Point weitergibt. Bei Controller-losen Infrastrukturen muss dies durch dem Routing-Protokoll ähnliche Mechanismen innerhalb des lokalen Netzes implementiert werden.

NET.2.1.M13 Regelmäßige Sicherheitschecks in WLANs

Um WLANs sicher betreiben zu können, ist es besonders wichtig, die Sicherheitsvorgaben umzusetzen und die Verfügbarkeit regelmäßig zu überprüfen. Die Messungen der Performance müssen in die vorhandene Monitoring- und Protokollierungsinfrastruktur integriert sein. Im einfachsten Fall kann eine WLAN-Analyse über einen WLAN-Client erfolgen, der mit entsprechender Spezial-Software ausgestattet ist. Diese Art der Überwachung ist jedoch nur für Szenario 1 zu empfehlen. Besser und stetiger kann die WLAN-Infrastruktur kontrolliert werden, wenn die hierfür notwendigen Überwachungsfunktionen mit in die Access Points integriert sind. Mit Hilfe von in den Access Points integrierten Detektoren können folgende Überwachungsaktionen automatisiert durchgeführt werden:

- Fremdgeräte (insbesondere fremde Access Points) können erkannt werden.
- Wireless Site Surveys können mit dem Ziel durchgeführt werden, Informationen zu Abdeckung, Datenraten, Übertragungskapazität, Applikationsbitrate, Bitübertragungsrate pro WLAN-Benutzer, Quality of Service (QoS) usw. zu erhalten.
- Die Konfiguration von WLAN-Netzelementen kann überwacht werden.

Der IT-Betrieb sollte die folgenden Aufgaben planen und festschreiben, um eine angemessene Alarm- und Fehlerbehandlung sicherzustellen:

- Alarme sollten ausgewertet und bewertet werden.
- Statistiken sollten zur Fehlersuche ausgewertet werden.
- Bei einem vermuteten Sicherheitsvorfall sollten abgestimmte Maßnahmen ausgelöst werden.
- Bei einer geänderten WLAN-Nutzung sollten die Schwellwerte zur Alarmauslösung angepasst werden.

Im Zuge eines Sicherheitschecks kann ein WLAN auch mit Hilfe eines Penetrationstests auf Schwachstellen untersucht werden. Dabei ist für alle getroffenen Sicherheitsmaßnahmen genau zu prüfen, ob diese den Angriffen gewachsen sind, gegen die sie wirken sollen. In Tabelle 8 sind Empfehlungen für Zeitintervalle abgebildet, um interne und externe Penetrationstests durchzuführen.

	Szenario 1	Szenario 2	Szenario 3
Zeitintervall für interne Penetrationstests	jährlich	halbjährlich	vierteljährlich
Zeitintervall für externe Penetrationstests	-	alle ein bis zwei Jahre	jährlich

Tabelle 8: Empfohlene Zeitintervalle für regelmäßige Penetrationstests

NET.2.1.M14 Regelmäßige Audits der WLAN-Komponenten

Bei allen Komponenten der WLAN-Infrastruktur (Access Points, Distribution System, WLAN-Management-Lösung etc.) sollte regelmäßig überprüft werden, ob alle festgelegten Sicherheitsmaßnahmen umgesetzt und korrekt konfiguriert sind. Das WLAN-Managementsystem sollte je nach bereitgestelltem Funktionsumfang nicht nur die aktuellen, sondern auch zurückliegende Konfigurationen der Access Points verwalten. Öffentlich aufgestellte Access Points sollten regelmäßig stichprobenartig darauf geprüft werden, ob es gewaltsame Öffnungs- oder Manipulationsversuche gab. Sollten Unregelmäßigkeiten oder Schwachstellen erkannt werden, sollten diese dokumentiert werden. Abweichungen sollte nachgegangen werden.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

NET.2.1.M15 Verwendung eines VPN zur Absicherung von WLANs (CI)

Um die Kommunikation über die WLAN-Infrastruktur zusätzlich abzusichern und so sicherzustellen, dass die Übertragung schutzbedarfsgerecht vollständig abgesichert ist, sollte ein VPN eingesetzt werden. Weiterführende Informationen zum Thema VPN können dem Baustein NET.3.3 *VPN* bzw. den zugehörigen Umsetzungshinweisen entnommen werden.

NET.2.1.M16 Zusätzliche Absicherung bei der Anbindung von WLANs an ein LAN (CIA)

Wird eine WLAN-Infrastruktur an ein LAN angebunden, sollte der Übergang zwischen WLAN- und LAN-Infrastruktur entsprechend dem höheren Schutzbedarf, beispielsweise durch ein Intrusion Detection System bzw. Intrusion Prevention System (IDS/IPS) abgesichert sein. Weiterführende Informationen zum Thema IDS/IPS können dem Baustein NET.3.4 *IDS/IPS* bzw. den zugehörigen Umsetzungshinweisen entnommen werden.

NET.2.1.M17 Absicherung der Kommunikation zwischen Access Points (C)

Zwischen den Access Points sollte über die Funkschnittstelle und das LAN verschlüsselt kommuniziert werden, um die Vertraulichkeit der übermittelten Informationen zu gewährleisten.

Kommunikation über die Funkschnittstelle

Um die Kommunikation über die Funkschnittstelle abzusichern, sind die Maßnahmen NET.2.1.M3 *Auswahl geeigneter Kryptoverfahren für WLAN* und NET.2.1.M5 *Sichere Basis-Konfiguration der Access Points* anzuwenden.

Kommunikation zwischen Access Point und WLAN-Managementsystem

Aufgrund des erhöhten Schutzbedarfs wird davon ausgegangen, dass die Kommunikation zwischen einem Access Point und dem WLAN-Managementsystem nicht cloudbasiert erfolgt. In der folgenden Tabelle sind Protokolle zu finden, die dazu eingesetzt werden können, um die Kommunikation abzusichern. Der zu erfüllende Schutzbedarf wird dabei berücksichtigt.

	Beispiel 1	Beispiel 2	Beispiel 3
Protokoll	CAPWAP + DTLS	IPSec	TLS v1.2
Authentisierung	Zertifikat oder Passwort (mit mindestens 16 Zeichen)	Zertifikat oder Passwort (mit mindestens 16 Zeichen)	Zertifikate (idealerweise im TPM)

Tabelle 9: Kommunikation zwischen Access Point und WLAN-Managementsystem

Kommunikation von Access Point zu Access Point

Eine Kommunikation von Access Point zu Access Point ist in der Controller-basierten WLAN-Infrastruktur nicht direkt möglich, sondern erfolgt immer über den zentralen WLAN-Controller. Die möglichen Protokolle und zugehörigen Authentisierungsmethoden wurden bereits in Tabelle 9 aufgezeigt. Die folgende Tabelle führt deshalb nur die Protokolle und zugehörigen Authentisierungsmethoden für eine Controller-lose WLAN-Infrastruktur auf.

	Beispiel 1	Beispiel 2	Beispiel 3
Protokoll	GRE (im Default-VLAN)	GRE-IPSec	TLS v1.2

	Beispiel 1	Beispiel 2	Beispiel 3
Authentisierung	keine	Zertifikat	Zertifikate

Tabelle 10: Kommunikation von Access Point zu Access Point

Das aufgezeigte GRE-Protokoll in Beispiel 1 bietet selbst keine Verschlüsselung und schützt nicht ausreichend hinsichtlich der Vertraulichkeit und Integrität für Roaming- und WLAN-Managementinformationen. Es dient an dieser Stelle nur der Sensibilisierung bei der Auswahl der WLAN-Produkte und sollte nicht verwendet werden.

NET.2.1.M18 Einsatz von Wireless Intrusion Detection / Wireless Intrusion Prevention Systemen (CIA)

Um Sicherheitsvorfälle und Schwachstellen zeitnah zu identifizieren und entsprechende Gegenmaßnahmen direkt einleiten zu können, sollten WIDS/ WIPS eingesetzt werden.

3 Weiterführende Informationen

3.1 Wissenswertes

WLANs können in zwei verschiedenen Architekturen betrieben werden. Im Ad-hoc-Modus kommunizieren zwei oder mehr mobile Endgeräte (also Clients), die mit WLAN-Funktionalität ausgestattet sind, direkt miteinander. In den meisten Fällen wird ein WLAN im Infrastruktur-Modus betrieben, d. h. die Kommunikation der Clients erfolgt über zentrale Access Points. Über die Access Points erfolgt auch die Verbindung in kabelgebundene LAN-Segmente.

Der Infrastruktur-Modus lässt mehrere Einsatzvarianten zu:

- Mittels mehrerer Access Points können überlappende Funkzellen installiert werden, sodass beim Übergang eines Clients in die nächste Funkzelle die Funkverbindung aufrecht erhalten werden kann ("Roaming"). Zwei Access Points können als Brücke (Bridge) zwischen zwei leitungsgebundenen LANs eingesetzt werden. Ebenso ist der Einsatz eines Access Points als Relaisstation (Repeater) möglich, um die Reichweite zu erhöhen
- Werden entsprechende Komponenten (Richtantennen) an den Access Points verwendet, können WLANs auch dazu eingesetzt werden, um Liegenschaften zu vernetzen. Hier können laut Herstellerangaben Reichweiten im Kilometerbereich erreicht werden. Die Access Points können dabei als Relaisstation oder Brücke betrieben werden.

Im Standard IEEE 802.11 werden die Bezeichnungen Independent Basic Service Set (IBSS) für Funk-Netze im Ad-hoc-Modus und Basic Service Set (BSS) für Konstellationen im Infrastruktur-Modus mit einem Access Point verwendet. Mehrere gekoppelte BSS werden als Extended Service Set (ESS) bezeichnet, das koppelnde Netz wird Distribution System (DS) genannt.

Im 2,4 GHz-Frequenzbereich stehen in Deutschland 13 Frequenzkanäle mit einem Frequenzabstand von 5 MHz für die Funkübertragung zur Verfügung. Bei einer Kanalbandbreite von ca. 22 MHz können jedoch nur maximal 3 Kanäle gleichzeitig überlappungsfrei genutzt werden. Im Frequenzbereich von 5,15 bis 5,35 GHz und bei 5,47 bis 5,725 GHz sind in Deutschland insgesamt 19 Kanäle in einem Abstand von 20 MHz unter Auflagen freigegeben worden. Bei einer Kanalbandbreite von 20 MHz werden direkt benachbarte Kanäle hier nicht gestört. Im 5 GHz Frequenzbereich arbeiten auch militärische und zivile Radar- und Navigationsanwendungen, und es dürfen hier nur Systeme eingesetzt werden, die eine dynamische Frequenzwahl und eine Anpassung der Sendeleistung unterstützen.

Die in IEEE 802.11 definierten Mechanismen dienen ausschließlich dazu, die Funkstrecke zwischen den Clients und Access Points zu sichern.

Als zusätzlicher Schutz der Authentisierung kann das Extensible Authentication Protocol (EAP) gemäß Standard IEEE 802.1X verwendet werden. EAP wird im RFC 3748 genau beschrieben. Die Benutzer melden sich hier bei einer Authentisierungsinstanz an, z. B. an einem RADIUS-Server, und dieser prüft die Zugangsberechtigung, bevor der Sitzungsschlüssel ausgetauscht wird. EAP unterstützt eine Reihe von Authentisierungsmethoden, so dass auch Zertifikate und Zwei-Faktor-Authentisierungen genutzt werden können.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "WLAN-Betrieb" finden sich unter anderem in folgenden Veröffentlichungen:

[BSIDKS] Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte

Bundesamt für Sicherheit in der Informationstechnik (BSI), 2009, https://www.bsi.bund.de/DE/Publikationen/Broschueren/Drahtloskom/drahtloskom.html, zuletzt abgerufen am 05.10.2018

[IEEE] Institute of Electrical and Electronics Engineers (IEEE)

https://www.ieee.org/index.html, zuletzt abgerufen am 05.10.2018

[ISILANA] Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA)

Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.1, August 2014
https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-LANA/lana_node.html, zuletzt abgerufen am 05.10.2018

[KB2977292] Microsoft security advisory

Sicherheitsupdate für Windows 7 für x64-basierte Systeme, https://www.microsoft.com/de-de/download/details.aspx?id=44350, zuletzt abgerufen am 05.10.2018

[NIST800153] Guidelines for Securing Wireless Local Area Network (WLANs)

NIST Special Publication 800-153, Februar 2013, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf, zuletzt abgerufen am 05.10.2018

[NIST80097] Establishing Wireless Robust Security Networks

A Guide to IEEE 802.11, NIST Special Publication 800-97, Februar 2007, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-97.pdf, zuletzt abgerufen am 05.10.2018

[RSWLAN] Mehr Rechtssicherheit bei WLAN

Bundesministerium für Wirtschaft und Energie (BMWi), https://www.bmwi.de/Redaktion/DE/Artikel/Digitale-Welt/wlan.html, zuletzt abgerufen am 05.10.2018

[TR03103] Technische Richtlinie Sicheres Wireless LAN

Bundesamt für Sicherheit in der Informationstechnik (BSI), Oktober 2005, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03103/index_htm.html, zuletzt abgerufen am 05.10.2018

[WIFIA] Hersteller-Konsortium Wi-Fi Alliance

http://www.wi-fi.org/, zuletzt abgerufen am 05.10.2018

Umsetzungshinweise zum Baustein NET.2.2 WLAN-Nutzung

1 Beschreibung

1.1 Einleitung

Über Wireless LANs (WLANs) können drahtlose lokale Netze aufgebaut oder bestehende drahtgebundene Netze erweitert werden. Bis heute basieren fast alle am Markt verfügbaren WLAN-Komponenten auf dem Standard IEEE 802.11 und seinen Ergänzungen. Eine besondere Rolle nimmt dabei das Hersteller-Konsortium Wi-Fi Alliance ein, das basierend auf dem Standard IEEE 802.11 mit "Wi-Fi" einen Industriestandard geschaffen hat. Dabei bestätigt die Wi-Fi Alliance mit dem Wi-Fi-Gütesiegel, dass ein Gerät gewisse Interoperabilitäts- und Konformitätstests bestanden hat.

Alle Benutzer (inklusive Leitung der Institution) müssen über WLAN-Grundlagen informiert und zu möglichen Gefahren sensibilisiert sein, die entstehen können, wenn WLANs unsachgemäß verwendet werden. Sie müssen über die erforderlichen Kenntnisse verfügen, um Sicherheitsmaßnahmen richtig verstehen und anwenden zu können. Insbesondere muss ihnen bekannt sein, was von ihnen im Hinblick auf Informationssicherheit erwartet wird und wie sie in bestimmten Situationen bei der Nutzung von WLANs reagieren sollten.

1.2 Lebenszyklus

Planung und Konzeption

Bevor WLANs betrieben und genutzt werden, ist eine sorgfältige Planung notwendig. Um Benutzer nicht mit zu vielen betrieblichen und sicherheitstechnischen Details einer WLAN-Infrastruktur zu überlasten, sollte eine eigene WLAN-Richtlinie speziell für diese Zielgruppe erstellt werden (siehe NET.2.2.M1 *Erstellung einer Benutzerrichtlinie für WLAN*).

Umsetzung

Um die Sicherheitsanforderungen der Institution in der täglichen Nutzung von WLANs zu erfüllen, müssen die Benutzer mit eingebunden werden. So müssen sie über Sicherheitsmaßnahmen informiert werden, die nicht nur mit technischen Mitteln umgesetzt werden können und die ihre Mitwirkung erfordern. Um Sicherheitsvorfälle zu minimieren und auf mögliche Gefahren hinzuweisen, die entstehen können, wenn WLANs unsachgemäß genutzt werden, sind Benutzer ausreichend zu schulen und zu sensibilisieren (siehe NET.2.2.M2 *Sensibilisierung und Schulung der WLAN-Benutzer*).

Betrieb

Dürfen externe Hotspots genutzt werden, dann müssen die Mitarbeiter gezielt hinsichtlich der Hotspot-Nutzung geschult werden und entsprechende Maßnahmen umsetzen (siehe NET.2.2.M3 *Absicherung der WLAN-Nutzung in unsicheren Umgebungen*).

Notfallvorsorge

Wurden Angriffe auf ein WLAN oder innerhalb eines WLANs erkannt, so müssen die Benutzer des WLANs wissen, wie sie sich zu verhalten haben (siehe NET.2.2.M4 *Verhaltensregeln bei WLAN-Sicherheitsvorfällen*).

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "WLAN-Nutzung" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

NET.2.2.M1 Erstellung einer Benutzerrichtlinie für WLAN [Leiter IT]

Um Benutzer nicht mit zu vielen betrieblichen und sicherheitstechnischen Details einer WLAN-Infrastruktur zu überlasten, sollte eine eigene WLAN-Richtlinie speziell für diese Zielgruppe erstellt werden. Die Benutzerrichtlinie baut auf der allgemeinen Sicherheitsrichtlinie der Institution auf und konkretisiert die wesentlichen Kernaspekte, um WLANs sicher zu nutzen. In einer solchen Benutzerrichtlinie sollten dann kurz die Besonderheiten bei der WLAN-Nutzung beschrieben werden, wie z. B.

- mit welchen internen und externen Netzen die WLAN-Clients verbunden werden dürfen,
- unter welchen Rahmenbedingungen sie sich an internen oder externen WLANs anmelden dürfen,
- ob und wie Hotspots genutzt werden dürfen,
- dass der Ad-hoc-Modus abzuschalten ist, damit kein anderer Client direkt auf die WLAN-Clients zugreifen kann,
- welche Schritte bei (vermuteter) Kompromittierung der WLAN-Clients zu unternehmen sind, vor allem, wer zu benachrichtigen ist.

Wichtig ist auch, dass klar beschrieben wird, wie mit clientseitigen Sicherheitslösungen umzugehen ist. Dazu gehört beispielsweise, dass

- keine sicherheitsrelevanten Konfigurationen verändert werden dürfen,
- eine vorhandene Personal Firewall nicht abgeschaltet werden darf,
- alle Freigaben von Verzeichnissen oder Diensten deaktiviert oder zumindest durch gute Passwörter geschützt sind,
- für die Nutzung externer WLANs nach Möglichkeit nur spezielle Benutzerkonten mit restriktiver Rechtevergabe verwendet werden sollten.

Außerdem sollte die Benutzerrichtlinie ein klares Verbot enthalten, ungenehmigt Access Points an das LAN der Institution anzuschließen. Auch muss in der Richtlinie darauf hingewiesen werden, dass die WLAN-Schnittstelle deaktiviert werden muss, wenn sie über einen längeren Zeitraum nicht genutzt wird. Des Weiteren sollte die Richtlinie insbesondere im Hinblick auf die Nutzung von klassifizierten Informationen, beispielsweise Verschlusssachen, Angaben dazu enthalten, welche Daten in WLANs genutzt und übertragen werden dürfen und welche nicht. Benutzer sollten für WLAN-Gefährdungen sowie für Inhalte und Auswirkungen der WLAN-Richtlinie sensibilisiert werden.

Es muss regelmäßig überprüft werden, ob die in der Richtlinie geforderten Inhalte richtig umgesetzt worden sind und die Ergebnisse sollten sinnvoll dokumentiert werden.

NET.2.2.M2 Sensibilisierung und Schulung der WLAN-Benutzer [Leiter IT, Vorgesetzte]

Heutzutage ist fast jeder Mitarbeiter mit einem mobilen Gerät ausgestattet und kann sich mit einem öffentlichen oder internen WLAN verbinden. Über mobile Geräte (z. B. Smartphones) lassen sich WLAN-Hotspots für andere erzeugen oder Ad-Hoc-WLANs aufbauen. Durch diese vielseitigen Nutzungsmöglichkeiten können Sicherheitsprobleme entstehen, wenn die Geräte unsachgemäß eingesetzt werden. Daher müssen alle Mitarbeiter entsprechend sensibilisiert werden. Dies kann beispielsweise mithilfe eines Merkblatts zu möglichen Gefahren, die mit der Nutzung von WLANs verbunden sind, geschehen. Das Merkblatt sollte außerdem die wichtigsten Maßnahmen und Verhaltensweisen enthalten, um entsprechenden Gefährdungen entgegenwirken zu können. Das Merkblatt sollte gemeinsam mit den Geräten übergeben werden, damit die Benutzer verantwortungsvoll mit den Geräten umgehen und diese gewissenhaft nutzen können. Sollte es den Benutzern erlaubt sein, über ihr Gerät sich selbst oder anderen ein WLAN (als Hotspot) zur Verfügung zu stellen, sollten die Schulungsinhalte auch die damit verbundenen Gefährdungen und Maßnahmen enthalten. Es kann beispielsweise darauf hingewiesen werden, dass die WLAN-Kommunikation geschützt werden kann, indem ein komplexes Passwort konfiguriert wird.

Die Sensibilisierung insbesondere von Benutzern, die auf vertrauliche Informationen zugreifen dürfen, sollte multimedial und durch praktische Beispiele geübt und unterstützt werden.

Eine besondere Gefährdung für die WLAN-Clients besteht, wenn öffentliche Funknetze (sog. Hotspots) genutzt werden. Hotspots verwenden häufig keine oder nur schwache Sicherheitsmechanismen, um Kunden einen unkomplizierten Zugang zu ermöglichen. Dadurch können übertragene Informationen in der Regel leicht abgehört werden. Sollen Hotspots für die Einwahl in die Institution genutzt oder vertrauliche Informationen hierüber übertragen werden, müssen die Benutzer gezielt hinsichtlich der Hotspot-Nutzung geschult werden und entsprechende Maßnahmen umsetzen. Beispielsweise müssen sie darauf achten, dass alle Verbindungen geeignet verschlüsselt sind. Bei eventuellen Verdachtsmomenten verursacht durch Warnhinweise oder Umleitungen auf IT-Systeme, die nicht zur Institution gehören, muss davon ausgegangen werden, dass dies ein Sicherheitsvorfall sein könnte.

Jedem Benutzer muss klar sein, dass WLANs zu nutzen die Mobilität stark unterstützt, jedoch auch Gefahren birgt, da Angreifer sich außerhalb des Sichtfeldes oder des vermuteten räumlichen WLAN-Empfangsbereiches befinden können.

NET.2.2.M3 Absicherung der WLAN-Nutzung in unsicheren Umgebungen [IT-Betrieb]

Bei Hotspots handelt es sich um einen räumlich begrenzten Funkbereich. Meistens werden Hotspots explizit aufgebaut, damit sie durch fremde Teilnehmer genutzt werden können. Ihr Hauptzweck ist üblicherweise der drahtlose Zugang zum Internet. Häufig findet man solche Hotspots in Hotels, Flughäfen, Messehallen, Bahnhöfen und Kongresszentren.

Hotspots sollten immer als unsicheres Netz betrachtet werden, zum einem, da das dort vorhandene Sicherheitsniveau von außen nur schwer einzuschätzen ist und zum anderen, weil die meisten Hotspots ihre Dienste in Form von "Shared Networks" anbieten. Dadurch kann im Allgemeinen von jedem Endgerät auf jedes andere Endgerät im Netz zugegriffen werden. Ist das Risiko, das bei der Nutzung eines Hotspots entsteht, generell nicht abschätzbar, so kann erwogen werden, die Nutzung von Hotspots durch die WLAN-Sicherheitsrichtlinie vollständig zu verbieten.

Die Betreiber von Hotspots können viel für die Sicherheit der von ihnen angebotenen Funkstrecke und anderen Dienstleistungen tun (siehe NET.2.3 *Betrieb von Hotspots*), ohne Mitarbeit der Benutzer ist eine vernünftige Absicherung allerdings nicht zu erreichen. Hierzu gehören unter anderem folgende Maßnahmen:

- Jeder Benutzer eines Hotspots sollte seine Sicherheitsanforderungen kennen und danach entscheiden, ob bzw. unter welchen Bedingungen ihm die Nutzung des Hotspots erlaubt ist.
- Die Anmeldung am Hotspot erfolgt meist über ein Web-Portal bzw. über eine Web-Applikation. Diese muss für den Schutz der Anmelde-Information sorgen. Die Authentisierung sollte immer verschlüsselt erfolgen.
- WLANs, die nur sporadisch genutzt wurden, sollten durch die Benutzer aus der Historie entfernt werden. Dazu wird die Kennung des WLANs (SSID) aus der Liste entfernt. Dadurch wird verhindert, dass sich das Endgerät ungewollt in das WLAN einbucht.
- Wenn möglich, sollten für die Nutzung von Hotspots spezielle Benutzerkonten mit sicherer Grundkonfiguration und restriktiven Rechten angelegt werden. Keinesfalls sollte sich ein Benutzer mit Administratorrechten von seinem Client aus an externen WLANs anmelden.
- Spätestens dann, wenn finanzrelevante, personenbezogene oder andere sensible Daten wie Kreditkartennummern, PINs, Passwörter oder auch E-Mails übertragen werden sollen, muss sichergestellt werden, dass alle notwendigen Sicherheitsmaßnahmen auf den Clients, vor allem Verschlüsselung, aktiviert sind. Als Beispiel wäre hier das sichere Bearbeiten von E-Mails über eine HTTPS-Webschnittstelle zu nennen. Vertrauliche Informationen dürfen nie unverschlüsselt über fremde Netze übertragen werden.
- Über fremde WLANs (z. B. bereitgestellte Gastzugänge fremder Institution oder öffentliche Hotspots) dürfen die Benutzer nur über VPNs auf interne Ressourcen der Institution zugreifen. Dadurch kann die Kommunikation in die eigene Institution unabhängig von den etablierten Schutzmechanismen der verwendeten WLAN-Infrastruktur zusätzlich abgesichert werden. Weitere Informationen hierzu finden sich im Baustein NET.3.3 VPN bzw. in den zugehörigen Umsetzungshinweisen.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "WLAN-Nutzung".

NET.2.2.M4 Verhaltensregeln bei WLAN-Sicherheitsvorfällen

Falls sich das WLAN in nicht vorgesehener Weise verhält (z. B. WLAN ist längere Zeit nicht verfügbar, auf Netzressourcen kann nicht zugegriffen werden, die Netzperformance bricht dauerhaft ein), kann dies durch einen Sicherheitsvorfall verursacht worden sein.

Die WLAN-Benutzer sollten Folgendes umsetzen:

- Sie sollten ihre Arbeitsergebnisse sichern, den WLAN-Zugriff beenden und die WLAN-Schnittstelle ihres Clients deaktivieren.
- Sollten Fehlermeldungen erscheinen oder sich der Client nicht normal verhalten haben, so sollten diese durch die Benutzer genau dokumentiert werden. Ebenso sollte dokumentiert werden, was der Benutzer getan hat bevor bzw. während der Sicherheitsvorfall eingetreten ist. Mithilfe dieser Informationen kann der IT-Betrieb den Grund und die Auswirkungen des Vorfalls eventuell schneller eingrenzen und Gegenmaßnahmen gezielter einleiten.
- Außerdem sollten sie den IT-Betrieb über eine geeignete Eskalationsstufe benachrichtigen.

3 Weiterführende Informationen

3.1 Wissenswertes

Über den Baustein, die Umsetzungshinweise und die Literaturübersicht hinausgehend liegen derzeit keine weiteren wissenswerten Informationen vor.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "WLAN-Nutzung" finden sich unter anderem in folgenden Veröffentlichungen:

[BSIDKS] Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte

Bundesamt für Sicherheit in der Informationstechnik (BSI), 2009, https://www.bsi.bund.de/DE/Publikationen/Broschueren/Drahtloskom/drahtloskom.html, zuletzt abgerufen am 05.10.2018

[IEEE] Institute of Electrical and Electronics Engineers (IEEE)

https://www.ieee.org/index.html, zuletzt abgerufen am 05.10.2018

[ISILANA] Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA)

Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.1, August 2014
https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-LANA/lana_node.html, zuletzt abgerufen am 05.10.2018

[KB2977292] Microsoft security advisory

Sicherheitsupdate für Windows 7 für x64-basierte Systeme, https://www.microsoft.com/de-de/download/details.aspx?id=44350, zuletzt abgerufen am 05.10.2018

[NIST800153] Guidelines for Securing Wireless Local Area Network (WLANs)

NIST Special Publication 800-153, Februar 2013, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf, zuletzt abgerufen am 05.10.2018

[NIST80097] Establishing Wireless Robust Security Networks

A Guide to IEEE 802.11, NIST Special Publication 800-97, Februar 2007, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-97.pdf, zuletzt abgerufen am 05.10.2018

[RSWLAN] Mehr Rechtssicherheit bei WLAN

Bundesministerium für Wirtschaft und Energie (BMWi), https://www.bmwi.de/Redaktion/DE/Artikel/Digitale-Welt/wlan.html, zuletzt abgerufen am 05.10.2018

[TR02102] Kryptographische Verfahren

Empfehlungen und Schlüssellängen: BSI TR-02102, Bundesamt für Sicherheit in der Informationstechnik (BSI), Januar 2018, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html , zuletzt abgerufen am 13.09.2018

[TR03103] Technische Richtlinie Sicheres Wireless LAN

Bundesamt für Sicherheit in der Informationstechnik (BSI), Oktober 2005, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03103/index_htm.html, zuletzt abgerufen am 05.10.2018

[WIFIA] Hersteller-Konsortium Wi-Fi Alliance

http://www.wi-fi.org/, zuletzt abgerufen am 05.10.2018

Umsetzungshinweise zum Baustein NET.4.1 TK-Anlagen

1 Beschreibung

1.1 Einleitung

Hinweis: Die Umsetzungshinweise basieren auf den Maßnahmen der 15. Ergänzungslieferung der IT-Grundschutz-Kataloge (Jahr 2015). Die Empfehlungen können sinngemäß umgesetzt werden, es ist jedoch nicht gewährleistet, dass sie immer dem Stand der Technik entsprechen. Das BSI freut sich daher über Anmerkungen, konstruktive Kritik und Verbesserungsvorschläge unter besonderer Berücksichtigung des aktuellen Stands der Technik. Bitte verwenden Sie hierfür die E-Mail-Adresse grundschutz@bsi.bund.de

---

Mit einer Telekommunikationsanlage, kurz TK-Anlage, können die Telefone einer Institution intern verbunden und extern an ein öffentliches Telefonnetz (Public Switched Telephone Network, PSTN) angeschlossen werden. Neben der Sprachtelefonie können, abhängig von den angeschlossenen Endgeräten, weitere Dienste genutzt werden. So ist es möglich, mittels TK-Anlagen Daten, Texte, Grafiken und Bewegtbilder zu übertragen. Die Informationen können dabei analog oder digital über drahtgebundene oder drahtlose Übertragungsmedien übermittelt werden.

Je nach Anbindung und genutzter Datennetze können in einer Institution Telekommunikationsanlagen in verschiedenen Ausprägungen eingesetzt werden:

- Klassische TK-Anlagen
  Klassische TK-Anlagen nutzen zum Verbindungsaufbau und zur Übertragung je nach vorhandener Technik ein separates Netz als TK-Infrastruktur. An die Anlage können beispielsweise Telefone, Faxgeräte, Modems und Anrufbeantworter angeschlossen werden.
- VoIP-System
  Bei Voice over IP (VoIP) wird anstatt einer separaten TK-Infrastruktur mit eigener Verkabelung ein IP-Datennetz genutzt, um die Endgeräte an die TK-Anlage anzuschließen. Die Endgeräte kommunizieren bei VoIP mit der TK-Anlage oder anderen VoIP-Geräten über IP-basierte Signalisierungs- und Medientransportprotokolle. Der Übergang in das öffentliche Telefonnetz erfolgt über ein Gateway innerhalb der Institution.
- Hybrid System / Hybrid Anlage
  Aufgrund der zunehmenden Bedeutung von VoIP werden TK-Anlagen angeboten, die die klassische Telefonie mit VoIP-Telefonie vereinen. Sogenannte Hybridanlagen verfügen neben den Bestandteilen einer klassischen TK-Anlage zusätzlich über einen Anschluss an das Datennetz, über den IP-Telefone mit der TK-Anlage kommunizieren können. Mit einer Hybrid-Anlage können die klassische digitale oder analoge Telefonie und VoIP gleichzeitig betrieben werden. Auch ist es möglich, mit einer Hybrid-Anlage schrittweise auf eine VoIP-Infrastruktur zu migrieren.
- IP-Anlagenanschluss
  Bei der Nutzung von VoIP kann der PSTN-Anschluss auch bei einem externen Anbieter liegen. Das (interne) VoIP-System kommuniziert auch nach außen primär über das Internet (IP) mit dem externen Dienstleister. Diese Variante wird IP-Anlagenanschluss genannt.

Generell lässt sich sagen, dass die großen TK-Anbieter das herkömmliche Telefonnetz durch einheitliche IP-basierte Lösungen (Next Generation Network) ablösen, da dann nicht mehr zwischen Daten- und Sprachtransport unterschieden werden muss. Dies wird auch Auswirkungen auf die Schnittstelle zwischen einer internen Telefonanlage und dem TK-Diensteanbieter haben.

1.2 Lebenszyklus

Für eine TK-Anlage sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung über die Beschaffung und den Betrieb bis zur Notfallvorsorge. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Planung und Konzeption

Vor dem Einsatz einer TK-Anlage sollte im Rahmen der Planung eine Anforderungsanalyse erstellt werden (siehe NET.4.1.M1 Anforderungsanalyse und Planung für TK-Anlagen). Eine Richtlinie zum Betrieb und der korrekten Nutzung der TK-Anlage sollte erstellt werden (NET.4.1.M6 Erstellung einer Sicherheitsrichtlinie für TK-Anlagen).

Beschaffung

Bei der Beschaffung einer TK-Anlage sollte darauf geachtet werden, geeignete TK-Diensteanbieter zu ermitteln (siehe NET.4.1.M2 Auswahl von TK-Diensteanbietern). Grundsätzlich sollten die Ergebnisse der Anforderungsanalyse die Grundlage für eine Beschaffung bilden (siehe NET.4.1.M13 Beschaffung von TK-Anlagen).

Umsetzung

Bei der Installation sind unbedingt die vom Hersteller voreingestellten Passwörter zu ändern, da die Anlage sonst von beliebigen Angreifern manipuliert werden kann. Ebenso sind alle Schnittstellen abzusichern. Bei der Konfiguration ist nach der Grundregel zu verfahren, dass alle nicht benötigten Leistungsmerkmale abzuschalten sind, weil sie unnötige Risiken mit sich bringen (siehe NET.4.1.M3 Änderung voreingestellter Passwörter und NET.4.1.M4 Absicherung von Remote-Zugängen).

Die TK-Anlage sollte in einem geeigneten Raum aufgestellt werden (siehe NET.4.1.M7 Aufstellung der TK-Anlage)

Betrieb

Die Administrationsarbeiten an der TK-Anlage sollten nach Möglichkeit protokolliert werden, um nachvollziehen zu können, ob sicherheitsrelevante Einstellungen verändert wurden (siehe NET.4.1.M5 Protokollierung bei TK-Anlagen). Bei hohen Sicherheitsanforderungen an den Betrieb der TK-Anlage ist eine regelmäßige Revision der Konfigurationseinstellungen erforderlich (siehe N*ET.4.1.M10 Dokumentation und Revision der TK-Anlagenkonfiguration*). Da die Sicherheit häufig durch die ungeeignete Bedienung der Endgeräte durch die Benutzer unterlaufen wird, sollten die Mitarbeiter in die korrekte Nutzung eingewiesen und regelmäßig für mögliche Gefährdungen sensibilisiert werden (siehe NET.4.1.M9 Schulung zur sicheren Nutzung der TK-Anlage).

Notfallvorsorge

Es müssen geeignete Maßnahmen zur Notfallvorsorge für die TK-Anlage getroffen werden. Zusätzlich sind ihre Konfigurationsdaten regelmäßig zu sichern, um die Anlage nach einem eventuellen Ausfall schnell wieder hochfahren und korrekt konfigurieren zu können (siehe NET.4.1.M14 Notfallfürsorge für TK-Anlagen).

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "TK-Anlagen" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

NET.4.1.M1 Anforderungsanalyse und Planung für TK-Anlagen [IT-Betrieb, Leiter IT]

Bevor eine TK-Anlage beschafft oder eine bestehende Anlage erweitert wird, ist es sinnvoll, eine Anforderungsanalyse durchzuführen. In deren Rahmen muss zunächst die grundsätzliche Frage geklärt werden, welche Funktionen die TK-Anlage neben der reinen Telefonie bieten muss. Darüber hinaus ist das Einsatzszenario der TK-Anlage zu klären. Denkbar ist die Installation einer TK-Anlage beispielsweise für reinen Kundenkontakt, für die bürointerne Kommunikation oder für die Nutzung in einem Call Center. Einsatzszenarien können klären, welche Kommunikationsdienste sinnvollerweise benötigt werden. Für die Auswahl einer TK-Anlage spielt weiterhin die Anzahl der Endgeräte und die Anzahl der gleichzeitig nutzbaren Verbindungen eine Rolle. Das Ergebnis soll die Planung und damit die Auswahl einer für die Institution passenden und sicheren TK-Anlage ermöglichen.

Die Ergebnisse der Anforderungsanalyse müssen dokumentiert und mit den entsprechenden IT-Verantwortlichen abgestimmt werden.

Im Rahmen der Anforderungsanalyse müssen unter anderem folgende Punkte geklärt werden:

- In welcher Ausprägung soll die TK-Anlage genutzt werden: als klassische TK-Anlage, als VoIP-System oder als Hybrid-Anlage? Oder ist ein IP-Anlagenanschluss eine mögliche Alternative?
- Wie viele interne und wie viele externe Anschlüsse soll die TK-Anlage verwalten können? Lässt sich diese Anzahl nach dem Kauf noch erhöhen?
- Wie wird die Anbindung ans öffentliche Telefonnetz (PSTN) erfolgen? Ist die Zahl der gleichzeitig zu führenden Gespräche festgelegt (ISDN bzw. S2m-Leitungen) oder soll diese variabel nach Bedarf gestaltet werden können (IP-Anlagenanschluss)?
- Wie viele interne Kommunikationsverbindungen sollen gleichzeitig möglich sein?
- Welche Aufgaben soll die zu planende TK-Anlage erfüllen? Welche Funktionen sollen bereitgestellt werden? Gibt es Funktionen, die in jedem Fall bereit gestellt werden müssen?
- Können vorhandene Endgeräte alle geforderten Funktionen im Zusammenspiel mit der TK-Anlage am Arbeitsplatz zur Verfügung stellen oder müssen neue Endgeräte beschafft werden?
- Genügt eine eventuell bereits vorhandene Verkabelung den Anforderungen der TK-Anlage oder muss die Verkabelung erneuert werden?
- Soll eine TK-Anlage neu beschafft oder kann eine bestehende TK-Anlage erweitert werden?
- Gibt es besondere Anforderungen an die Verfügbarkeit der TK-Anlage oder an die Vertraulichkeit oder Integrität der gespeicherten oder verarbeiteten Daten?
- Bietet die TK-Anlage die Möglichkeit, nachträglich weitere Funktionen zu implementieren (Hard-, Soft- und/oder Firmware)?
- Ist eine Kommunikation zwischen mehreren TK-Anlagen geplant, um verschiedene Standorte oder Niederlassungen der Institution miteinander zu verbinden? Sind diese vorhandenen TK-Anlagen mit der neu zu planenden kompatibel, so dass alle geforderten Funktionen unternehmensweit zur Verfügung stehen?
- Wie wird die Sicherheit der TK-Anlage (Zutritt und Zugriff), des Telefonnetzes und der Endgeräte gewährleistet?
- Ist ein Service- oder Wartungsvertrag für die TK-Anlage notwendig? Sind eine zeitnahe Reparatur und Störungsbehebung möglich?

Auf Grundlage der Ergebnisse sind die Anforderungen an die TK-Anlage zu definieren und festzulegen. Zusätzliche Marktanalysen und eventuell die Beratung externer Fachfirmen helfen, aus den Anforderungen eine konkrete Planung auszuarbeiten und die für die Institution passende TK-Anlage zu beschaffen.

Eine grundlegende Voraussetzung für den sicheren Einsatz von TK-Anlagen ist eine angemessene Planung im Vorfeld. Der Einsatz von TK-Anlagen kann in mehreren Schritten nach dem Prinzip des Top-Down-Entwurfs geplant werden: Ausgehend vom Gesamtsystem werden konkrete Planungen für Teilkomponenten durchgeführt. Die Planung betrifft dabei nicht nur Aspekte, die klassischerweise mit dem Begriff Sicherheit verknüpft werden, sondern auch normale betriebliche Aspekte, die Anforderungen im Bereich der Sicherheit nach sich ziehen können.

Es ist daher sinnvoll, das eventuell vorhandene Telekommunikationssystem der Institution mit seinen Funktionen detailliert zu erfassen. Zusätzlich ist es notwendig, einen Überblick über die am Telekommunikationssystem angeschlossenen Komponenten zu erhalten.

Von grundlegender Bedeutung ist auch die, in der Anforderungsanalyse bestimmte Betriebsart der TK-Anlage als klassische TK-Anlage, VoIP-Anlage, hybride TK-Anlage oder IP-Anlagenanschluss.

Die nachfolgenden Aspekte sollten bei der Planung des Einsatzes von TK-Anlagen berücksichtigt werden:

Richtlinien für die Nutzung

Um TK-Anlagen sicher und effektiv einsetzen zu können, müssen Sicherheitsvorgaben erstellt werden, die auf den vorhandenen Sicherheitszielen basieren. Außerdem sollen Anforderungen aus den geplanten Einsatzszenarien mit einbezogen werden. Diese spezifischen Sicherheitsvorgaben müssen mit dem übergreifenden Sicherheitskonzept der Institution abgestimmt sein.

Ausstattungsmerkmale/Endgeräte

Je nach Nutzung der TK-Anlage muss festgelegt werden, welche Endgeräte benötigt werden. Neben der klassischen Funktion der Sprachtelefonie bieten schon einfache TK-Anlagen eine Reihe von komfortablen Ausstattungsmerkmalen. Dabei wird sowohl bei klassischen als auch bei hybriden TK-Anlagen zwischen analogen und digitalen Geräten und den Gerätetypen wie Modem, Fax sowie schnurlosen und schnurgebundenen Telefonen unterschieden. Die Auswahl sollte auch Bedieneigenschaften, Bedienkomfort und Geräteeigenschaften berücksichtigen. So können bei den Telefonen beispielsweise je nach konkretem Einsatzbereich auch Headsets oder ganz einfache Geräte ausgewählt werden.

Leistungsmerkmale

TK-Anlagen bieten eine Vielzahl von Leistungsmerkmalen. Diese können sicherheitsrelevante Aspekte beinhalten, die beachtet werden müssen. So gehören zu den sicherheitskritischen Leistungsmerkmalen beispielsweise das Aufschalten, bei dem weitere Gesprächsteilnehmer zu einem bestehenden Telefongespräch hinzugefügt werden können, die Konferenzschaltung, bei der mehrere Teilnehmer gleichzeitig miteinander über die Anlage miteinander telefonieren, und das Heranholen eines ankommenden Telefongespräches von einem fremden auf das eigene Telefon. Während der Planung des Einsatzes ist zu entscheiden, welche der von der TK-Anlage bereitgestellten Leistungsmerkmale verwendet werden sollen.

Zuständigkeiten

Da bei der Nutzung von TK-Anlagen eine Vielzahl von Komponenten benötigt werden, ist zu klären, welche Organisationseinheiten für welche Aufgaben zuständig sind, also beispielsweise, wer sich um Beschaffung und Einrichtung von Hardware, Softwareupdates, Benutzerkennungen oder Benutzerbetreuung kümmert. Es ist auch zu klären, ob eventuell eine Betreuung durch einen externen Support erfolgen soll.

Berechtigungskonzept

Aufgrund der ausgewählten Leistungsmerkmale sollten in einem Rollenkonzept die Berechtigungen zur Nutzung festgelegt werden wie beispielsweise:

- Wer darf welche Funktionen und Kommunikationsdienste nutzen?
- Wer entscheidet darüber, wie der in der TK-Anlage integrierte Anrufbeantworter besprochen wird und wer darf wann welche Aufnahmen löschen?
- Wer kümmert sich um eine musikalische Ansage in der Warteschleife oder um die automatische Weiterleitung?
- Werden die Endgeräte zentral durch einen Administrator konfiguriert oder erhält jeder Benutzer eigene Berechtigungen?

Administration und Konfiguration

Die mit dem Berechtigungskonzept gestarteten Überlegungen zur Konfiguration und Administration der TK-Anlage müssen verfeinert werden. Es muss überlegt werden, wie das System administriert werden soll und welche Einstellungen über ein zentrales Administrations- und Konfigurationsmanagement und welche lokal an den Endgeräten vorgenommen werden. Zentrale Aufgaben wären beispielsweise das Anbinden zusätzlicher Gerätetypen, die Einrichtung von Notruf- und Sondernummern sowie die Adressbuchverwaltung beziehungsweise die Anbindung von Verzeichnisdiensten wie LDAP. An den Endgeräten könnten lokal Klingeltöne, Tastensperren, die Belegung von Funktionstasten oder private Telefonbücher eingestellt werden.

Zu klären ist weiterhin, wer für die Administration der TK-Anlage und ihrer Komponenten verantwortlich ist. Dazu gehören auch Aufgaben wie beispielsweise das Aufspielen von Patches oder Updates auf ein Teilsystem, die Einführung neuer Benutzergruppen, Änderungen der Rechte und in der Zusammensetzung von Benutzergruppen, die Aktivierung neuer Funktionen der TK-Anlage und Konfigurationsänderungen, die über eine einfache Benutzerverwaltung hinausgehen. Die TK-Anlage ist in das Patch- und Änderungsmanagement der Institution einzugliedern.

Änderungen an der Konfiguration der TK-Anlage sollten protokolliert werden, so das sie zu einem späteren Zeitpunkt nachvollziehbar sind.

Protokollierung

In der Planungsphase sollte entschieden werden, welche Informationen mindestens protokolliert und wie lange die Protokolldaten aufbewahrt werden sollen. Außerdem muss festgelegt werden, ob die Protokolldaten lokal in der Anlage oder auf einem zentralen Server im Netz gespeichert werden sollen. Auch bei einem IP-Anlagenanschluss muss eine Protokollierung möglich sein. Sinnvollerweise sollte bereits in der Planungsphase festgelegt werden, wie und zu welchen Zeitpunkten Daten ausgewertet werden. Hierbei ist zu prüfen, inwieweit das Datenschutzgesetz zu beachten ist und welche Konsequenzen daraus zu ziehen sind.

Eine TK-Anlage liefert im Allgemeinen Protokolldaten zu Zeiten und Rufnummern abgehender und ankommender Telefonate. Mit diesen Daten können beispielsweise Telefonate an Kostenstellen verrechnet werden. Die Daten können mithilfe entsprechender Software gesichert werden.

Datensicherung

Die Konfigurationen, die aktuellen Versionen der verwendeten Programme und die Protokolldaten der TK-Anlage und deren Komponenten sollten regelmäßig gesichert werden, um bei Ausfällen in kurzer Zeit ein Ersatzsystem bereitstellen zu können. Sicherungszeitpunkte und -formen sollten festgelegt werden, um den Anforderungen an den maximal tolerablen Datenverlust gerecht zu werden. Die entsprechenden Festlegungen sind in einen Gesamt-Datensicherungsplan des zentralen IT-Bereichs aufzunehmen.

Notfallvorsorge

Um schnell und effektiv auf Probleme zu reagieren, müssen die organisatorischen Rahmenbedingungen geschaffen werden, um in Notfällen schnell auf alternative Kommunikationskanäle umschalten oder Notrufe absetzen zu können. Dabei ist auch auf die Schulung aller Mitarbeiter zu achten. Sie müssen für mögliche Gefährdungen der TK-Anlage sensibilisiert, auf mögliche Warnanzeigen, -symbole und -töne hingewiesen und in die Bedienung der entsprechenden Kommunikationsdienste eingewiesen werden. Nicht nur für die Geschäftsprozesse ist die Verfügbarkeit der Telekommunikation eine wichtige Voraussetzung. Daher müssen entsprechende Vorkehrungen getroffen werden.

Die Planung muss der Leitungsebene zur Entscheidung vorgelegt und alle Entscheidungen nachvollziehbar dokumentiert werden.

NET.4.1.M2 Auswahl von TK-Diensteanbietern [Leiter IT]

Um mit Personen telefonieren zu können, die nicht an der institutionseigenen TK-Anlage angeschlossen sind (beispielsweise Endgeräte in anderen Standorten der Institution, Mobiltelefone und externe Gesprächspartner), muss die TK-Anlage über eine Teilnehmeranschlussleitung (TAL, auch "letzte Meile") an das PSTN (Public Switched Telephone Network) angeschlossen werden. Hierfür muss ein TK-Diensteanbieter ("Service Provider") beauftragt werden.

Der TK-Diensteanbieter stellt die physische Verbindung zwischen der TK-Anlage der Institution und dem PSTN bereit und regelt auch den Anschluss an das PSTN. Eine Ausnahme bilden IP-Anlagenanschlüsse, bei denen ausschließlich Internetverbindungen genutzt werden und der Anschluss an das PSTN komplett beim TK-Diensteanbieter liegt. Da die externen TK-Verbindungen über den TK-Diensteanbieter übermittelt werden, ist die Auswahl des Anbieters, der bereitgestellten Dienste und die Anzahl der gleichzeitig nutzbaren Verbindungen wichtig.

Für die Auswahl können folgende Anforderungen berücksichtigt werden:

- Anschlussart
  Soll die TK-Anlage mit einem oder mehreren ISDN-Basisanschlüssen oder S2m-Primärmultiplexanschlüssen an das PSTN angeschlossen werden? Ist ein IP-Anlagenanschluss möglich?
- Standortvernetzung
  Wie werden die TK-Anlagen unterschiedlicher Standorte verbunden?
- Referenzinstallationen bzw. -kunden
  Hat der TK-Diensteanbieter Erfahrungen mit Institutionen, deren Anforderungen sich mit den eigenen Anforderungen decken?
- Größe und Qualität des Serviceteams
  Wie schnell können die Techniker vor Ort sein? Welche Reaktionszeit garantiert der Anbieter?
- Hardware
  Wird zusätzliche Hardware beim Kunden benötigt? Kann diese gekauft oder gemietet werden? Welche Outsourcing- und Service-Verträge gibt es?
- Kapazität
  Kann der Anbieter nachweislich die geforderte Anzahl an ausgehenden Leitungen bereitstellen?
- Redundante Leitungen
  Kann die TK-Anlage für einen hohen Schutzbedarf bezüglich der Verfügbarkeit redundant über mehrere physisch unabhängige Leitungen und Trassen an das PSTN angebunden werden?

Neben den Sicherheitsaspekten sollten auch vertragliche und finanzielle Aspekte berücksichtigt werden:

- Vertragliche Bindung an den Anbieter
  Wie lange ist der Kunde an den Anbieter gebunden? Wie lange sind die Kündigungsfristen? Kann zu einem späteren Zeitpunkt problemlos zu einem anderen Anbieter gewechselt werden?
- Flexibilität und Bereitschaft
  Hat der TK-Diensteanbieter in der Vergangenheit regelmäßig neue Produkte, Serviceideen und Tarife eingeführt? Wird dem Kunden ermöglicht, einzelne Produkte oder Dienste nacheinander einzuführen?
- Tarifmodelle
  Gibt es Tarifmodelle die dem Nutzungsverhalten der Institution entgegenkommen, wie beispielsweise Festpreise ("Flatrate") oder gestaffelte Preise? Gibt es spezielle Tarifoptionen für günstige Auslandsgespräche, wenn oft mit Gesprächspartnern im Ausland telefoniert werden soll? Mit welcher Taktung werden die Gespräche abgerechnet (sekunden- oder minutengenau)?

Alle vereinbarten Leistungen müssen genau und eindeutig schriftlich festgehalten werden.

NET.4.1.M3 Änderung voreingestellter Passwörter

Viele IT-Systeme, TK-Anlagen und Netzkoppelelemente (beispielsweise ISDN-Router, Sprach-Daten-Multiplexer etc.) besitzen nach der Auslieferung durch den Hersteller noch voreingestellte Standardpasswörter. Von Herstellern oder Administratoren voreingestellte Passwörter sind direkt nach der Installation, spätestens bei erstmaliger Inbetriebnahme von Hard- oder Software zu ändern. Hierbei sind die einschlägigen Regeln für Passwörter zu beachten.

Bei einigen TK-Anlagen werden vorgenommene Änderungen der Konfiguration nur im RAM abgelegt. Dies gilt auch für Passwortänderungen. Daher ist nach einer solchen Operation stets eine Datensicherung vorzunehmen und eine neue Sicherungskopie zu erstellen. Unterbleibt dies, so ist nach einem "Restart" der Anlage wieder das Standardpasswort gültig. Weiterhin sollte überprüft werden, ob nach Einrichten eines neuen Passworts das Standardpasswort tatsächlich seine Gültigkeit verloren hat und nicht weiterhin für den Systemzugang genutzt werden kann.

NET.4.1.M4 Absicherung von Remote-Zugängen

TK-Anlagen verfügen oft über Fernwartungszugänge für Managementfunktionen. Diese Zugänge können für Administrations- und Wartungstätigkeiten sowie für sonstige Management-Aufgaben, wie die Alarmsignalisierung und -bearbeitung, genutzt werden. Solche Remote-Zugänge sind besonders bei komplexen TK-Anlagen nützlich und teilweise unverzichtbar.

Oft kann der Remote-Zugang über folgende Techniken genutzt werden:

- Zugang über ein Daten-Netz
- Direkte Einwahl über Direct Inward System Access (DISA)
- Zugang über dedizierte Management-Ports per Modem

Die Benutzung von Remote-Zugängen sollte so weit wie möglich eingeschränkt werden. Des Weiterem sollten alle Zugriffe und alle Aktivitäten während einer Administrationssitzung protokolliert werden können.

Grundsätzlich lässt sich zwischen

- einem Remote-Zugang im eigenen -Anlagenverbund (interner Zugang) und
- einem Remote-Zugang aus anderen Netzen (externer Zugang)

unterscheiden.

Beim internen Remote-Zugang wird die Absicherung einer Fernwartung innerhalb eines TK-Anlagenverbundes betrachtet. Unter Anlagenverbund wird hierbei eine aus mehreren separaten Anlagenteilen bestehende Gesamtanlage verstanden, die über ein eigenes Leitungsnetz miteinander verbunden ist. Sollte diese Verbindung über öffentliche Vermittlungseinrichtungen geführt sein, so sind zusätzliche Maßnahmen zu realisieren.

Der wichtigste Aspekt bei der Absicherung des internen Remote-Zuganges ist es, Eindringversuche aus externen Netzen wirksam zu unterbinden und gegebenenfalls auch erkennen zu können. Des Weiteren sollten die Zugänge aus dem eigenen Netz auf die berechtigten Stellen und Personen eingeschränkt werden können. Je nach Art der Zugangstechnik existieren hierfür unterschiedliche Methoden.

Absicherung eines internen Remote-Zugangs über IP-Netze

Wird die TK-Anlagen an ein IP-Netz angeschlossen, zum Beispiel damit sie konfiguriert und überwacht werden kann, gelten für sie ähnliche Empfehlungen wie für klassische IT-Systeme, darunter Server und Clients. Analog zu diesen IT-Systemen ist die Fernwartung zu schützen.

Die TK-Anlage muss so konfiguriert werden, dass sich nur berechtigte Administratoren nach einer geeigneten Authentisierung an der TK-Anlage anmelden können. Hierfür ist ein entsprechendes Authentisierungsverfahren auszuwählen. Wenn möglich, sollte die TK-Anlage so konfiguriert werden, dass nur berechtige IT-Systeme auf sie zugreifen dürfen, beispielsweise durch ein getrenntes Konfigurationsnetz oder Paket-Filter.

Damit die übertragenen Informationen zwischen den IT-Systemen der Administratoren und der TK-Anlage nicht abgehört werden können, sollten die übertragenen Informationen verschlüsselt werden.

Im Weiterem muss geprüft werden, ob die TK-Anlage in das Sicherheitskonzept gegen Schadprogramme aufgenommen werden sollte.

Absicherung eines internen Remote-Zugangs via Modem

Die nachfolgende Abbildung stellt ein typisches Szenario eines internen Remote-Zugangs dar, der über einen Fernadministrationsport via Modem angesprochen wird. Die TK-Anlage PBX 1 wird vom Wartungsplatz aus direkt über die V.24-Wartungsschnittstelle administriert. Die TK-Anlage PBX 2 wird vom Wartungsplatz aus über Modem 1 - PBX 1 - PBX 2 - Modem 2 - V.24-Wartungsschnittstelle administriert.

In einem solchen Fall können folgende Maßnahmen zur **Abschottung gegenüber Zugängen aus externen Netzen** ergriffen werden:

- Keine Amtsberechtigung für den Anschluss von Modem 2
  Der Modem-Anschluss, über den der Zugang zum Administrationsport der Anlage geführt wird, sollte in keinem Fall amtsberechtigt sein! Diese Minimalanforderung sollte als erstes überprüft werden. Hiermit wird vermieden, dass das Modem von außerhalb direkt angewählt werden kann.
- Geheimhaltung der Rufnummer des Wartungsports von Modem 2
  Um Missbrauch von vornherein zu erschweren, sollte die Rufnummer des Wartungsapparates nicht in Telefonverzeichnissen veröffentlicht werden. Ihre Kenntnis sollte den sie unmittelbar benötigenden Personen vorbehalten bleiben.
- Verwendung von Standleitungen (optional)
  Die Verwendung von eigenen, nicht über Vermittlungseinrichtungen geführten, Standleitungen für die Remote-Verbindungen, ist eine der sichersten Methoden, um den externen Zugriff auf die Remote-Zugänge zu unterbinden. Da dieses Verfahren in der Regel sehr teuer ist, wird es nur in Ausnahmefällen Anwendung finden können.

Um sicherzustellen, dass nur **die berechtigten Stellen** innerhalb des eigenen Netzes auf die Remote-Zugänge zugreifen können, müssen folgende Maßnahmen umgesetzt werden:

- Bildung geschlossener Benutzergruppen (Closed User Group, CUG)
  In einigen TK-Anlagen lassen sich CUGs anlagenübergreifend einrichten. Diese geschlossenen Benutzergruppen stellen eine Art Netz im Netz dar. Alle benötigten Remote-Zugänge sollten daher mit den jeweils zugangsberechtigten Stellen in solchen CUGs zusammengefasst werden.
- Automatischer Rückruf (Callback)
  Die Callback-Option der Modems sollte genutzt werden. Wird ein -Gateway eingesetzt, so sollte das Callback von dort gestartet werden.
- Beschränkung der Rechte des Remote-Ports (optional)
  Sollte die TK-Anlage eine Rechteverwaltung für verschiedene Ports unterstützen, kann diese genutzt werden, um sicherheitskritische Aktionen über Remote-Zugänge zu unterbinden und nur vor Ort zuzulassen. Viele TK-Anlagen besitzen diese Option jedoch nicht. In solchen Fällen können die über einen Port ausführbaren Transaktionen durch Zusatzprodukte wie Portcontroller beschränkt werden.

Um sicherzustellen, dass **nur die berechtigten Personen** innerhalb des eigenen Netzes auf die Remote-Zugänge zugreifen können, müssen folgende Maßnahmen umgesetzt werden:

- Identifikation und Authentisierung,
- Challenge-Response-Verfahren zur Authentisierung (optional).

Absicherung eines internen Remote-Zugriffes via ISDN-Vernetzung

Der Remote-Zugriff auf eine TK-Anlage kann auch über erfolgen. Zu diesem Zweck sind die PCs mit Managementaufgaben mit ISDN-Karten auszurüsten. Um den Zugang abzusichern, sollte eine geschlossene Benutzergruppe durch die Auswertung der Rufnummer des Management-PCs gebildet werden (CLIP: Calling Line Identification and Presentation). In vielen TK-Anlagen ist diese Beschränkung des Remote-Zugangs auf eine Telefonnummer eingebaut.

Absicherung direkter Systemzugänge (Direct Inward System Access, DISA)

Direkte Systemzugänge sollten nach Möglichkeit gesperrt werden. Ist dies nicht möglich, so sollten die Berechtigungen so gesetzt werden, dass der direkte Systemzugang nur über einen dedizierten Port erfolgen kann. Auf diese Weise wird es möglich, den DISA-Zugang über ein Gateway zu führen.

Einrichtung und Unterbringung eines Netzmanagement-Zentrums

Der Vorteil eines zentralen Netzmanagements ist, neben einer komfortablen Abwicklungsmöglichkeit der Systemadministration, dass für die alltäglichen Administrationsarbeiten kein physischer Zutritt zu den TK-Anlagen mehr notwendig ist.

Sollte die Einrichtung eines zentralen Netzmanagements erwogen werden, so ist dies in einem gesicherten Bereich unterzubringen. Der Zutritt zu diesem Zentrum ist durch organisatorische Maßnahmen zu regeln. Die Managementrechner, von welchem die Arbeiten durchgeführt werden können, sollten auch mit geeigneten Maßnahmen abgesichert werden.

Als externer Remote-Zugang wird in dieser Maßnahme jeder Zugriff über die Wartungsschnittstelle der Anlage via öffentliche Vermittlungssysteme und Datennetze, wie dem Internet, angesehen. Dies kann entweder dadurch notwendig werden, weil die einzelnen Anlagen des Verbundes nicht oder nicht nur (siehe Anmerkung 1) über Standleitungen verbunden sind oder weil auf eine schnelle Unterstützung des Herstellers in Notfällen nicht verzichtet werden kann. In diesen Fällen muss der Wartungsport (Modem) die volle Amtsberechtigung besitzen.

Moderne TK-Anlagen können oft über Datennetze konfiguriert werden. Je nach Netzstruktur befindet sich die TK-Anlage in einem oder in einem separaten Management-Netz. Der direkte Zugriff auf die TK-Anlage, die sich in internen Netzen befindet, von öffentlichen Netzen aus muss verhindert werden. Soll dennoch von einem öffentlichen Datennetz auf die TK-Anlage zugegriffen werden, sollte ein Virtuelles Privates Netz (VPN) genutzt werden. Hierbei wird eine geschützte Datenverbindung zu dem VPN-Endpunkt, der sich in der Regel in der demilitarisierte Zone (DMZ) befindet, generiert. Von dort kann eine Verbindung unter Berücksichtigung der entsprechenden Sicherheits-Empfehlungen aufgebaut werden.

Die nachfolgende Abbildung stellt ein typisches Szenario eines externen Remote-Zugangs zu einem Fernadministrationsport via Modem dar. Die TK-Anlage wird vom externen Wartungsplatz aus über Modem 1 - öffentliches Netz - PBX - Modem 2 - V.24-Wartungsschnittstelle administriert.

Aus Sicherheitsgründen ist es sinnvoll, auf externe Fernwartung zu verzichten. Ist dies nicht möglich, so sind, neben den Maßnahmen für interne Remote Zugänge, zusätzliche Sicherungsmaßnahmen unumgänglich.

Anmerkung 1: Einige Anlagen bieten die Möglichkeit, nur die Grundverkehrslast über Standleitungen abzuwickeln und Lastspitzen automatisch über das öffentliche Netz zu routen. Dieser Vorgang wird dem Benutzer nicht signalisiert.

PC-Gateway (siehe Anmerkung 2)

Zwischen Wartungsport und Modem sollte ein Gateway geschaltet werden. Dieser muss die folgenden Sicherheitsfunktionen realisieren:

- Identifikation und Authentisierung des Bedieners,
- Abbruch der Verbindung bei sicherheitskritischen Ereignissen,
- Automatischer Rückruf (call back) und
- Protokollierung aller Tätigkeiten.

Darüber hinaus können noch weitere Funktionalitäten implementiert werden:

- Verhängen einer Zeitsperre bei fehlerhaften Zugangsversuchen,
- Sperren der Fernwartung im Normalbetrieb und explizite Freigabe für eine genau definierte Zeitspanne; dies ist sinnvoll, um in Notfall dem Hersteller oder einem anderen Wartungsunternehmen einen Eingriff zu ermöglichen,
- Einschränkung der Rechte des Wartungspersonals; über eine auf dem Wartungs-PC installierte Zusatzsoftware kann der Benutzer in seinem Handlungsspielraum eingeengt werden, um eine abgestufte Rechteverwaltung zu realisieren,
- "Zwangslogout" bei Leitungsunterbrechung: wird die Verbindung zwischen Fernwartungsstelle und PC-Gateway auf irgendeine Weise unterbrochen, so muss der Zugriff auf das System durch ein "Zwangslogout" beendet werden.

Physikalische Abschaltung des Fernwartungszuganges

Sollte im Normalfall keine Fernwartung benötigt und nur im Bedarfsfall eine solche ermöglicht werden, so empfiehlt sich die physikalische Abschaltung des Zugangs. Im Bedarfsfall kann dieser, eventuell nach telefonischer Rücksprache mit dem Hersteller oder der Wartungsfirma, kurzfristig aktiviert werden.

Geschlossene Benutzergruppen (Closed User Group, CUG)

In öffentlichen ISDN- und X.25-Netzen wird das Leistungsmerkmal der Bildung von CUG angeboten. Auf diese Weise wird für einen Benutzer vom Netzbetreiber ein virtuelles "Netz-im-Netz" zur Verfügung gestellt. Die geschlossenen Benutzergruppen können beim Netzbetreiber gegen entsprechende Entgelte beantragt werden.

Alternativ kann überlegt werden, die geschlossenen Benutzergruppen durch Nutzung der ISDN-Hilfsdienste Calling Line Identification and Presentation (CLIP) und Connected Line Identification and Presentation (COLP) selbst zu realisieren. Dies kann, wenn möglich, durch entsprechende Konfiguration der eigenen TK-Anlage oder aber durch entsprechende Auslegung eines PC-Gateways geschehen.

Anmerkung 2: Diese Maßnahme sollte auch bei interner Fernwartung über virtuelle private Netze angewandt werden.

Vermeidung bzw. Kontrolle direkter Einwahlmöglichkeiten (Dial-In)

Eine direkte Einwahlmöglichkeit, z. B. aus anderen Netzen über Nachwahl im Mehrfrequenzwahlverfahren, in die TK-Anlage sollte nach Möglichkeit unterbunden werden. Solche Verfahren werden oft für den Zugang zu Serverdiensten genutzt. Sollte ein Unterbinden aus betrieblichen Gründen nicht vermeidbar sein, so empfiehlt sich das vollständige Aktivieren der möglichen Schutzmechanismen und eine regelmäßige Kontrolle auf möglichen Missbrauch.

NET.4.1.M5 Protokollierung bei TK-Anlagen

TK-Anlagen bieten in der Regel Möglichkeiten zur Protokollierung. Beispielsweise kann protokolliert werden, wer Dienste wie Telefon, Fax oder Datenübertragung nutzt und mit wem kommuniziert wird. Diese Informationen können erfasst, verarbeitet und gespeichert werden. Oft werden die Daten zu Abrechnungs- und Nachweiszwecken benutzt. Die protokollierten Informationen enthalten unter Anderem Einträge über:

- Zeit und Datum eines Gespräches oder einer Verbindung,
- Quell- und Zielrufnummer sowie die
- Gesprächsdauer.

Die Daten können mit der integrierten Verbindungsdatenerfassung intern ausgewertet oder auf entsprechende externe Systeme übertragen werden.

Da es sich um vertrauliche Daten handelt, müssen die Informationen auf allen Systemen und zusätzlich bei der Übermittlung geschützt werden. Es müssen entsprechende Vorkehrungen zum Schutz der Vertraulichkeit und Integrität getroffen werden. Beispielsweise könnten die Informationen über eine dedizierte Netzverbindung oder verschlüsselt über das übertragen werden. Zusätzlich ist sicherzustellen, dass nur Berechtigte auf die gesicherten Daten zugreifen können. Es ist zu dokumentieren, welche Personen in welchen Rollen Zugriff auf die Verbindungsdaten haben.

Protokolliert werden sollten zusätzlich alle systemtechnischen Eingriffe, die Programmveränderungen beinhalten sowie Auswertungsläufe, Datenübermittlungen und Datenzugriffe.

Administrationsarbeiten

Alle Administrationsarbeiten an der TK-Anlage sollten protokolliert werden, um nachvollziehbar zu machen, von wem und auf welche Weise Einstellungen verändert wurden. Dazu ist es sinnvoll, dass bei der Authentisierung die Benutzer-Kennung, das Datum und die Uhrzeit sowie die erfolgte Anmeldung protokolliert werden. Bei einem erfolgten Zugriff sollten neben den schon bei der Authentisierung protokollierten Daten zusätzlich die Art des Zugriffs (lesend, schreibend) sowie durchgeführte Administrationstätigkeiten aufgezeichnet werden. Die Protokollierung muss übersichtlich, vollständig und korrekt sein.

Die Protokollierungsfunktion darf von Unbefugten nicht deaktiviert und nachträglich verändert werden können. Auch sollte ausgeschlossen sein, dass die Protokolldaten verändert werden können.

Die protokollierten Informationen sind regelmäßig zu kontrollieren. Gehäufte fehlerhafte Anmeldeversuche sollten gezielt untersucht werden. Bestehen auch bei erfolgreichen Anmeldungen Zweifel, sollten diese mit der Dokumentation durchgeführter Konfigurations- und Wartungsmaßnahmen verglichen werden. Bei Auffälligkeiten muss sofort entsprechend den für die bestehenden Regelungen für einen vermuteten Sicherheitsvorfall verfahren werden, bis ein Angriffsverdacht schlüssig widerlegt ist.

Da die Protokolldateien in den meisten Fällen personenbezogene Daten beinhalten, ist sicherzustellen, dass diese Daten nur zum Zweck der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes verwendet werden. Der Umfang der Protokollierung und die Kriterien für deren Auswertung sollte dokumentiert und innerhalb der Institution abgestimmt werden. Gegebenenfalls sollten frühzeitig die jeweiligen Mitbestimmungsgremien beteiligt werden.

Gemeinsam mit den Basismaßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik für TK-Anlagen.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "TK-Anlagen".

NET.4.1.M6 Erstellung einer Sicherheitsrichtlinie für TK-Anlagen [Leiter IT]

Die Sicherheitsvorgaben für die TK-Anlage der Institution ergeben sich aus der institutionsweiten Sicherheitsrichtlinie. Ausgehend von dieser allgemeinen Richtlinie müssen die Anforderungen konkretisiert und in einer Sicherheitsrichtlinie für die TK-Anlage zusammengefasst werden. In diesem Zusammenhang ist zu prüfen, ob neben der institutionsweiten Sicherheitsleitlinie weitere übergeordnete Vorgaben wie IT-Richtlinien, Passwortrichtlinien oder Vorgaben wie beispielsweise zur Nutzung von VoIP (Voice over IP) zu berücksichtigen sind.

Die Sicherheitsrichtlinie sollte grundlegende Aussagen zur Verfügbarkeit der TK-Anlage sowie zur Vertraulichkeit und Integrität der gespeicherten oder verarbeiteten Daten treffen. Dabei ist zu beachten, dass für Kommunikationsdienste grundsätzlich hohe Erwartungen an die Verfügbarkeit und auch in die Vertraulichkeit gesetzt werden. Bei der Speicherung von personenbezogenen Daten müssen auch Aspekte wie Datenschutz und Aufbewahrungspflichten für Daten berücksichtigt werden. Letztere dienen als Basis für Sicherheitsanalysen im Verdachts- oder Revisionsfall.

Die Sicherheitsrichtlinie für TK-Anlagen muss allen Personen und Gruppen, die an der Beschaffung, dem Aufbau, der Umsetzung und dem Betrieb der TK-Anlage beteiligt sind, bekannt sein und die Grundlage für deren Arbeit darstellen. Wie bei allen Richtlinien sind ihre Inhalte und ihre Umsetzung im Rahmen einer übergeordneten Revision regelmäßig zu prüfen.

Im Rahmen der Sicherheitsrichtlinie für TK-Anlagen sollten die Benutzer in kurzer, verständlicher Form über die Gefährdungen informiert werden, die mit der Nutzung einer TK-Anlage und ihrer Kommunikationsdienste verbunden sind. Dabei sollten auch immer aktuelle Entwicklungen im Bereich der Technik und neu bekannt gewordenen Gefahren berücksichtigt werden. Diese Informationen sollen die Benutzer sensibilisieren und motivieren, diese Richtlinie auch einzuhalten.

Neben den Leistungsmerkmalen einer klassischen TK-Anlage, wie beispielsweise Makeln, Rückfrage, Rückruf bei Besetzt, Anklopfen und auch Aufschalten auf ein bestehendes Gespräch, Konferenzschaltung und Heranholen eines Gespräches, verfügen Hybrid-Anlagen und VoIP-Anlagen durch die Kopplung von Eigenschaften der klassischen TK-Anlage und von IT-Systemen zusätzlich über eine Vielzahl von weiteren IT-basierten Funktionen. Beispielsweise können Sprachnachrichten und Faxe über E-Mail übertragen, Anrufe per Mausklick von einer Anwendung am PC initiiert und vermittelt und die aktuelle Verfügbarkeit eines Teilnehmers angezeigt werden. In der Richtlinie sollte daher festgelegt werden, welche Funktionen und Leistungsmerkmale der TK-Anlage genutzt werden sollen. Zusätzlich muss festgelegt werden, wer für welche Zwecke welche Dienste benutzen darf. In diesem Zusammenhang ist ebenfalls der Umfang der privaten Nutzung festzulegen.

Weiterhin müssen Sicherheitsmaßnahmen beachtet werden, welche die Auswahl und Installation der erforderlichen Sicherheitshard- und -software sowie Vorgaben für die sichere Konfiguration der TK-Anlage und ihrer Endgeräte regeln. Bei Nutzung einer Hybrid-Anlage oder eines VoIP-Systems sind dies zusätzlich die für diese Systeme geltenden Richtlinien. In einigen Fällen kann es zweckmäßig sein, dass Benutzer bestimmte Konfigurationseinstellungen, wie beispielsweise das Sperren des Telefonendgeräts bei Abwesenheit, direkt am Endgerät selbst vornehmen dürfen. Dies sollte in den Richtlinien vermerkt, anderenfalls untersagt werden.

Sinnvoll ist es weiterhin, beispielsweise folgende Punkte in die Richtlinien mit aufzunehmen:

- Regelungen zur physikalischen Zugriffskontrolle:
  Eine TK-Anlage sollte grundsätzlich in einem separaten Sicherheitsbereich, wie zum Beispiel in einem abschließbaren Rechnerraum aufgestellt werden. Dabei ist zu regeln, wer Zutritt zu dem Raum beziehungsweise Zugriff auf die Anlage selbst erhalten soll. Der Zugang zur Administration, der in der Regel über eine Administrations-Software aber auch über separate Endgeräte erfolgen kann, sollte auf das TK-Betriebspersonal beschränkt sein.
- Regelungen für die Arbeit der Administratoren:
  Festzulegen ist, nach welchem Schema die Administrationsrechte vergeben werden. Es ist dabei zu überlegen, ob die Aufgabenbereiche des Administrators für die IT-Systeme von denen des Verantwortlichen für die TK-Anlage getrennt werden. Es ist darzulegen, welcher Administrator welche Rechte ausüben darf und wie er diese Rechte erlangt. In einem weiteren Schritt müssen die Zugangswege bestimmt werden, über die die Administratoren auf die Systeme zugreifen. Denkbar ist der lokale Zugriff an der TK-Anlage selbst, über ein eigenes Administrationsnetz oder über die Fernwartungsschnittstelle.

Zusätzlich muss geregelt werden, welche Vorgänge dokumentiert werden müssen und in welcher Form die Dokumentation erstellt und gepflegt wird. Dazu gehören die folgenden Vorgaben für die Installation und Konfiguration:

- Vorgehen bei der Installation der gesamten TK-Anlage und der Endgeräte,
- Überprüfung und gegebenenfalls Änderung der Default-Einstellungen hinsichtlich ihrer Sicherheitsgefährdungen sowie die Änderung der Standard-Passwörter,
- Verwendung und Konfiguration der TK-Anlage und Endgeräte,
- Dokumentation und Sicherung der Konfiguration.

Es sollten Vorgaben für den sicheren Betrieb gemacht werden, wie beispielsweise:

- Absicherung der Administration (Technische Beschränkung des Zugangs zur Administration auf das TK-Betriebspersonal),
- Logging aller Anmeldeversuche an der TK-Anlage, Protokollierung und regelmäßige Kontrolle von Fernwartungszugriffen,
- erlaubte Werkzeuge für Betrieb und Wartung,
- Abschaltung sonstiger, nicht zur Verwendung vorgesehener Zugriffsmöglichkeiten,
- Vergabe von Berechtigungen,
- Vorgehensweisen bei Software-Updates und Konfigurationsänderungen,
- Datensicherung und Wiederherstellung sowie
- Regelungen für die Reaktion auf Betriebsstörungen, technische Fehler (lokaler Support, Fernwartung) und Sicherheitsvorfälle.

Auch auf die sichere Entsorgung der Komponenten der TK-Anlage sollte in der Sicherheitsrichtlinie hingewiesen werden. So werden zum Teil Verbindungsdaten und andere personenbezogene Daten auf Datenträgern in der TK-Anlage gespeichert. Endgeräte sind häufig von außen mit Namen auf Schnellwahltasten, IP-Adressen, Telefonnummern oder sonstigen technischen Informationen beschriftet. Die einzelnen Komponenten müssen so vernichtet werden, dass eine Rekonstruktion der Daten nicht möglich ist.

Die Verantwortung für die Umsetzung der Sicherheitsrichtlinie für TK-Anlagen liegt beim IT-Betrieb, Änderungen und Abweichungen hiervon dürfen nur in Abstimmung mit dem Informationssicherheitsbeauftragten (ISB) erfolgen.

NET.4.1.M7 Aufstellung der TK-Anlage

Ideal ist eine Aufstellung in einem räumlich separaten Sicherheitsbereich. Die Anforderungen eines erhöhten Zutrittsschutzes lassen sich auf dieser Basis mit minimalem Zusatzaufwand realisieren.

Darüber hinaus ist eine Aufstellung in einer Umgebung wichtig, die durch entsprechende Vorkehrungen den erhöhten Anforderungen an Verfügbarkeit besonders genügt. Dies betrifft die folgenden Infrastrukturaspekte:

- Stromversorgung / Überspannungsschutz
- Klimatisierung / Schutz vor Wasserschäden
- Brandschutz
- Verwendung von Sicherheitstüren und Fenstern
- Einbindung des Raums in eine vorhandene Gefahrenmeldeanlage

Am Aufstellungsort der TK-Anlage sind mindestens dieselben Vorkehrungen zu treffen, die am selben Standort für kritische IT-Systeme realisiert sind (Unterbrechungsfreie Stromversorgung (USV), Klimatisierung, Brandschutz usw.). Jedoch ist eine gemeinsame Nutzung derselben Versorgungslösungen durch die TK-Anlage und durch andere IT-Systeme kritisch zu prüfen (z. B. ggf. zwingende separate USV für die TK-Anlage).

Als Basis für die Einleitung und Koordination notwendiger Maßnahmen kommt gerade bei Großstörungen bzw. in Notfallsituationen einer möglichst unterbrechungsfreien Verfügbarkeit der Telefonie und damit auch der zentralen TK-Anlage besondere Bedeutung zu.

Diesem Umstand sollte durch die genannten Maßnahmen gezielt Rechnung getragen werden. In notfallbedingten Engpass-Situationen ist es außerdem empfehlenswert, der Versorgung der TK-Anlage nochmals erhöhte Priorität einzuräumen (Wiederanlaufreihenfolge bzw. Maßnahmenpriorisierung in Notfällen).

Die Schnittstellen einer TK-Anlage, über die Administrationstätigkeiten ausgeführt werden können, stellen schützenswerte Punkte dar. Sie sollten daher besonders abgesichert werden. Über unbenutzte oder ungesicherte Schnittstellen können von Unbefugten, etwa unter Zuhilfenahme eines Laptops, Manipulationen am System durchgeführt werden. Der Passwortschutz auf einen TK-Bedienplatz oder PC-Gateway wäre in einem solchen Fall wirkungslos. Ziel ist es also, dies zu verhindern, zumindest aber den Versuch erkennbar zu machen. Aus diesem Grund sollten die benutzten Schnittstellen gut verschraubt und ggf. zusätzlich verplombt werden. Unbenutzte Schnittstellen können durch verschraubte und verplombte Abschlusskappen gesichert werden.

NET.4.1.M8 Einschränkung und Sperrung nicht benötigter oder sicherheitskritischer Leistungsmerkmale.

Soweit Leistungsmerkmale nicht benötigt werden bzw. bewusst nicht verwendet werden sollen, sind diese zu sperren. Auf diese Weise wird verhindert, dass die Anlage über solche Merkmale unnötig möglichen Angriffen ausgesetzt wird.

Bestimmte (ISDN-)Leistungsmerkmale können zu gezielten Angriffen, insbesondere auf Vertraulichkeit oder Verfügbarkeit, missbraucht werden. Neben der Gefährdung dieser Sicherheitsgrundwerte können im Zuge eines derartigen Missbrauchs außerdem (vom Anlagenbesitzer ungewollte) Anrufgebühren generiert werden. Merkmale mit Missbrauchspotenzial sind vor allem:

- Direktes Ansprechen bzw. automatische Rufannahme ist in Verbindung mit Freisprechfunktionalität des Telefons zum Abhören des Raums missbrauchbar.
- Der Amtszugang birgt bei leicht zugänglichen Apparaten die Gefahr der Nutzung durch Unbefugte für Amtsgespräche mit resultierendem Mehraufkommen an Anrufgebühren.
- Bei einer Rufumleitung kann z. B. durch versehentliche oder böswillige Fehlnutzung die Nichterreichbarkeit des Nutzers eines Telefonanschlusses die Folge sein.
- Dial-In-Möglichkeiten sollten im Endteilnehmer-Umfeld grundsätzlich abgeschaltet werden, da die Nutzung hier nur missbräuchlichen Hintergrund haben kann.
- Export-Merkmale sind zu Angriffen auf die Vertraulichkeit nutzbar (z. B. "Zeugenschaltung" oder "Abhören").

Für offen zugängliche Geräte sollten derartige Merkmale bei erhöhtem Schutzbedarf in jedem Fall zwingend gesperrt werden. Bei gesichert aufgestellten Endgeräten sollten mindestens die Merkmale, deren Sperrung Angriffe von außen abwehrt (vor allem direktes Ansprechen, automatische Rufannahme, Dial-In), so behandelt werden.

Sofern Endgeräte mit geeigneter Sicherheitsintelligenz eingesetzt werden, kann in Abhängigkeit von der konkreten Risikobewertung entschieden werden, solche Merkmale vollständig zu deaktivieren oder diese bis zu einer erfolgreichen Authentisierung zu sperren. Auch sollten bei entsprechend intelligenten Endgeräte diese im Rahmen der produkttechnisch gegebenen Möglichkeiten gezielt so zu konfiguriert werden, sodass diese warnen, wenn sicherheitskritische Merkmale genutzt werden.

Nicht benötigten bzw. wegen ihres Missbrauchspotenzials als kritisch eingestuften und daher zur Abschaltung vorgesehenen Leistungsmerkmalen sollten zentral abgeschaltet werden. Bietet die zentrale Anlage nur eingeschränkte bzw. nicht ausreichend differenzierte Möglichkeiten, so kann eine Sicherheitskonzeption Konfigurationsvorgaben für die zentrale Angabe gezielt mit entsprechenden Sperreinstellungen auf den Endgeräten kombinieren. Voraussetzung für die Maßnahmenumsetzung ist in einem solchen Fall, dass ausreichend sicherheitsintelligenter Endgeräte gezielt beschafft werden

NET.4.1.M9 Schulung zur sicheren Nutzung an TK-Anlagen [Leiter IT, Leiter Personal]

Für die korrekte und ihrer Bestimmung entsprechende Verwendung von Diensten und Geräten im Umfeld einer TK-Anlage sollten die Benutzer unterwiesen werden. Zusätzlich sollten den Benutzern der TK-Anlage alle notwendigen Unterlagen zur Bedienung der entsprechenden Endgeräte, wie die Bedienungsanleitung für die Telefone, zur Verfügung gestellt werden. Mangelnde Sicherheit bei der Bedienung kann die Vertraulichkeit und die Integrität gefährden, aber auch dazu führen, dass nicht alle gegebenen Möglichkeiten bekannt sind und die Anlage nicht wie geplant genutzt wird. In diesem Zusammenhang ist es vorteilhaft, auch Ansprechpartner und Verantwortliche zu nennen. Generell ist darauf hinzuweisen, dass die Richtlinien und Regelungen zur Nutzung von TK-Anlagen eingehalten werden.

Zusätzlich ist es für alle Benutzer einer (klassischen) TK-Anlage wichtig, die Bedeutung der üblichen Warnanzeigen, -töne und -symbole der TK-Anlage zu kennen. Zu diesen zählen insbesondere:

- Aufmerksamkeitston für direktes Ansprechen,
- Aufschalte-Warnton,
- Freisprechanzeige,
- Anzeige für aktiviertes direktes Ansprechen,
- Anzeige für automatischen Rückruf und
- Anzeige/Einblendung bei Dreierkonferenz.

Die Warnanzeigen sollen eindeutige Hinweise geben, sobald auf unsichere Merkmale der TK-Anlage zurückgegriffen wird. Die Nutzung bestimmter, eigentlich nicht freigegebener Leistungsmerkmale (Beispiel: Zeugenschaltung) kann zu Beeinträchtigungen der Informationssicherheit führen. Daher sollten besonders deren Warnanzeigen und -töne bekannt sein. Ein wichtiges Beispiel ist ein Warnsignal in dem Fall, dass gerade eine Aufschaltung durch einen Dritten auf ein zurzeit geführtes Telefonat erfolgt.

Jedes auffällige Verhalten der TK-Anlage sollte den entsprechenden Verantwortlichen gemeldet werden und wenn möglich bis zur Klärung alternative Kommunikationskanäle verwendet werden. Bei Manipulationen an der TK-Anlage ist der Informationssicherheitsbeauftrage oder der Datenschutzbeauftragte zu informieren.

Wichtig ist es, zusätzlich auf den Schutz der Endgeräte durch Passwörter oder PINs hinzuweisen, um zu verhindern, dass Unberechtigte auf vertrauliche, in den Endgeräten gespeicherte Informationen zugreifen können. Viele Endgeräte verfügen bereits über werksseitig eingestellte Standard-Passwörter, die bei der erstmaligen Inbetriebnahme durch den Benutzer geändert werden sollten.

Die Mitarbeiter sollten je nach Benutzergruppen unterschiedlich unterrichtet werden. Administratoren sollten Schulungen mit anderen Inhalten als die Benutzer erhalten. Bei allen kann die sichere Anwendung der geschulten Inhalte gezielt unterstützt werden. Dafür eignen sich unter anderem Einträge im Intranet, Informationsveranstaltungen, Handzettel zur Telefonnutzung für Anwender, Arbeitsanweisungen für das Wachpersonal oder Checklisten für Administratoren. Derartige Hilfsmittel sollten bereits zum Schulungszeitpunkt erstellt sein und gezielt mit einbezogen werden.

Neben klassischen Schulungen sind auch Schulungen mit Hilfe von webbasierten interaktiven Programmen im Intranet denkbar. Aktuelle Entwicklungen können auch mithilfe von Newslettern oder Rundbriefen und im Rahmen regelmäßiger Veranstaltungen wie Abteilungsbesprechungen kommuniziert werden.

NET.4.1.M10 Dokumentation und Revision der TK-Anlagenkonfiguration [Leiter IT]

Um die Sicherheit der TK-Anlagen zu gewährleisten, sind Revisionen der TK-Anlagenkonfiguration in regelmäßigen Abständen durchzuführen. Zur Revisionstätigkeit gehört speziell die Kontrolle der Tätigkeit der Systemverwaltung, des Wartungspersonals, des Ist-Zustands der TK-Anlage und der Einhaltung der datenschutzrechtlichen Vorschriften.

Jede Konfigurationsänderung, wie die Erteilung von Berechtigungen für einen Benutzer, sollte in eine Ist-Bestandsliste eingetragen werden. Diese Liste kann per Hand oder automatisiert geführt werden. In regelmäßigen Abständen, beispielsweise alle 6 Monate, sollte diese Ist-Bestandsliste zumindest stichprobenartig mit der Realität verglichen werden. Durch eine kontinuierliche Revision der Bestandsliste kann das angestrebte Sicherheits- und Datenschutzniveau sichergestellt werden. Werden Unstimmigkeiten festgestellt, sind diese mit Hilfe der Protokolle der TK-Anlage aufzuklären.

Es sollte beispielsweise kontrolliert werden, ob

- alle nicht vergebenen Rufnummern auch wirklich nicht eingerichtet sind,
- Rufnummern und Teilnehmer vollständig zugeordnet sind,
- verbotene Berechtigungen nirgendwo vergeben sind,
- deaktivierte Leistungsmerkmale und Kommunikationsschnittstellen sowie
- deaktivierte Dial-In-Funktionen auch wirklich inaktiv sind.

Ist es nicht gewünscht oder nicht möglich, die Rolle eines unabhängigen Revisors einzurichten, kann die Auswertung der Protokolldateien auch durch den Administrator erfolgen. Für diesen Fall bleibt zu beachten, dass damit eine Kontrolle der Tätigkeiten des Administrators selbst nur schwer möglich ist. Zudem kann der Administrator möglicherweise Einblick in geschützte Daten (Anrufprotokolle) erhalten. Das Ergebnis der Auswertung sollte daher zumindest dem Informationssicherheitsbeauftragten, dem IT-Verantwortlichen oder einem anderen, besonders zu bestimmenden Mitarbeiter vorgelegt werden.

NET.4.1.M11 Außerbetriebnahme von TK-Anlagen und -geräten [Leiter IT]

Auf einigen Komponenten von -Anlagen werden während des Betriebs vertrauliche Informationen gespeichert, zu denen personenbezogene Daten, wie beispielsweise Telefonbücher, Kontaktdaten sowie Verbindungsdaten zählen.

Bei WLAN-Komponenten gehören dazu insbesondere die Authentifizierungsinformationen für den Zugang zum WLAN. Auf VoIP-Komponenten können je nach Einsatzzweck eine Vielzahl verschiedener sensibler Informationen gespeichert sein. Dazu gehören beispielsweise IP-Adressen und weitere Informationen, die auf den Netzaufbau schließen lassen sowie institutionsweite Telefonverzeichnisse mit allen Mitarbeitern .

Lokal auf den verschiedenen Komponenten gespeicherten Daten, die noch benötigt werden, sollten entweder extern gesichert oder archiviert (beispielsweise auf Magnetbändern, CD- oder DVD-ROMs) oder auf ein Ersatzsystem übertragen werden.

Sollen Komponenten außer Betrieb genommen oder ersetzt werden, ist darauf zu achten, dass Datenträger wie Festplatten, auf denen personenbezogenen Daten gespeichert werden, sicher entsorgt werden. Dies gilt besonders dann, wenn die Komponenten ausgesondert und an Dritte weitergegeben (beispielsweise verkauft) werden. Auch wenn ein Gerät im Rahmen eines Garantieaustausches oder einer Reparatur an den Hersteller oder eine Service-Firma übergeben wird, müssen die vertraulichen Daten vorher unlesbar gemacht werden.

Hierfür sollten die Datenträger entweder physisch zerstört oder die Daten auf dem Datenträger so gelöscht werden, dass eine Rekonstruktion nicht möglich ist.

Oft sind die Komponenten zusätzlich von außen mit Namen auf Schnellwahltasten, IP-Adressen, Telefonnummern oder sonstigen technischen Informationen beschriftet. Auch diese Beschriftungen sollten vor der Entsorgung entfernt werden.

Zusätzlich muss darauf geachtet werden, dass den auszusondernden Komponenten die Berechtigungen entzogen werden, um eine unbefugte Verwendungen zu verhindern.

Auf die sichere Entsorgung der Komponenten des Telekommunikationssystems sollte auch in der Sicherheitsrichtlinie hingewiesen werden.

NET.4.1.M12 Datensicherung der Konfigurationsdateien

Die Konfigurations- und Anwendungsdaten der eingesetzten TK-Anlage sind regelmäßig zu sichern, insbesondere nachdem sich diese geändert haben. Dazu muss ein entsprechendes Konzept erstellt und mit den allgemeinen Konzepten der Datensicherung abgestimmt werden. Aufgrund der Ähnlichkeit kann sich das Konzept an dem für die aktiven Netzkomponenten orientieren. Bei Hybrid- oder VoIP-TK-Anlagen kann die Systeminstallation und -konfiguration über Images, Snapshots, Software- und Konfigurationssicherung gesichert werden.

Auch Anwendungsdaten wie Kontaktinformationen oder Abrechnungsdaten sollten gesichert werden. Sicherungszeitpunkte und Formen müssen die Anforderungen an den maximal tolerablen Datenverlust berücksichtigen. Die entsprechenden Festlegungen sind in einen Gesamt-Datensicherungsplan des zentralen IT-Bereichs aufzunehmen.

Wesentlich ist, dass in jedem Fall mit Hilfe der getroffenen Vorkehrungen der aktuelle Zustand vor Eintreten einer Störung oder eines Notfalls wiederhergestellt werden kann.

Es ist in regelmäßigen Abständen zu prüfen, ob diese Sicherungen auch tatsächlich als Basis für eine Systemwiederherstellung funktionsfähig sind. Typische Prüfungen dieser Art sind:

- Prüfung von Datenträgern mit System- oder Datensicherungen auf Lesbarkeit
- Prüfung von Images auf Lauffähigkeit nach Probeinstallation auf Testsystemen oder vergleichbarer Ersatzhardware.

Die durchgeführten Tests und Testergebnisse sind zu dokumentieren.

NET.4.1.M13 Beschaffung von TK-Anlagen

Bei der Beschaffung der TK-Anlagen oder anderer Komponenten, wie der Erweiterung einer klassischen TK-Anlage um VoIP, sollten die Ergebnisse der Anforderungsanalyse und der Planung mit einbezogen werden. Die Vielfalt der Funktionen und Einsatzmöglichkeiten machen die Auswahl und Beschaffung relativ kompliziert und zeitaufwändig.

Darüber hinaus müssen vorhandene Kommunikationssysteme und -komponenten der Institution bei der Beschaffung berücksichtigt werden. Wird eine TK-Anlage nicht vollkommen neu beschafft, muss darauf geachtet werden, dass Altbestand und Neubeschaffungen kompatibel zueinander sind. Bei der Beschaffung neuer TK-Anlagen ist darauf zu achten, dass diese so ausgewählt werden, dass im späteren Betrieb mit geringem personellen und organisatorischen Zusatzaufwand ein hohes Maß an Sicherheit erreicht werden kann. Hierfür müssen in erster Linie auf

- das Vorhandensein geeigneter Funktionalitäten für die Anlagenadministration,
- ausreichende Protokollmechanismen und Auswertemöglichkeiten sowie auf
- die Revisionsfähigkeit der TK-Anlage

geachtet werden.

Bei der Beschaffung einer klassischen TK-Anlage ist überdies zu beachten, ob sie neben digitalen auch analoge Teilnehmeranschlüsse anbieten muss. Analoge Anschlüsse können notwendig sein, weil analoge Endgeräte wie Faxgeräte, Anrufbeantworter, schnurlose Telefone, Modems für Datenanwendungen, wie Signalisierungen oder Notruf, angeschlossen werden sollen. Dazu kommen die, entsprechend der gewünschten Leistungsmerkmale ausgewählten, analogen oder digitalen Geräte.

Bei Hybridanlagen werden klassische TK-Anlagen um IP-Funktionen erweitert und ermöglicht, IP-Endgeräte an die TK-Anlage anzuschließen. Beschafft werden müssen neben der TK-Anlage herkömmliche oder IP-fähige Endgeräte. WerdenPCs als Endgerät eingesetzt, dann müssen diese geeignete Netzschnittstellen, Telefonie-Software, Soundkarte, Mikrofon und evtl. ein Headset aufweisen.

Bei einer VoIP-basierten Lösung müssen folgende Elemente betrachtet werden: VoIP-TK-Anlage, VoIP-Telefone, Softphones, VoIP-Serversoftware und weitere Netzelemente. Dazu kommt optional noch die Integration von Funklösungen und Mehrwertdiensten wie beispielsweise Unified Communications, zu denen CTI (Computer Telephone Integration), Unified Messaging und Voice-Mail gehören sowie ein Vermittlungsplatz oder Billing-System.

Zur Unterstützung bei der Beschaffung von TK-Anlagen kann Teil 2 (Beschaffungsleitfaden) der vom BSI erarbeiteten Technischen Leitlinie "Sichere TK-Anlagen" verwendet werden (siehe [TL02103]). Der Beschaffungsleitfaden nennt zunächst Auswahlkriterien für die Komponenten einer TK-Lösung, die aus den in Teil 1 der Technischen Leitlinie (siehe [TL02103]) spezifizierten Maßnahmen abgeleitet werden. Die Anforderungen werden in einer Bewertungstabelle je nach betrachteten Szenarien unterschiedlich stark gewichtet. Die Struktur orientiert sich an der Methodik der "Unterlage für die Ausschreibung und Bewertung von IT-Leistungen (UfAB IV)" (siehe [UFAB]). Für die Produktauswahl und die Abnahme werden Prüfkriterien entwickelt, die neben Prüfungen der Konfiguration auch Tests auf Ebene der Protokollschnittstellen unter Einsatz von Protokollanalysatoren und Simulationswerkzeugen beschreiben.

NET.4.1.M14 Notfallfürsorge für TK-Anlagen

In jedem IT-Betrieb treten Störungen auf, die vom sporadischen Fehlverhalten der Komponenten bis zum klar abzugrenzenden Ausfall eines Geräts reichen können. Grundlage eines sicheren Betriebs ist die Vorbereitung auf Störungssituationen. Hierzu gehören Ausfälle oder Beeinträchtigungen von Hardware und Software aufgrund von Defekten oder Kompromittierungen und aufgrund von Fehlbehandlung durch die Benutzer.

Um in derartigen Situationen effektiv und schnell reagieren zu können, müssen Diagnose und Fehlerbehebung bereits im Vorfeld geplant und vorbereitet werden. Es ist zudem sinnvoll, Verantwortliche und Ansprechpartner zu benennen. Für typische und für bereits aufgetretene Schadenssituationen sollten Sofortmaßnahmen und weiterführende Handlungsanweisungen erstellt werden. Eine typische Sofortmaßnahme dieser Art kann darin bestehen, einen separaten PSTN-Anschluss mit einem direkt angebundenem Telefon bereitzuhalten, um Notrufe absetzten zu können. Alternativ oder zusätzlich könnten Mobiltelefone als Ersatz vorgehalten werden.

Mittels der sogenannten Katastrophenschaltung, einer im Vorfeld umzusetzenden Maßnahme, können die vorhandenen ankommenden und abgehenden Telefon-Leitungen vorher festgelegten Anschlüssen zugewiesen werden. Dies gewährleistet, dass in einem Katastrophenfall wichtige Einrichtungen handlungsfähig bleiben.

Für bestimmte Elemente der TK-Anlage kann es sinnvoll sein, Ersatzgeräte festzulegen und bereitzuhalten, um eine unvorhergesehen lange Wartezeit auf gleichwertige Ersatzhardware überbrücken zu können. Die Ersatzgeräte können die Funktionalität sofort wieder herstellen, wenn die eventuell notwendige Konfiguration eingestellt wird. Dazu müssen die TK-Anlagen-Konfigurationsdaten gesichert worden sein.

Im Vergleich zum Normalbetriebszustand weist eine solche Ausweichlösung häufig Nachteile hinsichtlich ihrer Performance oder Redundanz auf. Typisches Beispiel für eine Ausweichlösung ist ein (ressourcenschwächeres) Testsystem. Alle Ausweichlösungen haben oft gemeinsam, dass mit ihrer Hilfe nicht der Normalbetriebszustand erreicht wird, sondern nur eine bestimmte Zeit überbrückt werden kann. In einem Notfallplan für die TK-Anlage ist daher festzuhalten, welche Ausweichlösungen eingesetzt werden sollen und welche Schritte für deren Inbetriebnahme notwendig sind. Die Bestimmung der geeigneten Wiederanlaufreihenfolge der Komponenten der TK-Anlage hilft bei der Auswahl der unbedingt zu überbrückenden Komponenten und grundlegenden Funktionen. Je grundlegender die Funktionalität eines Teilsystems für die Arbeit mit der TK-Anlage ist, umso früher sollte ein solches Teilsystem wiederhergestellt oder zumindest durch eine funktionsgleiche Ausweichlösung ersetzbar sein.

Es hat sich in der Praxis gezeigt, dass IT-Gesamtlösungen oft zu komplex sind, um alle möglichen Ausfallszenarien vorbereitend durchzuspielen und geeignete Wiederanlauffestlegungen zu treffen. Daher ist eine fallweise Bestimmung über Prioritätsklassen zu empfehlen. Für alle IT-Systeme werden zunächst Prioritätsklassen festgelegt, die sich aus den folgenden Kriterien ableiten lassen:

- technische Abhängigkeiten solcher Dienste untereinander
- Bedeutung für die Geschäftsprozesse der Institution
- Umfang des von ihrer Verfügbarkeit profitierenden Nutzerkreises

Alle Festlegungen, die zur Bestimmung der Wiederanlaufreihenfolge führen, sind im Rahmen der Notfallvorsorge vorbereitend zu dokumentieren (zum Beispiel im Notfallhandbuch der IT). Gerade bei komplexen Systemen ist auch die Darstellung von Verknüpfungen und Abhängigkeiten, die individuell für die Institution sind, entscheidend für die Beurteilung von Störungen und ein schnelles und sicheres Eingreifen.

Soweit nicht alle relevanten Festlegungen für die Notfallbehandlung der TK-Anlage aus einem übergeordneten Notfallhandbuch hervorgehen, sollten diese in einem Notfallplan festgehalten werden. Dieser nennt alle vorbereiteten und vorbereitend festgelegten Sofortmaßnahmen, Ausweichlösungen, Notbetriebsformen und Schritte zu deren Einleitung, sowie typische Schritte auf dem Weg zur Wiederherstellung des Normalbetriebs. Ebenfalls enthalten sind notwendige Kontaktinformationen für den Notfall, Festlegungen hinsichtlich Zuständigkeiten für die Einleitung/Durchführung von Maßnahmen und besondere Meldepflichten in Notfällen.

Die sichere Beherrschung notwendiger Notfallmaßnahmen ist von hoher Bedeutung. Entsprechend sind typische Maßnahmen regelmäßig einzuüben. Sofern dies nicht im Rahmen regelmäßig im Betriebsalltag wiederkehrender Tätigkeiten erfolgt, müssen die Maßnahmen in Form von Notfallübungen eingeübt werden.

NET.4.1.M15 Notrufe bei einem Ausfall der TK-Anlage

Bei Ausfällen im Bereich der zentralen Anlage ist es fraglich, ob an dieser Anlage angeschlossene Telefone noch Notrufe absetzen können. Als Ausweichlösung kann hier ein separater PSTN-Anschluss mit direkt angebundenem Telefon eingesetzt werden. Bei einer Umsetzung dieser Maßnahme ist entsprechend der räumlichen Ausdehnung des betrachteten Standorts darauf zu achten, dass diese Telefone geeignet platziert werden und eine angemessene Anzahl vorhanden sind.

Die Notrufmöglichkeiten müssen von allen Räumen aus auf ausreichend kurzen Wegen erreichbar sein. Eine einzige zentrale Lösung kann dazu führen, dass Notrufe nicht rechtzeitig abgesetzt werden können, um Schaden zu minimieren bzw. Gefahr für Leib und Leben geeignet abzuwenden.

Die Verkabelung für den TK-Ersatzanschluss sollte auf von der zentralen Anlage separierten Kabelwegen erfolgen. Selbstverständlich können auch Mobiltelefone für Notrufe verwendet werden. Für den erhöhten Schutzbedarf muss jedoch die im Vergleich zum PSTN geringere Verfügbarkeit von Mobilfunknetzen berücksichtigt werden.

NET.4.1.M16 Sicherung von Telefonie-Endgeräten in frei zugänglichen Räumen

Neben den TK-Anlagen können auch die Endgeräte zusätzlich zu der Anschlussmöglichkeit an die Telefonie-Verkabelung weitere Schnittstellen aufweisen. Dazu gehört unter anderem Bluetooth, um drahtlose Headsets zu verwenden, oder WLAN, mit dem ein drahtloses VoIP-Telefon an das LAN und mittelbar an die TK-Anlage angebunden wird. Ungenutzte Schnittstellen und nicht genutzte Leistungsmerkmale sind zu deaktivieren. Werden die Schnittstellen verwendet, so sind sie gegen unbefugten Zugriff mittels vorgeschalteter Authentisierung zu sichern.

Der Umfang der verfügbaren Leistungsmerkmale sollte auf das notwendige Minimum beschränkt und grundsätzlich nur die benötigten Leistungsmerkmale freigeschalten werden. Auf diese Weise wird verhindert, dass die Anlage über ihre Leistungsmerkmale unnötig möglichen Angriffen ausgesetzt wird. Bestimmte Leistungsmerkmale können zu gezielten Angriffen, insbesondere auf Vertraulichkeit oder Verfügbarkeit, missbraucht werden. Auch können im Zuge eines derartigen Missbrauchs vom Anlagenbesitzer ungewollte Gebühren entstehen.

Merkmale mit Missbrauchspotenzial an Endgeräten sind beispielsweise:

- das direkte Ansprechen bzw. die automatische Rufannahme, da mit dieser Funktion die Freisprechfunktionalität des Telefons zum Abhören des Raums missbraucht werden kann,
- der Amtszugang bei leicht zugänglichen Apparaten, da Unbefugte damit die Möglichkeit haben, Gespräche auf Kosten der Institution zu führen,
- die Rufumleitung, da beispielsweise durch versehentliche oder böswillige Fehlnutzung der Nutzer eines Telefonanschlusses nicht erreichbar ist,
- das Aufschalten, durch das ein Anrufer ein bestehendes Gespräch mithören kann,
- die Dial-In-Konferenzschaltung, da sich die Teilnehmer selbst in die Telefonkonferenz einwählen können, ohne das es weitere Teilnehmer mitbekommen und so Unbefugte mithören können und
- verschiedene, für den Export bestimmte Merkmale ("Zeugenschaltung" oder "Abhören"), da sie zu Angriffen auf die Vertraulichkeit nutzbar sind.

Die Endgeräte sollten im Rahmen ihrer vorgegebenen Möglichkeiten so konfiguriert werden, dass eine Warnung erfolgt, sobald sicherheitskritische Merkmale genutzt werden. Die nicht benötigten oder wegen ihres Missbrauchspotenzials als kritisch eingestuften Leistungsmerkmale müssen so weit wie möglich an der zentralen Anlage abgeschaltet werden. Bietet diese dafür nur eingeschränkte oder nicht ausreichend differenzierte Möglichkeiten, so können die zentralen Einstellungen mit entsprechenden Sperreinstellungen auf den Endgeräten kombiniert werden.

Zusätzliche Schutzmaßnahmen sollten für die auf den Endgeräten gespeicherten und abrufbaren vertraulichen Daten wie die Kontaktinformationen oder institutionsweite Telefonbücher, ergriffen werden. Dies gilt insbesondere für Endgeräte in ungeschützten Bereichen wie Besprechungsräumen oder Tiefgaragen. Teilweise ist es jedoch auch möglich, über die TK-Anlage selbst Berechtigungen für die entsprechenden Endgeräteanschlüsse zu vergeben.

Um zu verhindern, dass beispielsweise frei zugänglichen Endgeräten unberechtigt konfiguriert werden, sollten diese mit Passwörtern oder PINs geschützt werden.

Werksmäßig sind viele Endgeräte bereits mit Standard-Passwörtern oder PINs ausgestattet. Diese Standard-Passwörter sollten unbedingt bei der erstmaligen Inbetriebnahme geändert werden. Generell sollten Leistungsmerkmale, wie Rufumleitung, Heranholen von Anrufen oder ähnliches erst nach Eingabe der Authentisierungsinformationen am Gerät genutzt werden können. Um einen Missbrauch der Funktionen der Endgeräte zu verhindern, kann die Möglichkeit des Passwortschutzes genutzt werden.

Da für diese Konfiguration der Endgeräte die Benutzer selbst verantwortlich sind, ist es wichtig, sie zu sensibilisieren und zu schulen.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

NET.4.1.M17 Wartung von TK-Anlagen (CI)

In einer TK-Anlage gibt es eine Wartungseinheit, mit der die TK-Anlage konfiguriert und administriert werden kann. Bei älteren Anlagen kann das eine spezielle Hardware sein, bei neueren Anlagen ist es meist eine Steuerungssoftware. Von außen kann auf diese Einheit je nach TK-Anlage mit unterschiedlichen Mitteln zugegriffen werden, beispielsweise:

- über ein Systemtelefon, also ein Endgerät mit erweiterter Funktionalität gegenüber normalen Endgeräten,
- über einen lokal an die Telefonanlage angeschlossenen Computer (z. B. über RS232, USB, Ethernet),
- über einen PC im LAN, der spezielle Administrationssoftware installiert hat, falls die TK-Anlage auch an das LAN angeschlossen ist,
- über einen Browser eines PCs im LAN, falls die TK-Anlage auch an das LAN angeschlossen ist.

Bei einem IP-Anlagenanschluss, bei dem die TK-Anlage physisch bei einem externen Anbieter steht, wird die TK-Anlage in der Regel über einen Browser administriert.

Die Wartungseinheit sollte so konfiguriert werden, dass nur dedizierte Wartungsrechner zugreifen dürfen. Beispielsweise indem nur IT-Systeme mit fest zugeordneten IP-Adressen mit der Wartungseinheit kommunizieren können. Verbindungsversuche von anderen IT-Systemen sollten abgewiesen werden. Der Zutritt zu den Wartungsrechnern sollte ebenfalls beschränkt werden. Hierfür könnten sie beispielsweise in einem separaten Sicherheitsbereich aufgestellt werden, den unbefugte Personen nicht betreten können.

Generell sollte auf die Wartungseinheit nur nach einer erfolgreichen Authentisierung zugegriffen werden können. Wenn möglich, sollte die Datenverbindung zwischen den Geräten, die zur Wartung genutzt werden und der Wartungseinheit verschlüsselt sein, außer es handelt sich um eine ausschließlich für diesen Zweck genutzte Verbindung (wie ein serielles Kabel). Die Geräte, über die die TK-Anlage gewartet und konfiguriert wird, müssen mit Passwörtern oder PINs abgesichert werden.

Die Wartung einer TK-Anlage sollte von Mitarbeitern mit entsprechendem Wissen, beispielsweise geschulten Administratoren, durchgeführt werden. Fehlen den vorhandenen Mitarbeitern die notwendigen Kenntnisse, um die TK-Anlage optimal zu warten und zu administrieren, und können diese nicht zeitnah geschult werden, sollte überlegt werden, externe Experten zu beauftragen.

Fernwartung

Unter Umständen kann es erforderlich sein, dass TK-Anlagen von Dritten, wie beispielsweise externen Experten, konfiguriert und gewartet werden. Erfolgt die Administration über ein Datennetz, wird hierfür eine Kommunikationsverbindung zur TK-Anlage benötigt. Ist die TK-Anlage an das LAN des Standorts ("Hausnetz") angeschlossen, könnte ein Angreifer sowohl auf die TK-Anlage als auch auf das LAN zugreifen. Daher müssen die Zugänge abgesichert werden. Das kann wie folgt geschehen:

Sollen externe Experten für die Wartungs- und Reparaturarbeiten beauftragt werden, müssen entsprechende Regelungen getroffen werden. Hierzu gehört beispielsweise, wie externe Personen während ihrer Tätigkeit beaufsichtigt werden und wie mit Geräten umzugehen ist, die für eine Reparatur außer Haus gegeben werden. Generell können durch eine Fernwartung zahlreiche Sicherheitsprobleme auftreten. Um diese zu verringern, muss der Fernwartungszugriff geschützt werden. Die Datenverbindung bei IP-basierten Zugängen über öffentliche Netz sollte z. B. mit Secure Shell (SSH) oder über ein Virtuelles Privates Netz (VPN) abgesichert und verschlüsselt werden.

NET.4.1.M18 Erhöhter Zugriffsschutz (CI)

Bei erhöhtem Schutzbedarf ist es notwendig, die zentrale Anlage gezielt gegen Zugriff durch Unbefugte auch mit den Mitteln des Zutrittsschutzes besonders zu schützen. Typische Vorkehrung ist dabei die Aufstellung der Anlage in einem Raum nur mit Zugang für das Anlagen-Betriebspersonal.

Es sind Räume zu wählen, die mindestens mit denselben Maßnahmen gegen unbefugten Zutritt gesichert sind wie die Aufstellungsorte kritischer zentraler IT-Systeme. Sofern die räumlichen Gegebenheiten dies nicht zulassen, empfiehlt sich zumindest die Kombination aus folgenden Punkten:

- Die Aufstellung der Anlage erfolgt in einem Raum, der nur einem eingeschränkten Personenkreis zugänglich ist.
- Die Unterbringung der Anlage erfolgt in einem separaten abschließbaren Schrank.
- Das Schließsystem des Schranks sollte angesichts des erhöhten Schutzbedarfs so ausgelegt sein, dass passende Schlüssel auf das Betriebspersonal der TK-Anlage beschränkt werden können.
- Der Zugang für Externe zur Anlage erfolgt nur unter Aufsicht. Minimum ist dabei die Beaufsichtigung durch Personal, das auf die Unterbindung von nicht vorgesehenen physischen Eingriffen an der Anlage eingewiesen bzw. fallweise über die Notwendigkeit solcher Eingriffe vorab informiert ist. Bevorzugt sollte bei erhöhtem Schutzbedarf die Aufsicht durch Personal erfolgen, das mit der Anlage technisch vertraut ist und so besser beurteilen kann, ob eine vom Externen vorgenommene Änderung an der Anlage unschädlich und auftragsgemäß ist.
- Eine Protokollierung des Aufenthalts im Raum wird durchgeführt. Mindestens protokolliert wird der Aufenthalt Externer (Name, Firma, Zeitraum).
  Ist die Anlage zusammen mit anderem technischen Equipment untergebracht, sodass der Raum für verschiedenes Betriebspersonal zugänglich sein muss, bietet sich bei erhöhtem Schutzbedarf eine Protokollierung jeglicher Anwesenheit im Raum an. Ist der Raum durch ein entsprechendes elektronisches Schließsystem geschützt, können zu diesem gehörende Protokollierungsfunktionen bei der Umsetzung dieser Vorkehrung hilfreich sein.

NET.4.1.M19 Redundanter Anschluss (A)

Der Anschluss der TK-Anlage SOLLTE redundant ausgelegt sein. Bei IP-basierten TK-Anlagen SOLLTE ein zusätzlicher PSTN-Anschluss vorhanden sein.

3 Weiterführende Informationen

3.1 Wissenswertes

Im Bereich TK-Anlagen liegen über den Baustein, die Umsetzungshinweise und die Literaturübersicht hinausgehend keine weiteren wissenswerten Informationen vor.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "TK-Anlagen" finden sich unter anderem in folgenden Veröffentlichungen:

[TL2103] Technische Leitlinie für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf

BSI-TL-02103 - Version 2.0, Bundesamt für Sicherheit in der Informationstechnik, 2014, https://www.bsi.bund.de/DE/Publikationen/TL-sichere-TK-Anlagen/TL02103_htm.html , zuletzt abgerufen am 05.10.2018

[UFAB] Unterlage für Ausschreibung und Bewertung von IT-Leistungen, CIO Bund, 2018https://www.cio.bund.de/Web/DE/IT-Beschaffung/UfAB/ufab_node.html

Umsetzungshinweise zum Baustein NET.4.2 VoIP

1 Beschreibung

1.1 Einleitung

Hinweis: Die Umsetzungshinweise basieren auf den Maßnahmen der 15. Ergänzungslieferung der IT-Grundschutz-Kataloge (Jahr 2015). Die Empfehlungen können sinngemäß umgesetzt werden, es ist jedoch nicht gewährleistet, dass sie immer dem Stand der Technik entsprechen. Das BSI freut sich daher über Anmerkungen, konstruktive Kritik und Verbesserungsvorschläge unter besonderer Berücksichtigung des aktuellen Stands der Technik. Bitte verwenden Sie hierfür die E-Mail-Adresse grundschutz@bsi.bund.de

---

Voice over IP (VoIP) bezeichnet das Telefonieren über Datennetze, insbesondere über das Internet. Um Signalisierungsinformationen zu übertragen, beispielsweise bei einem Anruf, werden spezielle Signalisierungsprotokolle eingesetzt. Die eigentlichen Nutzdaten, wie Sprache oder Video, werden mit Hilfe eines Medientransportprotokolls übermittelt. Beide Protokolle werden jeweils benötigt, um eine Multimediaverbindung aufzubauen und aufrecht zu erhalten. Bei einigen Verfahren wird nur ein Protokoll sowohl für die Signalisierung als auch den Medientransport benötigt.

1.2 Lebenszyklus

Planung und Konzeption

Der Einsatz von VoIP muss sorgfältig geplant werden (siehe NET.4.2.M1 Planung des VoIP-Einsatzes). Die Auswahl eines Signalisierungsprotokolls spielt eine wichtige Rolle, weil die verschiedenen Hersteller von VoIP-Geräten oft nur ein Protokoll unterstützen. Da die Signalisierungsprotokolle untereinander nicht kompatibel sind, beeinflusst die Entscheidung für ein Signalisierungsprotokoll die Auswahl der VoIP-Komponenten. Vertiefende Informationen dazu sind im Abschnitt "Wissenswertes" zu finden.

Beim Telefonieren über VoIP können die gleichen Probleme wie bei jeder anderen Kommunikation über IP auftreten. Viele der von IP-Datennetzen bekannten Angriffe auf die Vertraulichkeit und Integrität können direkt für VoIP übernommen werden. Schutz hiergegen bietet unter anderem eine Verschlüsselung der Signalisierungs- oder Medientransportinformationen. Welche Inhalte in welchen Netzen geschützt werden sollten, verdeutlicht die Maßnahme NET.4.2.M8 Verschlüsselung von VoIP. Die Maßnahmen NET.4.2.M14 Verschlüsselung der Signalisierung und NET.4.2.M15 Sicherer Medientransport mit SRTP vertiefen die Funktionsweise der Verschlüsselung für Signalisierungs- und Medientransportinformationen.

Parallel dazu ist die allgemeine Sicherheitsrichtlinie um eine detaillierte Richtlinie für den Einsatz von VoIP zu ergänzen (siehe NET.4.2.M7 Erstellung einer Sicherheitsrichtlinie für VoIP).

Beschaffung

Im nächsten Schritt sollten die Endgeräte und VoIP-Middleware beschafft werden. Dabei können Softwarelösungen oder Appliances eingesetzt werden. Aufbauend auf die Einsatzszenarien sind die Anforderungen an die zu beschaffenden Produkte zu formulieren und basierend darauf geeigneten Produkte auszuwählen. In der Maßnahme NET.4.2.M7 Geeignete Auswahl von VoIP-Komponenten sind Empfehlungen für die Auswahl zu finden.

Umsetzung

Um auf die Einführung oder den Umstieg auf VoIP vorbereitet zu sein, sollten die Administratoren ausreichend geschult werden (siehe NET.4.2.M10 Schulung der Administratoren für die Nutzung von VoIP).

Neben VoIP-spezifischen Änderungen muss oft das bestehende IP-Datennetz angepasst werden. In einigen Fällen bietet es sich an, zwei Datennetze parallel zu betreiben. Die nicht immer unproblematische Trennung des VoIP-Sprachnetzes vom restlichen Datennetz, die in NET.4.2.M16 Trennung des Daten- und VoIP-Netzes beschrieben wird, kann durch logische oder physikalische Segmentierung erfolgen. Daneben sollte auch der Zugriff auf die VoIP-Komponenten abgesichert werden (siehe Maßnahme NET.4.2.M4 Einschränkung der Erreichbarkeit über VoIP).

Besonders für die Erreichbarkeit aus einem öffentlichen Netz müssen Vorkehrungen getroffen werden. Diese betrifft unter anderem die Anpassung des Übergangs zwischen dem öffentlichen und privaten Netz. Beispielsweise kann die Übersetzung von privaten IP-Adressen in öffentliche IP-Adressen über Network Adress Translation (NAT) sehr aufwendig sein (siehe "Wissenswertes"). Aber auch für die Firewall gelten besondere Voraussetzungen, die in Maßnahme NET.4.2.M13 Anforderungen an eine Firewall für den Einsatz von VoIP beschrieben sind.

Betrieb

Nach der Erstinstallation und einer Testbetriebsphase wird der Regelbetrieb aufgenommen, siehe NET.4.2.M2 Sichere Administration der VoIP-Middleware und NET.4.2.M3 Sichere Administration und Konfiguration von VoIP-Endgeräten. Um auf Probleme reagieren zu können, müssen wichtige Ereignisse protokolliert und ausgewertet werden. Empfehlungen hierfür sind in Maßnahme NET.4.2.M6 Protokollierung bei VoIP zu finden.

Eine Benutzer-Schulung über die Benutzung eines Telefons ist oft nicht wirtschaftlich und sinnvoll, auch wenn typische Büro-Endgeräte heutzutage hochkomplex sind. Dennoch sollten die Benutzer über grundlegende Gefährdungen informiert werden, vertiefende Informationen hierzu sind im Baustein NET4.1.TK-Anlage zu finden.

Aussonderung

Sehr oft sind im Speicher der VoIP-Komponenten schutzbedürftige Informationen abgelegt. Bei der Entsorgung der Komponenten sollte die Maßnahme NET.4.2.M12 Sichere Außerbetriebnahme von VoIP-Komponenten berücksichtigt werden.

Notfallvorsorge

Nur eine regelmäßige und umfassende Datensicherung gewährleistet zuverlässig, dass alle gespeicherten Daten auch im Falle von Störungen, Ausfällen der Hardware oder (absichtlichen oder unabsichtlichen) Löschungen wieder verfügbar gemacht werden können. Die notwendigen Maßnahmen sind im Baustein CON.3 Datensicherungskonzept beschrieben.

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "VoIP" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

NET.4.2.M1 Planung des VoIP-Einsatzes [Leiter IT]

Eine grundlegende Voraussetzung für den sicheren Einsatz von VoIP ist eine angemessene Planung im Vorfeld. Der Einsatz von VoIP kann in mehreren Schritten nach dem Prinzip des Top-Down-Entwurfs geplant werden: Ausgehend von einem Grobkonzept für das Gesamtsystem werden konkrete Planungen für Teilkomponenten in spezifische Teilkonzepten festgelegt. Die Planung betrifft dabei nicht nur Aspekte, die klassischerweise mit dem Begriff Sicherheit verknüpft werden, sondern auch normale betriebliche Aspekte, die Anforderungen im Bereich der Sicherheit nach sich ziehen können.

Im Grobkonzept sollten beispielsweise folgende typische Fragestellungen behandelt werden:

- Soll vollständig oder partiell auf VoIP umgestiegen werden? Soll VoIP nur für die Kommunikation der leitungsvermittelnden TK-Anlagen untereinander eingesetzt?
- Gibt es besondere Anforderungen an die Verfügbarkeit von VoIP oder an die Vertraulichkeit und Integrität der Telefonate bzw. der Signalisierungsinformationen?
- Welche Signalisierungs- und Medientransportprotokolle sollen eingesetzt werden?
- Wie vielen Benutzern soll die Kommunikation über VoIP ermöglicht werden?
- Wie soll die Anbindung ans öffentliche Telefonnetz erfolgen? Sollen VoIP-basierte Kommunikationsverbindungen direkt aus dem öffentlichen Datennetz gestattet werden?
- Kann die Sicherheit des vorhandenen LANs durch VoIP beeinträchtigt werden? Ist das vorhandene LAN für die Nutzung von VoIP ausreichend dimensioniert? Müssen Änderungen an der Netzarchitektur vorgenommen werden?

Die folgenden Teilkonzepte sollten bei der Planung des VoIP-Einsatzes berücksichtigt werden:

- Umfang der Verschlüsselung: Es muss festgelegt werden, was verschlüsselt werden soll. Beispielsweise kann entschieden werden, dass die gesamte Kommunikation im LAN nicht verschlüsselt, aber alle externen Gespräche vor der Einsicht und Manipulation durch Dritter geschützt werden sollen (siehe Maßnahme NET 4.2.M8 Verschlüsselung von VoIP). Im Weiterem muss entschieden werden, ob die Multimediadaten sowie die Signalisierung verschlüsselt werden sollen.
- Verschlüsselungsmechanismen: Wenn für einzelne Kommunikationsstrecken die Verschlüsselung festgelegt wurde, muss entschieden werden, wie der Schutz integriert werden kann. Die Verschlüsselung kann sowohl auf der Anwendungsschicht, wie beispielsweise über H.235 oder SRTP (siehe NET4.2.M14 Verschlüsselung der Signalisierung und NET.4.2.M15 Sicherer Medientransport mit SRTP), als auch auf tieferen Schichten, wie über SSL/TLS, IPSec oder VPNs, erfolgen.
- Komponentenauswahl: Um die getroffenen Entscheidungen umsetzen zu können, müssen die einzusetzenden Geräte diese auch unterstützen. Können keine entsprechenden Geräte beschafft werden, weil beispielsweise nicht alle Anforderungen erfüllt werden können, muss die Planung korrigiert werden. Hierdurch entstehende Änderungen müssen mit dem Sicherheitsmanagement abgestimmt und dokumentiert werden.
- Notfallvorsorge: Nicht nur für die Geschäftsprozesse ist die Verfügbarkeit der Telefonie eine wichtige Voraussetzung. Bei einem Ausfall der Telefonie kann keine Hilfe in Notfällen gerufen werden. Daher müssen entsprechende Vorkehrungen getroffen werden.
- Netztrennung: In einigen Fällen kann die logische oder physikalische Trennung des VoIP-Netzes vom Datennetz sinnvoll sein (siehe Maßnahme NET.4.2.M16 Trennung des Daten- und VoIP-Netzes). In der Planungsphase ist zu entscheiden, ob eine Segmentierung notwendig ist.
- Leistungsmerkmale: Sehr oft bieten VoIP-Komponenten zusätzliche Leistungsmerkmale. Diese können den Betrieb einer zusätzlichen Middleware-Komponente erfordern oder besitzen andere sicherheitsrelevante Nachteile. Zu den sicherheitskritischen Leistungsmerkmalen gehören beispielsweise das Aufschalten auf ein bestehendes Gespräch, Raumüberwachungsfunktionen und das Wechselsprechen. Während der Planung ist zu entscheiden, welche Leistungsmerkmale verwendet werden soll.
- Administration und Konfiguration: Es ist frühzeitig festzulegen, wer die Administration und Konfiguration vornehmen soll. Hierfür sollte ein für VoIP zuständiger Administrator benannt werden. Im Weiterem ist zu entscheiden, wie die Administration erfolgen soll (siehe NET.4.2.M2 Sichere Administration der VoIP-Middleware und NET.4.2.M3 Sichere Administration von VoIP-Endgeräten).
- Protokollierung: Die Protokollierung von Meldungen der einzelnen VoIP-Komponenten spielt eine wichtige Rolle, beispielsweise bei der Diagnose und Behebung von Störungen oder bei der Erkennung und Aufklärung von Angriffen. In der Planungsphase sollte entschieden werden, welche Informationen mindestens protokolliert werden sollen und wie lange die Protokolldaten aufbewahrt werden sollen. Außerdem muss festgelegt werden, ob die Protokolldaten lokal auf dem System oder auf einem zentralen Logserver im Netz gespeichert werden sollen.

Alle Entscheidungen, die in der Planungsphase getroffen wurden, müssen so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können. Dabei ist zu beachten, dass diese Informationen meist von anderen Personen als dem Autor ausgewertet werden müssen. Daher müssen die Dokumente geeignet strukturiert und verständlich formuliert sein.

NET.4.2.M2 Sichere Administration der VoIP-Middleware [Leiter IT]

Bei VoIP-Middleware handelt es sich oft um Server-Systeme, die mit den gleichen Sicherheitsmaßnahmen zu schützen sind, wie sie auch für andere Serversysteme eingesetzt werden. Darüber hinaus sind weitere Sicherheitsmaßnahmen anzuwenden, die den besonderen Bedrohungen bei VoIP-Systemen gerecht werden.

Vor der Inbetriebnahme müssen die VoIP-Komponenten sicher konfiguriert werden. Das Vorgehen bei der Erstinstallation ist zu dokumentieren. Im Folgenden werden einige Punkte vorgestellt, die für eine sichere Konfiguration und Administration berücksichtigt werden müssen.

Leistungsmerkmale

VoIP-Systeme bieten, wie auch traditionelle TK-Systeme, eine Vielzahl verschiedener Leistungsmerkmale. Es sollte vor Inbetriebnahme eines VoIP-Systems geklärt sein, welche Leistungsmerkmale und Funktionalitäten vorhanden sind und welche benötigt werden (siehe NET.4.2.M1 Planung des VoIP-Einsatzes). Die nicht benötigten sowie die sicherheitskritischen Leistungsmerkmale müssen deaktiviert werden. Zu den sicherheitskritischen Leistungsmerkmalen gehören beispielsweise das Aufschalten auf ein bestehendes Gespräch, Raumüberwachungsfunktionen und Wechselsprechen.

Administration und Zugänge

Administration und Konfiguration der Middleware ist immer an der Konsole oder über gesicherte Verbindungen durchzuführen. Die Administration kann beispielsweise über eine Secure Shell (SSH) oder eine verschlüsselte VPN-Verbindung erfolgen.

Viele VoIP-Systeme ermöglichen eine Konfiguration über eine Web-Oberfläche. Der dabei installierte Web-Server kann ein zusätzliches Sicherheitsrisiko darstellen. Daher ist es empfehlenswert, den Web-Server für eine mögliche Web-basierte Konfigurationsoberfläche nicht auf der kritischen Middleware, wie Gateways und Gatekeeper zu betreiben. Eine Web-basierte Konfiguration sollte immer gesichert erfolgen, beispielsweise durch den Einsatz von SSL oder TLS.

Bei der Planung des Administrationskonzeptes sollte ein Rollenkonzept vorgesehen sein, das verschiedene Berechtigungsstufen umfasst. Jeder Rolle sollten im Sinne einer Vertretungsregelung mindestens zwei Personen zugeordnet werden.

Sehr oft bietet es sich an, die VoIP-Komponenten, wie Softphones oder Middleware-Applikationen, auf Standard-PCs mit allgemein verbreiteten Betriebssystemen zu installieren. Die Administration der Betriebssysteme ist, wenn möglich, von der Administration der VoIP-Applikationen personell zu trennen.

Konfigurationsänderungen sollten durch das System so protokolliert werden, dass Manipulationen zeitnah nachvollzogen werden können. Die Protokolldaten selber müssen so abgesichert werden, dass Manipulationen an ihnen ausgeschlossen sind. Hierauf sollten auch Administratoren möglichst keine Zugriffsmöglichkeiten haben. Zum Schutz der Protokolldaten können diese z. B. auf WORM-Medien gespeichert werden oder der Zugriff kann auf Revisoren beschränkt werden.

Backup

Ein umfassendes Datensicherungskonzept ist eine zentrale Anforderung zur Sicherstellung bzw. zur raschen Wiederherstellung der Verfügbarkeit, aber auch, um die Integrität jederzeit überprüfen zu können. Dabei ist darauf zu achten, dass bei der Sicherung personenbezogener Daten, wie beispielsweise privater Verbindungsdaten, diese so abgelegt werden, dass sie vor unbefugtem Zugriff geschützt sind, also beispielsweise verschlüsselt.

Sicherheit der Software

Es ist darauf zu achten, dass die eingesetzte Software immer auf einem aktuellen Stand ist und etwaige sicherheitsrelevante Patches unverzüglich aufgespielt werden. Dies gilt insbesondere auch für das eingesetzte Betriebssystem.

Es muss gewährleistet werden, dass nur Original-Updates und -Patches eingespielt werden. Dies gilt sowohl für die Beschaffung, beispielsweise von den Internetseiten eines Herstellers, als auch für die Übertragung auf die VoIP-Komponenten. Durch folgende Maßnahmen können die Manipulationen bei der Übertragung erschwert beziehungsweise entdeckt werden:

- Vergleich von Prüfsummen
- Nutzung von sicheren Kommunikationswegen
- Verwendung von Zertifikaten

Für die Verlässlichkeit des Gesamtsystems ist eine korrekt implementierte Software von großer Bedeutung. Insbesondere die vitalen Funktionen des Telefoniesystems, wie die einfache Vermittlung von Gesprächen und die Gateway-Funktion in das digitale Fernsprechnetz, sollten daher einem besonderen Evaluierungsprozess unterzogen werden.

Wünschenswert ist es deshalb, dass die Software für die Basisfunktionen des Telefoniesystems, wie die einfache Vermittlung von Gesprächen und die Gateway-Funktion in das digitale Fernsprechnetz, nach einem bewährten Modell entwickelt und möglichst auch von einer unabhängigen Instanz überprüft wurde.

Betriebssystemsicherheit

Die VoIP-Komponenten sollten so konzipiert werden, dass verschiedene Dienste auf verschiedenen Servern betrieben werden. Allerdings ist insbesondere bei kompakten Stand-alone-Systemen, die meist nur aus einer Hardware-Komponente bestehen, die vollständige Trennung von Diensten nicht immer möglich.

Das eingesetzte Betriebssystem sollte als minimales Betriebssystem ausgelegt sein und die Anzahl der auf der Middleware ausgeführten Applikationen so klein wie möglich gehalten werden. Jede zusätzliche Applikation kann Schwachstellen enthalten, die für Angriffe ausgenutzt werden können. Daher ist genau zu prüfen, welche Applikationen benötigt werden. Nicht benötigte Anwendungen sind zu deinstallieren. Software, die nur zur Installation benötigt wird, sollte im Anschluss gelöscht werden (beispielsweise Compiler). Nicht benötigte Netzdienste sind ebenfalls zu deaktivieren und der Zugriff auf die verbleibenden Netzdienste ist durch lokale Paketfilter zu beschränken.

NET.4.2.M3 Sichere Administration und Konfiguration von VoIP-Endgeräten

Wie die VoIP-Middleware müssen auch die VoIP-Endgeräte zahlreiche Sicherheitsvorgaben erfüllen. Ein Unterschied zwischen den Sicherheitsmaßnahmen der Middleware und den VoIP-Endgeräten besteht darin, wie diese sicher konfiguriert werden.

Vertrauenswürdige Firmware-Updates

Viele VoIP-Endgeräte bieten die Möglichkeit zum automatischen Update ihrer Firmware. Es muss sichergestellt werden, dass neue Firmware nur nach erfolgreicher Überprüfung der Authentizität und Integrität des Codes auf die Endgeräte aufgespielt wird. Falls der Hersteller für die Updates Prüfsummen zur Verfügung stellt oder die Update-Pakete digital signiert, müssen die Prüfsummen oder Signaturen vor der Installation überprüft werden. Stellt der Hersteller keine Prüfsummen bereit, muss sichergestellt sein, dass Updates nur über vertrauenswürdige Quellen bezogen werden.

Vertrauenswürdiges Konfigurieren und Digitale Zertifikate

Die meisten VoIP-Endgeräte bieten verschiedene Möglichkeiten zur Konfiguration. Beispiele hierfür sind die lokale Konfiguration am Endgerät, die Web-basierte Konfiguration durch Zugriff auf einen im Endgerät integrierten Webserver sowie die automatische Konfiguration durch "Ziehen" (Pull) der Konfiguration von einem http(s)- oder TFTP-Server.

Die lokale Konfiguration wird in der Praxis selten eingesetzt. Sie sollte mit einem Passwort geschützt sein. Falls sie nicht genutzt werden soll, sollte sie deaktiviert werden. Der Zugang zur Web-basierten Konfiguration sollte ebenfalls nur mit einem Passwort möglich sein und über eine gesicherte Verbindung, beispielsweise über SSL oder TLS, erfolgen. Ein zusätzlicher Schutz wird durch die Verwendung eines Client-Zertifikats zur Authentisierung der Clients erreicht.

Die automatische Konfiguration über einen TFTP-Server sollte nicht gewählt und stattdessen deaktiviert werden, da sie nicht ausreichend sicher ist. Insbesondere die automatische Auswahl eines TFTP-Servers während des DHCP-Bootvorganges bietet zahlreiche Angriffsmöglichkeiten.

Eine automatische Konfiguration sollte grundsätzlich über einen https-Server erfolgen. Der https-Server sollte sich mit einem Zertifikat authentisieren, das vom Endgerät vor dem Laden der Konfiguration überprüft werden kann. Üblicherweise wird das Server-Zertifikat bei der Erstinbetriebnahme manuell auf die Endgeräte installiert.

Sicherheitsfunktionalität

Viele VoIP-Telefone bieten die Möglichkeit zur passwortbasierten ein- oder mehrstufigen Zugangskontrolle (z. B. personenbezogenes Login oder Passwort für Amtsberechtigung). Es ist zu entscheiden, ob die Benutzer nur mit einer vorherigen Anmeldung das Telefon benutzen dürfen. Bei aktiviertem Passwortschutz sollten dann nur Notrufdienste zur Verfügung stehen. Um eine Nutzung durch unautorisierte Personen zu verhindern, müssen die Benutzer dann auch bei kurzfristiger Abwesenheit das Telefon sperren.

Sicherheitsfunktionalitäten, wie beispielsweise Anmeldepasswörter oder Passwörter für Amtsberechtigungen, müssen vor dem Produktiveinsatz ausführlich getestet werden, ob sie auch korrekt implementiert sind. Diese Authentisierungsmechanismen sollten von den Benutzern verwendet werden. Allerdings müssen sie über die Schwächen informiert werden. Anderenfalls besteht die Gefahr, dass nur eine Scheinsicherheit besteht.

Softphones werden in der Regel auf einem Standard-PC, der weitere Aufgaben erfüllt, betrieben. Dieser muss ebenfalls so administriert werden, dass er ein angemessenes Sicherheitsniveau erreicht. Hierzu gehören beispielsweise auch Maßnahmen, dass das Mikrofon nicht durch Dritte aktiviert werden kann. Wird diese Anforderung nicht umgesetzt, könnte das Mikrofon durch einen Angreifer zum Abhören missbraucht werden.

Durch die umfangreiche Angriffsfläche, die komplexe Arbeitsplatzsysteme bieten können, dürfen bei einem hohen oder sehr hohen Schutzbedarf keine Softphones eingesetzt werden.

In der Dokumentation der Komponenten sind oft Informationen zu finden, welche weiteren Sicherheitsfunktionen unterstützt werden. Es ist zu dokumentieren, welche Sicherheitsfunktionen aktiviert wurden.

NET.4.2.M4 Einschränkung der Erreichbarkeit über VoIP [Leiter IT]

In den wenigsten Fällen ist es ratsam, dass direkt aus dem Internet auf die VoIP-Komponenten einer Behörde beziehungsweise eines Unternehmens zugegriffen werden kann. Ein direkter Zugriff, beispielsweise durch den Verbindungsaufbau auf eine interne IP-Adresse, kann einem Angreifer zahlreiche Möglichkeiten eröffnen. Daher ist zu entscheiden, wie externen Gesprächspartnern die Kontaktaufnahme über die VoIP-Architektur ermöglicht werden soll.

Zunächst ist zu prüfen, ob überhaupt der direkte Aufbau einer VoIP-Verbindung von außerhalb unterstützt werden soll. Oft ist es ausreichend, dass die Kontaktaufnahme über ein leitungsvermittelndes Telefonnetz stattfindet. In diesem Fall dürfen keine internen VoIP-Komponenten aus dem öffentlichen Datennetz erreichbar sein. Auf das Gateway, das zwischen dem öffentlichen, leitungsvermittelnden Telefonnetz und dem lokalen VoIP-Netz betrieben wird, sollte vom öffentlichen Datennetz ebenfalls kein Zugriff möglich sein. Bei einem generellen Verzicht auf die Erreichbarkeit über VoIP von außen ergeben sich aber Nachteile für externe Gesprächspartner. Besitzen diese einen Anschluss an ein öffentliches Datennetz, müssen sie dennoch über das öffentliche, leitungsvermittelnde Telefonnetz eine Verbindung aufbauen. Die hierfür anfallenden Kosten sind in der Regel höher als die für ein direkter Verbindungsaufbau zu einer VoIP-Adresse, wie einer SIP-URL. Da diesem Nachteil jedoch viele Vorteile, besonders bei sicherheitskritischen Anwendungsfällen, gegenüberstehen, sollte die Erreichbarkeit über VoIP von außen kritisch betrachtet werden.

Werden Verbindungen von außen nur über das öffentliche, leitungsvermittelnde Telefonnetz zugelassen, so kann auch SPIT (Spam over IP-Telephone) vermieden werden. Da SPIT dann nicht kostengünstig über das Datennetz übermittelt werden kann, fallen die gleichen Kosten wie bei einem Anruf bei einem Benutzer an, der nicht VoIP einsetzt.

Soll dennoch ein Verbindungsaufbau von oder in das öffentliche Datennetz gewünscht werden, ist die Entscheidung inklusive der Restrisiken zu dokumentieren. Außerdem müssen entsprechende Sicherheitsmaßnahmen ergriffen werden. Beispielsweise kann der gesamte Datenverkehr über einen Konzentrator geleitet werden, der wie ein Proxy-Server Verbindungsanfragen annimmt und an das nächste System, wie beispielsweise einen weiteren Server oder direkt an ein Endgerät, weiterleitet. Bei dem Einsatz eines Konzentrators sollten folgende Punkte beachtet werden:

- Sowohl die Signalisierungs- als auch die Sprachinformationen zwischen dem öffentlichen und privaten Datennetz müssen über den Konzentrator geleitet werden. Der Aufbau von individuellen Verbindungen sollte unterbunden werden. Die Paketfilter und Firewalls müssen dementsprechend konfiguriert werden, so dass die VoIP-Kommunikation mit externen Kommunikationspartnern nur über einen Konzentrator stattfinden kann. Beispielsweise kann der Konzentrator innerhalb der demilitarisierten Zone () der Firewall betrieben werden. Auf diese Weise könnte der direkte Verbindungsaufbau aus dem lokalen Netz ins öffentliche Netz beziehungsweise aus dem öffentlichen Netz ins lokale Netz vermieden werden.
- Wegen eines fehlenden Signalisierungsstandards empfiehlt es sich, so viele Signalisierungsprotokolle wie möglich nach außen zu unterstützen. Daher sollte der Konzentrator als Gateway zwischen den im lokalen Datennetz verwendeten Protokoll und den Protokollen, die für externe Benutzer zur Verfügung stehenden, betrieben werden können.
- Um einem Missbrauch entgegenzuwirken, sollte ein Gesprächsaufbau aus dem internen in das externe Datennetz nur nach einer Authentisierung am Konzentrator möglich sein.
- Bei Verbindungen innerhalb des lokalen Datennetzes sollte der Konzentrator nicht beteiligt werden.
- Es muss festgelegt werden, welche Funktionen neben der Sprachkommunikation externen Teilnehmern angeboten werden sollen.
- Der Konzentrator sollte Signalisierungs- und Sprachpakete, die nicht protokollkonform (Beispiele sind zu große Datenpakete) sind, erkennen und abweisen.
- Da direkt auf den Konzentrator aus dem öffentlichen Datennetz zugegriffen werden kann, sollte die sicherheitskritische Konfiguration im Vordergrund stehen.
- Gesprächsteilnehmer aus dem öffentlichen Datennetz müssen die IP-Adresse des Konzentrators kennen, um eine Verbindung zu ihm aufbauen zu können. Daher bietet es sich an, die Adresse des Konzentrators durch einen entsprechenden Eintrag im DNS-Server der Behörde beziehungsweise des Unternehmens zu veröffentlichen.
- Der Empfang, die Bearbeitung und die Weiterleitung der Sprach- und Signalisierungsinformationen können hohe Ressourcen beanspruchen. Daher sollte sowohl die Netzanbindung als auch die Systemressourcen ausreichend dimensioniert werden.
- Werden hohe Anforderungen an die Verfügbarkeit der Erreichbarkeit gestellt, sollte der Konzentrator redundant ausgelegt werden können. Bei einer redundanten Auslegung zur Lastverteilung müssen die verbleibenden Systeme genügend Ressourcen bereitstellen, um einen möglichen Ausfall ausgleichen zu können.

Viele Hersteller bieten hierfür teilweise proprietäre Systeme an. Als Alternative im Open-Source-Umfeld erfüllt die Software-Telefonanlage Asterisk, die als Appliance betrieben werden kann, viele diese Anforderungen. Ein weiterer Vorteil beim Einsatz eines Konzentrators ist die Vermeidung der Probleme, die bei der Verwendung von NAT (Network Adress Translation) auftreten.

NET.4.2.M5 Sichere Konfiguration der VoIP-Middleware

Die Funktion und die Sicherheit der VoIP-Middleware wird wesentlich durch die eingestellten Konfigurationsparameter bestimmt. Sehr oft werden mehrere unabhängige VoIP-Komponenten, wie Gatekeeper und Gateways, benötigt. Das nicht abgestimmte Ändern eines Konfigurationsparameters bei einer Komponente kann daher im Zusammenspiel mit den anderen Komponenten zu Fehlfunktionen führen.

Die für die VoIP-Komponenten zuständigen Administratoren müssen nach der Inbetriebnahme zahlreiche weitere Änderungen vornehmen können. Verlassen Mitarbeiter die Behörde oder das Unternehmen oder kommen neue hinzu, müssen Änderungen vorgenommen werden. Auch bei einem Wechsel in ein anderes Netzsegment, beispielsweise durch einen Umzug in ein anderes Gebäude, müssen Anpassungen durchgeführt werden können. Daher sollte eine Konfigurationsoberfläche gewählt werden, über die die Administratoren diese Anpassungen effizient vornehmen können.

In der Regel werden den Benutzern jeweils ein Benutzername und ein Passwort für die VoIP-Nutzung zugewiesen. Bei der Nutzung von Voice-Mails kann an dieser Stelle eine E-Mail-Adresse eingetragen werden. Es ist darauf zu achten, dass die Benutzer Passwörter auswählen, die nicht zu kurz oder leicht zu erraten sind. Einstellungen, die nur sichere Passwörter akzeptieren, sollten aktiviert werden. Benutzer, die nur stationäre Geräte mit einer gleichbleibenden IP-Adresse besitzen, sollten sich nur mit dem Gerät, dem diese IP-Adresse zugewiesen wurde, anmelden dürfen.

Bei der Zuordnung zwischen Benutzernamen und Telefonnummer müssen eventuell vorhandene interne Vorgaben beachtet werden. Die Vergabe von Telefonnummern, die keinem Benutzer zugeordnet werden, spielt eine weitere Rolle. Ein Beispiel hierfür sind für Besucher frei zugängliche Telefone in Konferenzräumen. Prinzipiell sollten diese Telefonanschlüsse so wenig Privilegien wie möglich erhalten. In der Regel ist die Beschränkung, dass nur interne Gesprächsteilnehmer angerufen werden können, akzeptabel und ausreichend.

Oft kann festgelegt werden, welche Benutzer welche Signalisierungsprotokolle verwenden dürfen. Wenn es möglich ist, sollten alle Benutzer nur ein Protokoll verwenden dürfen, da dies den Administrationsaufwand verringert. Unterstützen die Endgeräte verschlüsselte Signalisierungsprotokolle, sollte darauf geachtet werden, dass eine unverschlüsselte Anmeldung nicht möglich ist.

Den Benutzern des TK-Systems können bestimmte Rechte (Privilegien) zugeordnet oder entzogen werden. Beispielsweise kann das recht eingeschränkt werden, ins Ausland oder kostenpflichtige Service-Rufnummern anzurufen. Bei der Konfiguration muss das Ziel verfolgt werden, dass jeder Benutzer nur die Privilegien erhält, die für ihn vorgesehen sind.

Kleine, selbstentwickelte und den Gegebenheiten angepasste Makros können den Administratoren die Konfiguration erleichtern. Diese Makros sind ausführlich zu dokumentieren. Bei dem Einsatz der Makros ist darauf zu achten, dass sie vor dem Einsatz einer ausführlichen Qualitätssicherung unterzogen und gründlich getestet wurden. Anderenfalls besteht beispielsweise die Gefahr, dass solche Makros schwer auffindbare Konfigurationsmängel erzeugen oder unerwünschte Seiteneffekte mit sich bringen.

Während der Konfiguration muss darauf geachtet werden, dass zusätzliche und nicht zwingend benötigte Dienste deaktiviert werden beziehungsweise bleiben. Anderenfalls besteht die Gefahr, dass diese Dienste für Angriffe ausgenutzt werden.

Zahlreiche Ereignisse können protokolliert werden. Über die Signalisierungsinformationen kann beispielsweise ausgewertet werden, welcher Benutzer wie lange mit wem telefoniert hat. Werden die Medieninformationen nicht direkt zwischen den Endgeräten, sondern über die Middleware ausgetauscht, ist eine zentrale Auswertung der Gesprächsinhalte grundsätzlich möglich. Einerseits können Protokollierungsfunktionen zur Nachvollziehbarkeit des VoIP-Betriebs beitragen. Andererseits muss verhindert werden, dass Protokollierungsfunktionen für Verletzungen der Informationssicherheit oder des Datenschutzes missbraucht werden.

Es muss deshalb systematisch und verbindlich festgelegt werden, welche Informationen protokolliert werden und wie die regelmäßige Auswertung der Protokolldaten erfolgt. Dabei ist in jedem Fall der Datenschutzbeauftragte und der Personal- beziehungsweise Betriebsrat zu beteiligen. Treten bei der Auswertung Unstimmigkeiten auf, müssen diese näher beleuchtet und die Ursachen gegebenenfalls beseitigt werden.

Alle Einstellungen sind durch eine regelmäßige Revision zu überprüfen.

NET.4.2.M6 Protokollierung bei VoIP

Bei einer Kommunikation über VoIP können zahlreiche Informationen protokolliert werden. Meist müssen bestimmte Statusinformationen der VoIP-Middleware protokolliert werden, um für einen reibungslosen Betrieb zu sorgen. Erst die regelmäßige Auswertung dieser Protokolldaten ermöglicht es, die korrekte Funktion der Geräte zu beurteilen und Angriffsversuche zu erkennen. Mit Hilfe der Protokolldaten kann oft auch die Art eines Angriffsversuches nachvollzogen und die Konfiguration entsprechend angepasst werden.

Die sorgfältige Konfiguration der Protokollierungsfunktionen ist besonders wichtig, da nur eine sinnvollen Filterung aus der Vielzahl von Informationen die relevanten Daten extrahiert.

Je nach Art der protokollierten Ereignisse kann es erforderlich sein, schnellstmöglich einzugreifen. Daher müssen die Protokolldaten regelmäßig ausgewertet werden.

Einerseits können Protokollierungsfunktionen zur Nachvollziehbarkeit des VoIP-Betriebs beitragen. Andererseits besteht die Gefahr, dass Protokollierungsfunktionen für Verletzungen der Informationssicherheit oder des Datenschutzes missbraucht werden. Es muss deshalb verbindlich festgelegt und dokumentiert werden, welche Informationen protokolliert werden und wie die regelmäßige Auswertung der Protokolldaten erfolgt. Dabei ist in jedem Fall der Datenschutzbeauftragte und der Personal- beziehungsweise Betriebsrat zu beteiligen. Der Umfang der Protokollierung und die Kriterien für deren Auswertung sollten dokumentiert und innerhalb der Institution abgestimmt werden. Gegebenenfalls sollten frühzeitig die jeweiligen Mitbestimmungsgremien beteiligt werden.

Protokollierung der Signalisierung

Durch die Auswertung der Signalisierung können zahlreiche Informationen ermittelt werden. An einem Sip-Proxy, Gatekeeper oder Gateway sollten folgende Daten aufgezeichnet werden:

- wer mit wem telefoniert hat,
- wie lange telefoniert wurde,
- ob der Empfänger das Gespräch entgegen genommen hat,
- von welchem Netz und welcher IP-Adresse aus das Gespräch geführt wurde sowie
- welche Medientransportprotokolle und welcher Codec ausgehandelt wurden.

Diese Informationen können beispielsweise für eine Kostenabrechnung oder für eine Optimierung der VoIP-Infrastruktur genutzt werden.

Protokollierung des Medientransports

Durch die Protokollierung an einer geeigneten Stelle im Netz können unter bestimmten Bedingungen die eigentlichen Gesprächsinhalte aufgezeichnet werden. Bei Gesprächen, die das Netz über eine definierte Stelle verlassen, wie beispielsweise über einen Proxy, könnte die Protokollierung direkt an dieser Stelle vorgenommen werden.

Bei internen Gesprächen ist häufig kein Proxy erforderlich. Auch in diesem Fall ist eine Aufzeichnung der Gesprächsinhalte in der Regel möglich, beispielsweise an den beteiligten Endgeräten oder Routern.

Werden die kryptographischen Schlüssel bei einem wirksam verschlüsselten Medientransport direkt von den beteiligten Gesprächsteilnehmern ausgehandelt, können weniger Informationen an zentraler Stelle erfasst werden.

Protokollierung der Systemstatusinformationen

Neben den oben genannten Punkten sollten folgende Informationen nach Möglichkeit an der VoIP-Middleware protokolliert werden:

- Alle direkten Anmeldungen auf der Appliance beziehungsweise auf dem IT-System,
- Veränderungen der Konfiguration,
- Fehlerhafte Anmeldungen am VoIP-Dienst,
- Systemfehler,
- Auslastung,
- Änderungen an der Benutzerverwaltung (Anlegen oder Löschen von Benutzern, Änderungen der Zuordnung zwischen Benutzer und Telefonnummer, etc.),
- Hardware-Fehlfunktionen, die zu einem Ausfall eines IT-Systems führen können und
- wichtige Systemereignisse des IT-Systems, auf dem die VoIP-Applikation betrieben wird. Weitere Informationen hierzu sind dem entsprechenden IT-Grundschutz-Baustein zum Betriebssystem entnehmen.

Zentrale Verwaltung der Protokolldaten

Es ist zu empfehlen, die Protokolldaten über das Netz auf einen eigenen syslog-Server zu übertragen. Dies dient der zentralen Sammlung, Archivierung und Auswertung der Protokolldaten, da auf den VoIP-Applicances oft keine ausreichenden Betriebsmittel dafür vorhanden sind. Außerdem bietet dies den Vorteil, dass bei einer Kompromittierung eines Gerätes die bereits übertragenen Protokolldaten vom Angreifer nicht direkt verändert oder gelöscht werden können.

Falls die Übertragung zum syslog-Server unverschlüsselt erfolgt, ist ein Mithören auf dem Übertragungsweg möglich. Daher sollten die Protokolldaten entweder nur am Server selber gespeichert werden, oder verschlüsselt oder über ein eigenes Netz (Administrationsnetz) übertragen werden.

Zeitsynchronisation

Alle Protokolldaten sollten möglichst mit einem korrekten Zeitstempel versehen sein. Nur so ist eine effektive Auswertung dieser Daten, insbesondere bei der Analyse von versuchten oder erfolgten Angriffen, möglich. Deshalb sollten im internen Netz entsprechende Server eingerichtet werden, die allen Systemen die korrekte Zeit bereitstellen. Dies kann beispielsweise auf Basis des NTP-Dienstes geschehen.

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich VoIP.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "VoIP".

NET.4.2.M7 Erstellung einer Sicherheitsrichtlinie für VoIP

Bei der Telefonie werden hohe Erwartungen in deren Verfügbarkeit gesetzt. Ebenso wichtig ist aber deren Vertraulichkeit. Daher ist der sichere und ordnungsgemäße Betrieb von Telekommunikationseinrichtungen besonders wichtig. Dieser kann nur sichergestellt werden, wenn das Vorgehen in die bestehenden sicherheitstechnischen Vorgaben integriert ist.

Die zentralen sicherheitstechnischen Anforderungen an VoIP sowie das zu erreichende Sicherheitsniveau ergeben sich aus der institutionsweiten Sicherheitsleitlinie. Sie sollten in einer spezifischen Sicherheitsrichtlinie für VoIP formuliert werden, um die übergeordnete und allgemein formulierte Sicherheitsleitlinie zu konkretisieren und umzusetzen. In diesem Zusammenhang ist zu prüfen, ob neben der institutionsweiten Sicherheitsleitlinie weitere übergeordnete Vorgaben wie beispielsweise IT-Richtlinien, Passwortrichtlinien, Richtlinien zu den IT-Systemen, auf denen die VoIP-Komponenten betrieben werden, oder Vorgaben zur Internetnutzung zu berücksichtigen sind.

Die VoIP-Sicherheitsrichtlinie muss allen Personen und Gruppen, die an Planung, Beschaffung und Betrieb der VoIP-Komponenten beteiligt sind, bekannt und Grundlage für deren Arbeit sein. Wie bei allen Richtlinien sind ihre Inhalte und ihre Umsetzung im Rahmen einer übergeordneten Revision regelmäßig zu prüfen.

Die Sicherheitsrichtlinie sollte zunächst das generell zu erreichende Sicherheitsniveau spezifizieren und grundlegende Aussagen zum Betrieb von VoIP treffen. Nachfolgend sind einige Punkte aufgeführt, die berücksichtigt werden sollten.

Allgemeine Regelungen für die VoIP-Nutzung

Alle VoIP-Benutzer sollten über potentielle Risiken und Probleme bei der VoIP-Nutzung sowie über den Nutzen, aber auch die Grenzen der eingesetzten Sicherheitsmaßnahmen aufgeklärt sein.

Da für die VoIP-Komponenten immer wieder neue Sicherheitslücken offen gelegt werden, sollte sich der Informationssicherheitsbeauftragte (ISB) regelmäßig über aktuelle Risiken informieren. Gegebenenfalls ist es angebracht, die Mitarbeiter regelmäßig über die neu bekannt gewordenen Gefahren zu informieren und damit auch zu sensibilisieren.

Bei der Erstellung einer VOIP-Sicherheitsrichtlinie ist es empfehlenswert, so vorzugehen, dass zunächst ein Maximum an Forderungen und Vorgaben für die Sicherheit der Systeme aufgestellt wird. Diese sollten anschließend zwischen allen Beteiligten abgestimmt werden und auf Machbarkeit überprüft werden. Idealerweise wird so erreicht, dass alle notwendigen Aspekte berücksichtigt werden. Für jede im zweiten Schritt verworfene oder abgeschwächte Vorgabe sollte der Grund für die Nicht-Berücksichtigung dokumentiert werden.

In der Sicherheitsrichtlinie muss klar geregelt sein,

- ob und wo VoIP-Komponenten eingesetzt werden dürfen,
- unter welchen technischen Einsatzbedingungen VoIP eingesetzt wird. Hierzu gehören vor allem die Festlegung von Sicherheitsmaßnahmen, die Auswahl und Installation der erforderlichen Sicherheitshard- und -software sowie Vorgaben für die sichere Konfiguration der betroffenen IT-Systeme,
- welche Informationen nicht über VoIP kommuniziert werden dürfen und
- welche Leistungsmerkmale und Funktionen unterstützt werden sollen.

Mitarbeiter müssen darüber informiert sein, unter welchen Bedingungen sie VoIP außerhalb der eigenen Institution benutzen dürfen, da hier unter Umständen andere Sicherheitsregelungen gelten.

VoIP-Middleware

Für den Betrieb von VoIP-Middleware muss unter anderem folgendes geregelt werden:

- Die Vorgaben für Beschaffung von Geräten anhand eines Anforderungsprofils (siehe auch NET.4.2.M9 Geeignete Auswahl von VoIP-Systemen) müssen erstellt werden.
- Es müssen Regelungen für die Arbeit der Administratoren und Revisoren getroffen werden. Folgende Fragen sollten hierfür beantwortet werden:
  - Über welche Zugangswege dürfen Administratoren und Revisoren auf die Systeme zugreifen (beispielsweise nur lokal an der Konsole, über ein eigenes Administrationsnetz oder über verschlüsselte Verbindungen)?
  - Welche Vorgänge müssen dokumentiert werden? In welcher Form wird die Dokumentation erstellt und gepflegt?
  - Gilt für bestimmte Änderungen das Vier-Augen-Prinzip?
  - Kann der Aufgabenbereich des Administrators für die IT-Systeme von dem Verantwortlichen für die VoIP-Applikation getrennt werden?
- Die Verantwortlichkeiten müssen festgelegt und geregelt werden.
- Vorgaben für die Installation und Konfiguration müssen festgelegt und dokumentiert werden, wie
  - das Vorgehen bei der Erstinstallation,
  - die Überprüfung der Default-Einstellungen hinsichtlich ihrer Sicherheitsgefährdungen und
  - die Verwendung und Konfiguration.
- Eine Benutzer- und Rollenverwaltung muss eingeführt, beziehungsweise erweitert werden. Hierzu gehören:
  - Regelungen zur Benutzer- und Rollenverwaltung, Berechtigungsstrukturen (Ablauf und Methoden der Authentisierung und Autorisierung, Berechtigungen für Installation, Updates, Konfigurationsänderungen etc.),
  - ein Rollenkonzept für die Administration und
  - eine Konzeption der Benutzerverwaltung. Die Benutzer müssen angelegt und Telefonnummern zugewiesen werden. Den Benutzern können bestimmte Privilegien, wie der Möglichkeit kostenpflichtige Servicenummern anzurufen, zuwiesen werden.
- Ein sicherer Betrieb erfordert Regelungen
  - zur Erstellung und Pflege von Dokumentation, Form und Umfang der Dokumentation, z. B. Verfahrensanweisungen, Betriebshandbücher,
  - dazu, welche Dienste und Protokolle zugelassen bzw. nicht zugelassen werden,
  - zu den erlaubten Kommunikationsverbindungen, wie zum Beispiel sollte ein direkter Verbindungsaufbau von internen VoIP-Systemen in öffentliche Netzen vermieden werden,
  - für die Durchführung von Softwareaktualisierungen und
  - zu den Vorgaben in der Sicherheitsrichtlinie der IT-Systeme, auf denen die VoIP-Middleware betrieben wird.
- Die Vorgaben für den sicheren Betrieb sollten Informationen dazu beinhalten, wie
  - die Administration abzusichern ist (beispielsweise sollte ein Administrationszugriff nur über abgesicherte Verbindungen erfolgen),
  - verschlüsselnde Signalisierungs- und Medientransport-Protokollen einzusetzen sind,
  - welche Werkzeuge für Betrieb und Wartung einzusetzen sind,
  - Berechtigungen zu vergeben sind und welche Vorgehensweisen bei Software-Updates und Konfigurationsänderungen zu beachten sind und
  - welche Sicherheitsmaßnahmen auf dem Betriebssystem umzusetzen sind, auf dem die Middleware betrieben wird.
- Für die Protokollierung ist zu entscheiden,
  - welche Ereignisse protokolliert,
  - wo die Protokolldateien gespeichert und
  - wie und in welchen Abständen die Protokolle ausgewertet werden sollen.
- Für die Datensicherung und Wiederherstellung bei VoIP-Komponenten muss das institutionsweite Datensicherungskonzept erweitert werden.
- Es müssen Regelungen für die Reaktion auf Betriebsstörungen, technische Fehler (lokaler Support, Fernwartung) und Sicherheitsvorfälle getroffen werden.

VoIP-Endgeräte

Im Folgenden werden Vorgaben für den Betrieb von VoIP-Endgeräten vorgestellt, die in der Sicherheitsrichtlinie ergänzt werden sollten.

- Es müssen Vorgaben für Beschaffung von Geräten anhand eines Anforderungsprofils gemacht werden.
- Es müssen Regelungen für die Arbeit der Administratoren und Revisoren getroffen werden. Ein Beispiel hierfür wäre die Trennung der Administration des einzusetzenden Softphones von der Administration des IT-Systems.
- Vorgaben für die Installation und Konfiguration müssen in der Sicherheitsrichtlinie aufgenommen werden. Hierzu sollten folgende Fragen beantwortet werden:
  - Ist eine Konfiguration bei der Auslieferung der Hardphones ausreichend oder soll im Betrieb eine Konfiguration möglich sein?
  - Wie werden bei einer hohen Anzahl von Endgeräten die Änderungen der Konfiguration im Betrieb durchgeführt?
  - Über welche Zugangswege dürfen Administratoren auf die Endgeräte zugreifen?
  - Welche Arten von Konfigurationen der Leistungsmerkmale, wie beispielsweise Weiterleitungen, dürfen die Benutzer durchführen?
- Vorgaben für den sicheren Betrieb spielen eine wichtige Rolle. Hierzu gehören
  - die Absicherung der Administration (beispielsweise Zugriff nur über abgesicherte Verbindungen),
  - der Einsatz von verschlüsselnden Signalisierungs- und Medientransport-Protokollen,
  - Werkzeuge für Betrieb und Wartung, Integration in ein bestehendes Netzmanagement,
  - Berechtigungen und Vorgehensweisen bei Software-Updates und Konfigurationsänderungen,
  - Vorgaben für Maßnahmen bei der Abwesenheit des Benutzers, wie beispielsweise Rufumleitungen und Sperren des Telefons und
  - der sichere Betrieb des Betriebssystems, auf dem ein Softphone betrieben wird.
  - Für die Notfallvorsorge müssen in der Sicherheitsrichtlinie Regelungen für die Bereitstellung von alternativen Kommunikationswegen aufgenommen werden.

Die Verantwortung für die Umsetzung der VoIP-Sicherheitsrichtlinie liegt beim IT-Betrieb, Änderungen und Abweichungen hiervon dürfen nur in Abstimmung mit dem ISB erfolgen.

NET.4.2.M8 Verschlüsselung von VoIP

Gelingt es einem Angreifer, sich an einer geeigneten Stelle Zugang zu einem internen Netz zu verschaffen, kann er die gesamte Netzkommunikation im LAN protokollieren. Falls die VoIP-Nutzlast nicht verschlüsselt ist, kann der Angreifer sämtliche Informationen mitlesen. Beispielsweise kann er durch die Auswertung der Signalisierungsinformationen ermitteln, wer wie lange mit wem telefoniert hat. Allerdings könnte ein Angreifer auch die Nachrichten auswerten, die über das Medientransport-Protokoll ausgetauscht werden und dadurch die Telefongespräche mithören. Daher sollte überlegt werden, dass die VoIP-Nutzdaten verschlüsselt werden. Eine Verschlüsselung müssen aber alle beteiligten TK-Systeme unterstützen.

Bei der Überlegung, ob die Kommunikation über VoIP verschlüsselt werden soll, ist es häufig zweckmäßig, zwischen interner und externer Kommunikation zu unterscheiden.

Für VoIP-Telefonate innerhalb eines LANs kann überlegt werden, ob auf eine Verschlüsselung verzichtet werden kann. Dabei muss sichergestellt werden, dass auf diese Informationen nicht über einen unsicheren Netzbereich, wie einem ungeschützten WLAN, durch einen Außentäter zugegriffen werden kann. Um die internen Gespräche vor dem Zugriff durch Innentätern zu schützen, kann der Einsatz einer Verschlüsselung aber sinnvoll sein. Hierfür ist der Betrieb der VoIP-Endgeräte als VPN-Endpunkte oder die Nutzung eines verschlüsselten Medientransportprotokolls, wie SRTP, denkbar.

Wenn alle eingesetzten VoIP-Geräte verschlüsselte Signalisierungsprotokolle unterstützen, wird empfohlen, diese zu nutzen. Hierdurch wird unter anderem verhindert, dass ein Angreifer Passwörter mitlesen und sich als ein anderer Benutzer beispielsweise am SIP-Registrar anmelden kann.

Verlassen Pakete mit VoIP-Inhalten das gesicherte LAN, müssen sie mit entsprechenden Verfahren geschützt werden. Für den Schutz der VoIP-Kommunikation ist eines oder mehrere der folgenden Verfahren auszuwählen:

- Nutzung verschlüsselnder Medientransportprotokolle, wie SRTP (Secure Realtime Transport Protocol).
- Verschlüsselung der Signalisierungsprotokolle, beispielsweise mit TLS (Transport Layer Security)
- **Virtual Private Networks (VPNs):**
  Durch den Einsatz von VPN-Gateways können Informationen verschlüsselt zwischen entfernten LANs übertragen werden. Einzelne Geräte können als VPN-Endpunkte betrieben werden. Dies hat den weiteren Vorteil, dass ein Innentäter ebenfalls keinen Zugriff auf die Informationen erhält. Ohne eine direkte Unterstützung von verschlüsselnden Signalisierungs- und Medientransportprotokollen kann auf dieser Weise eine protokollunabhängige Verschlüsselung eingesetzt werden.
  Werden, beispielsweise für eine Kommunikation zwischen verschiedenen Liegenschaften, mehrere VoIP-Vermittlungseinheiten (Middleware) benötigt, sollten diese ebenfalls in einen VPN zusammengefasst werden, wenn keine anderen Verschlüsselungsmechanismen aktiviert werden können. Wird die Verbindung, beispielsweise zwischen mehreren Middleware-Komponenten in unterschiedlichen Liegenschaften, nicht ausreichend geschützt, könnte ein Angreifer unter Umständen alle Gespräche zwischen den Liegenschaften abhören. Wird die Middleware auf einem IT-System betrieben, kann in der Regel eine VoIP-protokollunabhängige VPN-Unterstützung problemlos nachinstalliert werden.
- **Verschlüsselung des Funknetzes:**
  Auf ein ungesichertes Funknetz innerhalb einer Institution könnte auch von außerhalb der Liegenschaft auf das Netz zugegriffen werden. Sind die VoIP-Gesprächsteilnehmer über ein WLAN miteinander verbunden, muss ein qualifizierter Schutz für das WLAN, wie WPA2, genutzt werden (siehe hierzu Baustein NET.2.1 WLAN-Betrieb). Da sich diese Verschlüsselung auf das Funknetz beschränkt, ist zu beachten, dass die Informationen im restlichen LAN ungeschützt übertragen werden. Verlassen die VoIP-Informationen nicht über andere Wege das LAN, gelten bei einer qualifizierten Verschlüsselung die gleichen Bedingungen wie bei einer internen Kommunikation, bei der unter Umständen auf eine Verschlüsselung verzichtet werden kann.

Soll ein Gespräch zu einem Telefonteilnehmer über ein öffentliches Telefonnetz aufgebaut werden, kann die Verbindung zwischen dem VoIP-Endgerät und dem Gateway, der zwischen dem IP-Netz und dem öffentlichen leitungsvermittelnden Netz eingesetzt wird, gegebenenfalls mit VPNs oder verschlüsselnden Signalisierung- und Medientransportprotokollen geschützt werden. Da nur sehr wenige Telefone für leitungsvermittelnde Netze Schutzmechanismen bereitstellen und deren Einsatz vom jeweiligen Empfänger abhängig ist, ist eine Verschlüsselung zwischen VoIP-Gateway und dem Gesprächspartner meist nicht realistisch.

Ist eine verschlüsselte Kommunikation, beispielsweise zu externen Gesprächspartnern, nicht möglich, müssen die Benutzer hierüber informiert und sensibilisiert werden. Vertrauliche Gespräche sollten bei einer fehlenden Verschlüsselung nicht über das Telefon geführt werden.

Bei der Beschaffung von VoIP-Komponenten muss darauf geachtet werden, dass diese verschlüsselnde Signalisierungs- und Medientransportprotokolle wie z. B. TLS und SRTP unterstützen (siehe NET.4.2.M9 Geeignete Auswahl von VoIP-Komponenten).

NET.4.2.M9 Geeignete Auswahl von VoIP-Komponenten

Die verschiedenen Hersteller von TK-Produkten bieten zahlreiche Lösungen zur Telefonie an. Neben reinen Geräte für VoIP und für analoge und digitale Telefonie können auch Produkte, die beide Architekturen unterstützen, erworben werden. Beispiele sind TK-Anlagen für leitungsvermittelnde Netze, die über einen IP-Anschluss verfügen und Gateways, die zwischen eine VoIP-Architektur und ein öffentliches, leitungsvermittelndes Telefonnetz geschalten werden können. Für die Auswahl sind neben der Grundfunktionalität, wie der Unterstützung der benötigten Signalisierungs- und Medientransportprotokolle, zahlreiche sicherheitstechnische Aspekte zu berücksichtigen.

Bevor VoIP-Komponenten beschafft werden, muss eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden. Aufgrund der Bewertung kann dann eine fundierte Kaufentscheidung erfolgen, die sicherstellt, dass das zu beschaffende Produkt im praktischen Betrieb den Anforderungen genügt.

Allgemeine Anforderungen

Nachfolgend werden einige allgemeine Anforderungen aufgelistet, die bei der Beschaffung von VoIP-Endgeräten und der Middleware berücksichtigt werden sollten:

1. Allgemeine Kriterien

- Soll eine VoIP-Appliance oder eine Lösung, die auf einem Standard-PC betrieben werden kann, beschafft werden?
  In jedem Fall muss das meist komplexe Betriebssystem so konfiguriert werden, dass nur die wirklich benötigten Funktionen aktiviert sind, die Zugriffsrechte restriktiv vergeben und Schwachstellen systematisch beseitigt werden.
- Unterstützt das Produkt alle benötigten Protokolle?
- Werden Schulungen von dem Hersteller oder einem unabhängigen Anbieter zu dem Produkt angeboten?
- Gibt es verlässliche Informationen zur Zuverlässigkeit und Ausfallsicherheit von Hard- und Software?
- Können die VoIP-Komponenten den Ansprüchen an die Performance gerecht werden?
- Ist das Produkt nach formalen Methoden, wie den Common Criteria, evaluiert?
- Ist die VoIP-Komponente interoperabel zu bestehenden Produkten?
- Unterstützen die VoIP-Komponenten eine sichere Anmeldung und eine sichere Benutzerverwaltung?
- Enthält die mitgelieferte Produktdokumentation eine genaue Beschreibung aller technischen und administrativen Details?
- Wird für die VoIP-Komponenten die Möglichkeit des Abschlusses von Wartungsverträgen angeboten? Oft ist der Zugriff auf Updates und Unterstützungsleistungen vom Hersteller nur in Verbindung mit einem gültigen Wartungsvertrag möglich. Können im Rahmen der Wartungsverträge maximale Reaktionszeiten für die Problembehebung festgelegt werden? Bietet der Hersteller einen technischen Kundendienst (Hotline) an, der in der Lage ist, sofort bei Problemen zu helfen?
- Lässt sich das Produkt einfach installieren, konfigurieren, und administrieren?

2. Protokollierung

Die angebotenen Möglichkeiten zur Protokollierung müssen mindestens die in der Sicherheitsrichtlinie festgelegten Anforderungen erfüllen. Insbesondere sind die folgenden Punkte relevant:

- Ist der Detailgrad der Protokollierung konfigurierbar?
- Werden durch die Protokollierung alle relevanten Daten erfasst?
- Ist der Zugriff auf die Protokolldaten mit einem Zugriffsschutz versehen?
- Unterstützt das System zentrale Protokollierung? Eine zentrale Protokollierung erleichtert eine gezielte Auswertung der Protokolldaten.
- Kann die Protokollierung so erfolgen, dass die Bestimmungen des Datenschutzes erfüllt werden können?

3. Updates

- Werden regelmäßig Updates und Patches für das Produkt angeboten? Werden Sicherheitspatches zeitnah nach Bekanntwerden einer Sicherheitslücke angeboten?
- Können durch eine Aktualisierung der Software auch neuere Versionen der Signalisierungs- und Medientransportprotokolle, in denen Sicherheitsprobleme beseitigt wurden und die zusätzlichen Sicherheitsmechanismen bereitstellen, verwendet werden?
- Berücksichtigen die Updates tiefere Schichten der VoIP-Komponente, wie Updates im Betriebssystem oder Dienste, die nicht in unmittelbaren Zusammenhang zu VoIP stehen? Um bestehende Schwachstellen im Betriebssystem der Appliance oder im IT-System zu beseitigen, sollten diese Bestandteile ebenfalls aktualisiert werden.
- Werden Updates und Patches so abgesichert, dass ausgeschlossen werden kann, dass bei der Übertragung der Updates diese gegen manipulierte Versionen ausgetauscht werden können?

4. Administration

- Unterstützen die VoIP-Komponenten sichere Protokolle zur Administration?
- Können die VoIP-Komponenten so konfiguriert werden, dass die vorgegebenen Sicherheitsziele erreicht werden können?
- Können wichtige Konfigurationsparameter vor Veränderungen durch Benutzer geschützt werden?
- Können die VoIP-Komponenten über eine zentral gesteuerte Management-Software administriert werden? Ist die administrative Schnittstelle so gestaltet, dass auf fehlerhafte, unsichere oder inkonsistente Konfigurationen hingewiesen wird oder solche verhindert werden?

5. Verschlüsselung

Um über VoIP verschlüsselt kommunizieren zu können, müssen die beteiligten Geräte entsprechende Funktionalitäten beinhalten. Je nach Schutzbedarf kann aber während der Planung entschieden worden sein, auf eine Verschlüsselung der internen VoIP-Kommunikation zu verzichten. Dennoch sollten auch dann VoIP-Komponenten angeschafft werden, die über die Möglichkeit zur Verschlüsselung verfügen oder bei denen diese nachgerüstet werden kann. Folgende Aspekte sollten berücksichtigt werden:

- Unterstützen die VoIP-Komponenten die Verschlüsselung der Medientransport- und Signalisierungsinformationen oder kann die Unterstützung nachträglich eingebunden werden?
- Können die VoIP-Komponenten als VPN-Endpunkte betrieben werden?

Auswahl von Vermittlungssystemen (Middleware)

Telefonie stellt oft einen essentiellen Geschäftsprozess dar. Daher werden unter anderem hohe Anforderungen an die Verfügbarkeit gestellt. Folgende Kriterien sollten bei der Beschaffung berücksichtigt werden:

- Kann die VoIP-Middleware redundant ausgelegt werden?
- Bietet der Hersteller gegebenenfalls Hochverfügbarkeitslösungen an?
- Sollen ein oder mehrere, zentrale Geräte die VoIP-Gesamtfunktionalität bereitstellen oder sollen mehrere einzelne, voneinander abhängige Geräte beschafft werden?
  Einzelne, voneinander abhängige Geräte sind zum Beispiel SIP-Registrare, Proxy-Server und Location Server. Systeme, die alle VoIP-Funktionalitäten in einer Gesamtlösung bereitstellen, lassen sich oft leichter konfigurieren. Mehrere, verteilte Systeme können dagegen besser skaliert werden. Da die Administration bei mehreren Geräten oft aufwendiger ist, sind dadurch Fehlkonfigurationen wahrscheinlicher.

Auswahl der aktiven Netzkomponenten

Falls für den Umstieg auf VoIP neue Netzkomponenten wie Switches beschafft werden, müssen diese ebenfalls besondere Voraussetzungen erfüllen. Soll VoIP über ein bestehendes Datennetz genutzt werden, müssen die Geräte VoIP-Pakete erkennen und bevorzugt weiterleiten können. Soll zwischen zwei lokalen Netzen über ein unsicheres Datennetz, wie dem Internet, telefoniert werden können, müssen weitere Anforderungen gestellt werden. Wenn bisher keine Maßnahmen zur Verschlüsselung ergriffen wurden, sollten beispielsweise die am unsicheren Netz angeschlossenen Gateways als VPN-Endpunkte eingesetzt werden können.

NET.4.2.M10 Schulung der Administratoren für die Nutzung von VoIP

Telefonie stellt unabhängig von der TK-Anlage zugrunde liegenden Technologie die Kommunikationsbasis der Institution dar. Deswegen ist es unerlässlich, dass die Administratoren ausreichend geschult sind, damit sie in der Lage sind, die benötigten Funktionen und Sicherheitsmerkmale optimal zu nutzen.

In den Schulungen sollten ausreichende Kenntnisse zu den für die Einrichtung und den Betrieb der VoIP-Komponenten notwendigen Vorgehensweisen, Werkzeugen und Techniken vermittelt werden. Dies gilt auch für herstellerspezifische Aspekte einzelner Produkte, die als VoIP-Komponenten eingesetzt werden.

Für den effizienten Einsatz von VoIP werden ausführliche Kenntnisse über Netze benötigt. Diese müssen ebenfalls in der Schulung vermittelt werden. Oft werden die VoIP-Komponenten auf Standard-IT-Systemen mit eigenständigem Betriebssystem eingesetzt. Hinweise zu diesem Schulungsbestandteil sind in den jeweiligen IT-Grundschutz-Bausteinen zu den Betriebssystemen zu finden.

Im Allgemeinen sollten in den entsprechenden Schulungen mindestens folgende Elemente enthalten sein:

- Grundlagen zu VoIP-Kompression und Übertragung von Sprachnachrichten mit möglichen Auswirkungen wie Jitter, Delay und Echo
- Grundlagen der eingesetzten Protokolle der Anwendungsschicht (beispielsweise RTP, SIP und H.323)
- Administration
    - Sicherheitsrelevante Grundlagen und Konzepte der Administration, Kenntnisse der Kommandos zu Einrichtung, Betrieb, Wartung und Fehlersuche für jede VoIP-Komponente. Eine Schulung sollte eine ausgewogene Mischung aus Theorie und Praxis darstellen.
    - Kenntnisse über die Administration der IT-Systeme, auf denen die VoIP-Komponenten betrieben werden sollen.
    - Überblick über relevante rechtliche Aspekte beim VoIP-Betrieb wie z. B. Datenschutz
    - Management der Geräte, Werkzeuge
    - Protokollierung
    - Sicherung und Verwaltung von Konfigurationsdaten
    - Angriffsszenarien (z. B. Denial of Service Angriffe, ARP-Spoofing, IP-Spoofing, DNS-Spoofing, Viren und andere Schadsoftware)
    - Grundlagen zum Thema Virtuelle Private Netze (VPN)
    - Grundlagen zum Umgang mit verschlüsselten Daten (Verschlüsselung z. B. mit SRTP oder IPSec) und Möglichkeiten zur Behandlung verschlüsselter Daten
- Netztechnik
    - Grundlagen der Strukturierung von Netzen und Dienstgüte
    - Grundlagen von IP und der darauf aufbauender Protokolle (IP-Adressierung, ICMP, TCP, UDP)
    - Virtuelle Netzsegmentierung (VLAN)
- Fehlerbehebung
    - Fehlerquellen und Ursachen
    - Mess- und Analysewerkzeuge, Werkzeuge zur automatischen Überprüfung der einzelnen Komponenten der Firewall auf korrekte Funktion
    - Teststrategien zur Fehlersuche

Auch wenn in einer Gruppe von Administratoren die Aufgaben verteilt sind, ist es unverzichtbar, dass alle Administratoren ein allgemeines Grundwissen besitzen. Die individuellen Schwerpunkte können davon ausgehend gezielt ausgebaut und gepflegt werden. Zu vielen Produkten gibt es von den Herstellern oder spezialisierten Anbietern ein umfangreiches Angebot an aufeinander aufbauenden und individuell vertiefenden Seminaren. Das Angebot an qualifizierten Schulungen stellt ebenfalls ein Kriterium dar, das bei der Entscheidung für einen bestimmten Hersteller berücksichtigt werden sollte.

Für Schulungsmaßnahmen sollte bereits bei der Beschaffung von IT-Komponenten ein ausreichendes Budget eingeplant und ein Schulungsplan für alle Administratoren erstellt werden.

NET.4.2.M11 Sicherer Umgang mit VoIP-Endgeräten [Benutzer]

Die Benutzer sollten über die grundlegende VOIP-Gefährdungen und Sicherheitsmaßnahmen informiert sein. Dies könnte z. B. durch eine kurze Unterweisung oder mit Hilfe von Merkblättern geschehen. Es ist darauf hinzuweisen, dass ein abnormes Verhalten gemeldet werden soll.

Viele VoIP-Telefone bieten die Möglichkeit zur passwortbasierten ein- oder mehrstufigen Zugangskontrolle (z. B. personenbezogenes Login oder Passwort für Amtsberechtigung). Es ist zu entscheiden, ob die Benutzer nur mit einer vorherigen Anmeldung das Telefon benutzen dürfen. Bei aktiviertem Passwortschutz sollten dann nur Notrufdienste zur Verfügung stehen. Um eine Nutzung durch unautorisierte Personen zu verhindern, müssen die Benutzer dann auch bei kurzfristiger Abwesenheit das Telefon sperren.

Bei der Nutzung von VoiceMails kann an dieser Stelle eine E-Mail-Adresse eingetragen werden. Es ist darauf zu achten, dass die Benutzer Passwörter auswählen, die nicht zu kurz oder leicht zu erraten sind. Einstellungen, die nur sichere Passwörter akzeptieren, sollten aktiviert werden. Benutzer, die nur stationäre Geräte mit einer gleichbleibenden IP-Adresse besitzen, sollten sich nur mit dem Gerät, dem diese IP-Adresse zugewiesen wurde, anmelden dürfen.

NET.4.2.M12 Sichere Außerbetriebnahme von VoIP-Komponenten

Sollen VoIP-Komponenten, beispielsweise Endgeräte oder Middleware, außer Betrieb genommen oder ersetzt werden, so müssen von den Geräten alle sicherheitsrelevanten Informationen gelöscht werden. Dies gilt nicht nur, wenn Geräte an Hersteller, Service-Unternehmen, Entsorgungsunternehmen oder sonstige Dritte weitergegeben werden. Auch bei Verschrottung, Umzug oder Weitergabe an andere Benutzer müssen entsprechende Maßnahmen ergriffen werden. Neben der endgültigen Außerbetriebnahme betrifft dies insbesondere auch Reparaturen, Wartung und Garantieaustausch.

In vielen Fällen ist es erforderlich, frühzeitig mit Herstellern, Händlern beziehungsweise Service-Unternehmen zu klären, welche Maßnahmen zur Löschung sicherheitsrelevanter Informationen mit den Vertrags- und Garantiebedingungen vereinbar sind. Oft können hier gemeinsam sinnvolle Vorgehensweisen festgelegt werden.

Je nach Einsatzzweck der Komponenten können beispielsweise folgende Informationen auf den Geräten gespeichert sein:

- Auflistungen, wer mit wem telefoniert hat,
- Zeitpunkt und Dauer der Anrufe,
- Benutzernamen und Passwörter für die Anmeldung an der VoIP-Infrastruktur,
- Rechte und Privilegien der einzelnen Benutzer,
- E-Mail-Adressen der einzelnen Benutzer für Voice-Mails,
- Ansagen für den Anrufbeantworter,
- hinterlassene Nachrichten für die Benutzer,
- IP-Adressen und weitere Informationen, die auf den Netzaufbau schließen lassen,
- Protokolldateien,
- Zertifikate und Schlüssel,
- Konfigurationsdateien,
- persönliche Telefonbücher,
- institutionsweite Telefonverzeichnisse mit allen Mitarbeitern,
- Passwörter, um private Gespräche abzurechnen,
- Informationen über weitere Dienste für die Benutzer, wie Terminerinnerungen und
- in Ausnahmefällen die vollständige Aufzeichnung der eigentlichen Telefongespräche.

Aufgrund des Schutzbedarfs dieser Informationen ist darauf zu achten, dass die Daten gelöscht beziehungsweise unlesbar gemacht werden, bevor defekte oder veraltete Geräte außer Betrieb genommen oder ausgetauscht werden. Nach dem Löschen der Daten muss überprüft werden, ob das Löschen auch erfolgreich war. Die Vorgehensweise hängt dabei stark von der Art und vom Verwendungszweck des Gerätes ab.

Bei "normalen" IT-Systemen, die als VoIP-Komponenten eingesetzt waren, sollten die Festplatten mit einem geeigneten Tool so gelöscht werden, dass keine Wiederherstellung der Dateien mehr möglich ist. Die kann beispielsweise dadurch geschehen, dass der Rechner von einem externen Boot-Medium gestartet wird und die Festplatten mit Zufallsdaten überschrieben werden. Dabei ist es empfehlenswert, den Überschreibvorgang mehrfach zu wiederholen.

Bei Appliances hängt die Vorgehensweise davon ab, ob in dem Gerät eine Festplatte eingebaut ist oder ob die Daten in einem nichtflüchtigen Speicher gespeichert werden. Oft bieten die Geräte eine "Factory-Reset" Option, mit der sämtliche Konfigurationseinstellungen auf die Werte des Auslieferungszustands zurückgesetzt werden können. Auch nach dem Ausführen eines "Factory-Reset" sollte überprüft werden, ob die Daten wirklich gelöscht beziehungsweise zurückgesetzt wurden oder ob bestimmte Daten oder Dateien noch vorhanden sind.

Neben den Informationen, die auf dem Gerät selbst gespeichert sind, sollte auch überprüft werden, ob auf den Backup-Medien sensitive Informationen enthalten sind. Falls es nicht aus anderen Gründen (beispielsweise Archivierung, Aufbewahrungspflicht aufgrund gesetzlicher Regelungen) erforderlich ist, die Backup-Medien aufzubewahren, so sollten die Medien nach der Außerbetriebnahme des Gerätes ebenfalls gelöscht werden.

Oft sind die Komponenten von außen mit Namen auf Schnellwahltasten, IP-Adressen, Telefonnummern oder sonstigen technischen Informationen beschriftet. Auch diese Beschriftungen sollten vor der Entsorgung entfernt werden.

NET.4.2.M13 Anforderungen an einer Firewall für den Einsatz von VoIP

Wird ein IP-Datennetz für VoIP genutzt, ergeben sich zusätzliche Anforderungen, insbesondere auch an die Sicherheit des Netzes. Oftmals ist die strikte Trennung von Sprach- und Datennetzen nicht möglich, da beispielsweise Softphones von Arbeitsplatzrechnern aus dem Datennetz auf den VoIP-Server im Sprachnetz zugreifen, Groupware-Clients das direkte Wählen von Rufnummern gespeicherter Kontakte aus der Applikation ermöglichen oder VoIP-Server mit Verzeichnisdiensten, wie LDAP (Lightweight Directory Access Protocol) gekoppelt werden. Hinzu kommt eventuell die Vernetzung geografisch getrennter Behörden-, Unternehmens- bzw. Institutionsstandorte, die beispielsweise einen zentralen VoIP-Server für die institutionsweite Kommunikation verwenden und gleichzeitig diese Verbindung für den Austausch von Daten nutzen.

Eine Firewall soll ein internes, sicheres System vor unberechtigten Zugriffen aus einem unsicheren Netz schützen und gleichzeitig berechtigte Zugriffe zu den geschützten Bereichen zulassen. Was als sicheres bzw. unsicheres Netz gilt, welche Ressourcen schützenswert sind und wie sie zu schützen sind, wird in den Sicherheitsrichtlinien der Institution festgelegt (siehe hierzu auch NET.3.2. Firewall).

Bei der Planung der VoIP-Nutzung sollte überprüft werden, ob die bestehende Firewall für den Einsatz von VoIP angepasst werden kann. Anderenfalls muss eine zusätzliche Firewall hierfür beschafft und installiert werden.

Auswahl und Anforderungen an eine Firewall

Die Leistungsfähigkeit der eingesetzten Firewall bei der Nutzung von VoIP beeinflusst nicht nur den Schutz, sondern auch die Qualität der übertragenen Sprache. Durch die Verarbeitung vieler kleiner Datenpakete, die bei VoIP üblich sind, wird die Firewall stark belastet, wodurch Delay und Jitter der übertragenen Sprachsignale direkt beeinflusst werden.

Werden Signalisierungs- und Sprachdaten über die Firewall hinaus geleitet, sollte eine VoIP-fähige Firewall verwendet werden, das in der Lage ist, die verwendeten Signalisierungsprotokolle mit dem gesamten Rufauf- und -abbau zu analysieren und die jeweiligen Zustände zu speichern. Anhand der Protokolldaten (z. B. die zu verwendenden UDP-Ports für die mit RTP übertragenen Sprachdaten) werden die benötigten Ports für die Dauer der Kommunikation geöffnet.

Im Weiterem hängt die Auswahl des richtigen Systems von den folgenden Faktoren ab:

- Wie groß ist das Netz?
- Welche Systemkomponenten stehen zur Verfügung? Ermöglichen bestehende Switches eine VLAN-Trennung von Sprach- und Datennetzen? Unterstützen bestehende Router Zugriffslisten (ACLs) oder Funktionalitäten von Firewalls?
- Welche Firewalls werden bereits im Datennetz eingesetzt?
- Ist nur eine auf das LAN begrenzte IP-Telefonie oder auch die Internet-Telefonie geplant?
- Wie umfassend sind die Kenntnisse des betreuenden IT-Personals?
- Welche VoIP-Systemkomponenten werden eingesetzt?
- Welcher finanzielle Rahmen steht für die Umsetzung der Sicherheitsziele zur Verfügung?

Konzeption einer Firewall

Unabhängig davon, ob eine bestehende Firewall für die Nutzung von VoIP verändert oder ob ein neues System beschafft werden soll, kann es aus folgenden Komponenten bestehen:

- **Zustandsloser Paketfilter (Stateless Packet Filter)**
  Einfache Paketfilter können auf Routern, Layer-3-Switches bzw. Firewalls zur Trennung von Daten- und Sprachnetz eingesetzt werden, wobei ihre Filterfunktionalität gegenüber zustandsbasierenden Filtern bzw. Application Level Gateways deutlich eingeschränkt ist.
- **Zustandsbasierende Filterung (Stateful Packet Inspection)**
  Zustandsbasierende Paketfilter können die für eine Kommunikation benötigten Rückpakete dynamisch durchlassen und so ein erhöhtes Maß an Sicherheit für ein Netz bereitstellen. Sie speichern Zustände einer Verbindung ab und können so Rückpakete, die zu einer bestehenden Verbindung gehören, durchlassen, ohne das dafür explizite Zugriffslisten konfiguriert werden müssen.
- **Application Level Gateway** (ALG)
  Ein Application Level Gateway kann im Gegensatz zu den vorgenannten Systemen nicht nur auf IP-Adressen und Ports, sondern auch auf der Applikationsebene filtern. Der Vorteil eines Application Level Gateways macht sich gerade bei der Übertragung von RTP-Paketen bemerkbar. Die für die RTP-Übertragung zu verwendenden UDP-Ports werden im Rahmen der Signalisierung (mittels SDP) zwischen den Endpunkten ausgetauscht. Diese Ports variieren in der Regel bei jedem neuen Gespräch und müssen an der Firewall freigegeben werden. Da das ALG den Austausch der Protokollnachrichten verfolgt, in denen die IP-Adressen und die zu verwendenden UDP-Ports vereinbart werden, kann es dynamisch Filter anpassen, die den betreffenden RTP-Strom passieren lassen.

Vergleicht man zustandslose Paketfilter, zustandsorientierte Paketfilter und ALGs miteinander, so empfiehlt es sich aufgrund der Vorteile möglichst ein ALG einzusetzen. Um eingehenden RTP-Verkehr zu ermöglichen, müssen zustandslose und zustandsorientierte Firewalls große Portbereiche dauerhaft öffnen, damit RTP-Pakete mit Sprachdaten durchgelassen werden können. Eine solche Konfiguration stellt ein erhebliches Sicherheitsrisiko dar.

Application Level Gateways hingegen öffnen nur die tatsächlich benötigten Ports für die Dauer der Kommunikation und bieten daher weniger potentielle Angriffsmöglichkeiten.

Die Verwendung von Protokollen wie IAX (InterAsterisk eXchange) erleichtert die Konzeption der Firewall. Da hierbei sowohl die Signalisierungs- und die Medientransportinformationen über einen Nachrichtenstrom übertragen werden, wird nur ein festgelegter Port benötigt. Aufgrund der fehlenden Portaushandlung müssen keine dynamischen Portfilterungen durchgeführt werden.

Konfiguration einer Firewall

Die bei der Nutzung von VoIP eingesetzten Firewalls unterscheiden sich kaum von klassischen Firewalls. Für deren Aufbau und sicheren Betrieb sind die im Baustein NET.3.2.Firewall beschriebenen Maßnahmen umzusetzen.

Die VoIP-spezifischen Einstellungen müssen analog zu den Maßnahmen aus diesem Baustein vorgenommen werden, wie diese konkret umzusetzen sind, ist der Dokumentation des eingesetzten Produktes zu entnehmen.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

NET.4.2.M14 Verschlüsselung der Signalisierung (CI)

Weitaus wichtiger als der Schutz der Medienströme ist die Sicherstellung der Integrität und Vertraulichkeit der Signalisierungsinformationen beim Einsatz von VoIP. Eine Möglichkeit hierfür ist der Transport der Signalisierungsinformationen über verschlüsselte VPN-Kanäle. Eine weitere Möglichkeit besteht im Einsatz von Signalisierungsprotokollen, die eigene Schutzmechanismen bereitstellen. Die beiden wichtigsten Protokolle zur VoIP-Signalisierung sind SIP und H.225 (Setup-Signalisierung) sowie H.245 (Aufbau der logischen Kanäle) innerhalb des H.323 Frameworks. Die Sicherheitsmechanismen dieser Signalisierungsprotokolle werden im Folgenden beschrieben.

Neben diesen Protokollen gibt es weitere Signalisierungsprotokolle wie IAX2, das über keine eigenen Sicherheitsmechanismen verfügt. Darüber hinaus existieren spezielle Signalisierungsprotokolle, wie beispielsweise MGCP, zur Steuerung von Media Gateways, die ebenfalls keine eigenen Sicherheitsmechanismen bieten. Die Absicherung dieser Protokolle muss daher im Allgemeinen durch geeignete Sicherheitsmaßnahmen auf der Vermittlungsschicht erfolgen.

H.235

Grundsätzlich kann die Signalisierung über das Framework H.323 durch Sicherheitsmechanismen auf der Transport- oder Vermittlungsschicht (beispielsweise SSL bzw. TLS oder IPSec) geschützt werden. Diese vom Signalisierungsprotokoll unabhängigen Mechanismen können für Umgebungen mit erhöhten Sicherheitsanforderungen eingesetzt werden. Im Weiterem kann zusätzlich, auch als einziger Schutz der Signalisierung bei normalem Schutzbedarf, das Protokoll H.235 zum Schutz der Integrität und Vertraulichkeit genutzt werden. Es muss entschieden werden, ob und wie die Signalisierung mit H.323 geschützt werden soll. Die Entscheidung ist zu dokumentieren.

H.235 definiert umfangreiche Sicherheitsmechanismen zum Schutz von H.323-basierter Telefonie. Die spezifizierten Mechanismen umfassen insbesondere den Schutz der Anrufsignalisierung (H.225/Q.931) und des Steuerungskanals (H.245) sowie die Sicherheit des Medienstroms.

H.235 betrachtet alle Systemkomponenten, die Endpunkte eines verschlüsselten H.245 Kontrollkanals oder eines verschlüsselten logischen Kanals sind, als vertrauenswürdige Komponenten, die entsprechend authentisiert werden müssen. Beispiele für vertrauenswürdige und zu authentisierende Systemkomponenten sind Gateways.

Eine der folgenden Arten der Authentisierung sollte ausgewählt werden:

1. Authentisierung mittels symmetrischer Kryptographie und eines gemeinsamen, zuvor ausgetauschten Geheimnisses (beispielsweise eines Passwortes). Als kryptographische Verfahren können entweder symmetrische Verschlüsselungsverfahren oder Keyed-Hash-Funktionen dienen, wobei das gemeinsame Geheimnis jeweils als symmetrischer kryptographischer Schlüssel verwendet oder kryptographisch sicher daraus abgeleitet wird.
2. Authentisierung basierend auf zertifizierten öffentlichen Schlüsseln und signierten Nachrichten.Jedes dieser Verfahren kann jeweils mit zwei Nachrichten unter Verwendung von Zeitstempeln oder mit drei Nachrichten mit zufälligen Challenges als Challenge-Response-Protokoll implementiert werden.
3. Diffie-Hellman-Schlüsselvereinbarungsprotokoll mit optionaler Authentisierung: In einer ersten Phase führen beide Kommunikationsparteien ein Diffie-Hellman-Schlüsselvereinbarungsprotokoll basierend auf zertifizierten öffentlichen Schlüsseln durch. Der dabei erzeugte gemeinsame symmetrische Schlüssel wird in der optionalen zweiten Authentisierungsphase zur eigentlichen Authentisierung, basierend auf symmetrischer Verschlüsselung, verwendet.

H.235 spezifiziert im Weiterem einen Mechanismus (Media Anti-Spam), über den ein Empfänger von RTP-Paketen effizient überprüfen kann, ob ein RTP-Paket authentisch ist und von einem autorisierten Sender stammt. Dazu wird ein kurzer MAC (Message Authentication Code) über ausgewählte Felder des RTP-Paketes berechnet, den der Empfänger prüft, bevor er mit der eigentlichen Verarbeitung des RTP-Paketes beginnt. Der MAC kann entweder durch einen Verschlüsselungsalgorithmus oder durch eine Keyed-Hash-Funktion berechnet werden. Dieser Mechanismus ist zur Abwehr von DoS-Angriffen durch RTP-Flooding und SPIT auf bekannt gewordenen RTP-Ports gedacht und sollte, wenn möglich, aktiviert werden.

Wird die Kommunikation über H.235 von den VoIP-Gateways nicht unterstützt, so ist dringend zu empfehlen, den Zugriff auf das Gateway auf Basis von IP-Adressen und H.323-Identitäten so weit wie möglich einzuschränken. Dafür empfiehlt sich der Einsatz eines Gatekeepers und die Einschränkung des Zugriffs auf das VoIP-Gateway nur im "Routed Mode". Im Gegensatz zum "Bridged Mode", bei dem der Gatekeeper nur an der Authentisierung und die Registrierung beteiligt ist, findet beim "Routed Mode" die gesamte Signalisierung über den Gatekeeper statt.

SIP

Ein grundlegendes Problem in der Absicherung von Signalisierungsprotokollen, wie beispielsweise SIP, besteht darin, dass bei der Signalisierung häufig mehrere Komponenten (Endgeräte und Server) involviert sind, die jeweils Teile der Signalisierungsnachrichten lesen oder sogar verändern müssen. Aus diesem Grund ist eine einfache Anwendung von Ende-zu-Ende Sicherheitsmechanismen nicht möglich, anwendungsspezifische Anpassungen müssen vorgenommen werden.

Der SIP-Standard befürwortet deshalb die Verwendung von Sicherheitsmechanismen auf Schichten unterhalb der Anwendungsschicht. Dabei wird nur jeweils die Kommunikation zwischen den einzelnen SIP-Komponenten (UA, Proxy-, Registrar-, Redirect- und Location-Server) abgesichert, was häufig als "Hop-by-Hop"-Sicherheit bezeichnet wird.

Als weiteres Argument für "Hop-by-Hop"-Sicherheitsmechanismen wird im Standard SIP 2.0 darauf hingewiesen, dass den Servern ohnehin in gewissem Umfang vertraut werden muss. Hier sollte jedoch deutlich zwischen Vertrauen bezüglich Signalisierung und Vertrauen bezüglich des Medientransports, d. h. der Sprachdaten, unterschieden werden. Bei erhöhten Sicherheitsanforderungen sollte deshalb geprüft werden, ob zusätzlich geeignete Ende-zu-Ende-Sicherheitsmechanismen zum Schutz des Medientransports erforderlich sind. Dies betrifft beispielsweise auch den Schlüsselaustausch für SRTP.

Besonders bei erhöhten Sicherheitsanforderungen sollte die Signalisierung mit SIP mit SSL bzw. TLS (Transport Layer Security) geschützt werden. Die SIP-Spezifikation RFC 3261 schreibt vor, dass alle konformen SIP-Server (Proxy-Server, Redirect-Server, Location-Server und Registrar-Server) das TLS-Protokoll mit gegenseitiger Authentisierung sowie Einweg-Authentisierung unterstützen müssen. Die Endgeräte sollten TLS verwenden, um ihre Kommunikation mit Proxy-, Redirect- sowie Registrar-Servern zu schützen.

NET.4.2.M15 Sicherer Medientransport mit SRTP (CI)

Das Real-Time Transport Protocol (RTP) wird zur Übertragung von Mediendaten der IP-Telefonie und das Real-Time Streaming Protocol (RTSP) zu deren Kontrolle eingesetzt. Beide Protokolle bieten keine eigenen Schutzmechanismen gegen das Abhören und gegen Manipulationen von IP-Telefonaten an. Erweiterungen von RTP/RTCP sind SRTP/SRTCP, die Schutzmechanismen für die Übertragung zur Verfügung stellen. Beim Einsatz von VoIP sollte überlegt werden, die Nutzdaten durch den Einsatz von SRTP/SRTCP zu schützen. Die Entscheidung ist zu dokumentieren.

Überblick

SRTP kann in VoIP eingesetzt werden, um Vertraulichkeit, Authentizität und Schutz gegen Replay-Angriffe (Wiedereinspielen von Nachrichten) für die Medienübertragung auf Basis von RTP zu erreichen. Es ermöglicht eine sichere Unicast- und Broadcast-Übertragung. Zum Transport werden die RTP/RTCP-Pakete in SRTP/SRTCP-Pakete eingebettet.

Schlüsselmanagement

Das Protokoll SRTP definiert einen Masterschlüssel und jeweils einen Sitzungsschlüssel für Verschlüsselung und Authentisierung. SRTP enthält keinen eigenen Mechanismus zur Erzeugung und Verwaltung der mindestens 128 Bit langen Masterschlüssel. Dies muss mit anderen Standards, wie z. B. Multimedia Internet Keying (MIKEY) realisiert werden.

Falls SRTP eingesetzt wird, ist festzulegen, in welchen zeitlichen Abständen der Masterschlüssel einerseits und die Sitzungsschlüssel andererseits gewechselt werden.

Verschlüsselung

Bei der Verwendung von SRTP im Rahmen von VoIP sollte in der Regel das symmetrische Verschlüsselungsverfahren AES-CTR (Advanced Encryption Standard - Counter Mode) aktiviert werden. Es eignet sich sowohl für Ende-zu-Ende- als auch für abschnittsweise ("Hop-by-Hop") Verschlüsselung.

Authentizität und Integrität

Authentizität und Integrität von RTP-Nachrichten können in SRTP mittels der Funktion HMAC-SHA1 in Kombination mit einem entsprechenden Sitzungsschlüssel gesichert werden. Dabei beträgt die empfohlene Länge der übertragenen Prüfsumme 80 Bit. Demnach muss die 160 Bit lange Prüfsumme aus HMAC-SHA1 auf 80 Bit reduziert werden. Diese Anpassung verringert zwar die Übertragungsgröße von SRTP-Paketen, schwächt aber den Integritätsschutz der Nachrichten. Daher sollte diese Anpassung nur in Ausnahmefällen aktiviert werden. Alternativ können auch Funktionen verwendet werden, die auf anderen anerkannten Hash-Algorithmen basieren. Für die Auswahl ist zu beachten, dass in einigen verbreiteten Hash-Algorithmen kryptographische Schwächen entdeckt wurden. Die Auswahl der Hash-Funktion ist zu begründen und dokumentieren. Vertiefende Informationen hierzu sind im Baustein CON.1 Kryptokonzept zu finden.

Der gleiche Sicherheitsmechanismus ist auch für SRTCP vorgesehen.

SRTP erlaubt eine schwächere Authentisierung (z. B. 32 Bit) beziehungsweise gar keine Authentisierung von Nachrichten für solche Anwendungen, bei denen es unwahrscheinlich ist, dass der Angreifer eine verschlüsselte Nachricht so manipulieren kann, dass eine spätere Entschlüsselung eine sinnvolle Nachricht liefern wird. Wenn möglich, sollte die schwächere Authentisierung für RTP-Pakete nicht verwendet werden. Für RTCP sollte bei erhöhten Sicherheitsanforderungen der oben beschriebene Schutz mittels HMAC-SHA1-Prüfsumme aktiviert werden.

Schutz gegen Replay-Angriffe (Wiedereinspielen von Nachrichten)

SRTP bietet Schutz gegen Replay-Angriffe, bei denen ein Angreifer abgefangene RTP- oder RTCP-Pakete speichert und diese später erneut verschickt, um unter anderem Denial of Service Angriffe durchzuführen. Um das Wiedereinspielen von Nachrichten verhindern zu können, muss ein Integritätsschutz und Nachrichten-Authentisierung vorhanden sein. Der Empfänger von SRTP-Paketen führt dann eine so genannte Replay-Liste, die Kennzahlen von vorher empfangenen authentischen Paketen enthält.

Die maximal mögliche Anzahl der gespeicherten Kennzahlen muss vorher festgelegt werden. Beim Empfang eines neuen Pakets wird diese Liste auf Übereinstimmungen untersucht und die wiederholten Pakete werden verworfen. Bei IP-Telefonen, die einen geringeren Speicher besitzen, ist die Länge der Replay-Liste ein Sicherheitsparameter, der im Fall von erhöhten Sicherheitsanforderungen berücksichtigt werden sollte. Der Umfang der Replay-Liste ist größtmöglich auszuwählen und die Entscheidung ist zu dokumentieren.

Schlüsselmanagement mit MIKEY

MIKEY (Multimedia Internet KEYing) beschreibt das Schlüsselmanagement für die Echtzeit-Multimedia-Kommunikation und ermöglicht den Austausch von Schlüsseln sowie weiteren Sicherheitsparametern zwischen den Teilnehmern. In VoIP kann MIKEY für den Austausch des Masterschlüssels und weiterer Sicherheitsparameter benutzt werden, um eine sichere SRTP-Übertragung zwischen den Endgeräten zu ermöglichen.

MIKEY ist unabhängig vom darunterliegenden Signalisierungsprotokoll, wie H.323 oder SIP. Zudem unterstützt MIKEY einen parallelen Austausch von Schlüsseln und Sicherheitsparametern für unterschiedliche Kommunikationssitzungen und Kommunikationsprotokolle. Demnach ist es möglich, RTP- und RTCP-Verbindungen getrennt voneinander abzusichern. Mit dem Bündelungskonzept von Kommunikationssitzungen erlaubt es MIKEY, einen gemeinsamen Masterschlüssel für mehrere parallele Sitzungen zu benutzen. Somit können z. B. VoIP-Konferenzen effizienter abgesichert werden.

Falls der Einsatz von VoIP mit Hilfe kryptographischer Mechanismen abgesichert werden soll, müssen die von den VoIP-Systemen unterstützten Verfahren für den Schlüsselaustausch in Erfahrung gebracht werden. Von diesen Verfahren ist ein geeignetes Verfahren festzulegen und die getroffene Wahl ist zu dokumentieren.

NET.4.2.M16 Trennung des Daten- und VoIP-Netzes (CIA)

Trennung der Netze über VLANs

Lokale Netze können physikalisch durch aktive Netzkomponenten oder logisch durch eine entsprechende VLAN-Konfiguration, also über virtuelle lokale Netze (Virtual Local Area Networks), segmentiert werden. Eine logische Trennung kann mit VLAN-Technologie auf der Ebene 2 mit VLAN-fähigen Switches aufgebaut werden. VLANs alleine bieten jedoch keinen Schutz vor Angreifern, die sich mit ihrem IT-System (PC, Laptop oder Server) physikalisch an ein VLAN anschließen. Da die Netzdose, also der VLAN-Port, des Telefons jedem unmittelbar zugänglich ist, könnte ein Angreifer direkt die Telefone im VLAN angreifen, indem er z. B. anstatt eines Telefons seinen PC mit dem VLAN verbindet.

Aus diesem Grunde sollten weitere, über die logische Netztrennung hinausgehende Maßnahmen getroffen werden, um derartigen Angriffe zu begegnen.

Physikalische Trennung der Netze

Bei erhöhten Sicherheitsanforderungen kann eine komplette physikalische Trennung des Sprachnetzes vom Datennetz sinnvoll sein. Die physikalische Trennung von Daten- und Sprachnetzen verringert deutlich die Angriffsmöglichkeiten. Außerdem kann bei dem Ausfall eines Netzes, beispielsweise durch den Ausfall der aktiven Netzkomponenten oder einem Kabelbruch, weiterhin über das verbleibende Netz kommuniziert werden. Durch die Trennung hat die Auslastung des Datennetzes keinen Einfluss auf die Auslastung des Sprachnetzes.

Probleme einer Trennung

Bei einer konsequenten Trennung des VoIP-Netzes vom IP-Datennetz können in der Praxis allerdings anderswo zusätzliche Aufwände entstehen:

- Die VoIP-Komponenten benötigen Zugriff auf Benutzerdatenbanken, wie LDAP-Verzeichnisse, die sich typischerweise bereits im Datennetz befinden, aber bei einer Netztrennung eventuell doppelt gepflegt werden müssten.
- Die Verwaltung des VoIP-Netzes, wie die Namensauflösung über DNS, erfordert in der Regel den Zugriff auf das Datennetz.
- Die Administration der VoIP-Komponenten kann bei einer konsequenten Trennung der Netze aufwendiger sein, beispielsweise da Software-Aktualisierungen der VoIP-Komponenten dann nicht mehr über ein Datennetz übertragen werden können, beispielsweise über SFTP, sondern vor Ort eingespielt werden müssen. Auch eine Remote-Konfiguration von VoIP-Komponenten, beispielsweise über SSH oder SHTTP, setzt einen Anschluss an ein Datennetz oder separate IT-Systeme zur Konfiguration voraus.

Diese Probleme können aber durch entsprechende Gateways zwischen dem Daten- und Sprachnetz gelöst werden. Für viele Dienste könnte ein Proxy-Server im Sprachnetz betrieben werden, von dem die Anfragen aus dem Sprachnetz in das Datennetz weitergeleitet werden.

- Weitere Probleme bei der Netztrennung stellen die Nutzung von Multifunktionsgeräten, wie VoIP-Telefone mit integrierten Mail-Client, oder die weit verbreiteten Softphones dar. Diese Endgeräte benötigen sowohl Zugriff auf das Sprach- als auch auf das Datennetz. Ein Ansatz zur Lösung wäre, diese Geräte in einem dafür angelegten logischen Netz zu betreiben. Eine physikalische Trennung ist hier nicht möglich.
- Um den Aufwand der Verkabelung zu verringern, besitzen viele Hardphones einen integrierten "Miniswitch". Dabei wird das Telefon direkt an die Netzdose angeschlossen und ein weiteres IT-System, wie der Arbeitsplatzrechner, wird mit dem Telefon verbunden. Diese Anordnung verhindert die physikalische Trennung des Sprach- vom Datennetz. Für eine logische Trennung muss der Access-Switch die beiden an einem Switchport angeschlossenen Geräte unterscheiden können. Dies ist beispielsweise über die MAC-Adresse oder durch eine IEEE 802.1X-Anmeldung möglich.

Schutz der Ports

Sollen Hardphones oder andere VoIP-Endgeräte, über die nur telefoniert werden soll, eingesetzt werden, ist darauf zu achten, dass von den Netzanschlüssen, mit denen diese Geräte verbunden sind, ausschließlich die vorgesehen VoIP-Verbindungen aufgebaut werden können. Anderenfalls könnte ein Angreifer ein mobiles IT-System an die Netzdose für das TK-Endgerät anschließen und Zugriff auf nicht für ihn bestimmte Informationen und Dienste erhalten. Ein Beispiel hierfür ist ein Telefon in einer nicht dauerhaft beaufsichtigten Umgebung, wie einer Tiefgarage. Dieser Schutz kann durch entsprechende Filterregeln an den aktiven Netzkomponenten erfolgen.

Je nach Schutzbedarf können zusätzliche Maßnahmen, wie Authentisierung nach IEEE 802.1X, eingesetzt werden, um einen sichereren Betrieb zu gewährleisten. Es muss aber berücksichtigt werden, dass eine dynamische oder statische Zuordnung der MAC-Adresse zu einem (Switch) Port oder einer VLAN-Zugriffsliste keinen ausreichenden Schutz darstellt, da MAC-Adressen leicht gefälscht werden können.

3 Weiterführende Informationen

3.1 Wissenswertes

Für VoIP, also die Sprachübertragung über IP-Netze, gibt es unterschiedliche Anwendungsszenarien. Das Bedrohungspotenzial und die Sicherheitsanforderungen sind dementsprechend ebenfalls unterschiedlich. Im Folgenden werden derzeit typische Anwendungsfälle dargestellt.

Einsatz von VoIP im Endgeräteanschlussbereich

Das erste Anwendungsszenario besteht darin, VoIP für die interne Sprachkommunikation in Firmen- und Behördennetzen zu verwenden.

Dies umfasst, vollständig oder auch nur komponentenweise, den Einsatz von IP-Telefonen, eines LAN-basierten Telekommunikationssystems, das die Vermittlungs- und Mehrwertfunktionen übernimmt, sowie die Verbindung in die Außenwelt sicherstellt, und eines IP-Netzes für die Verbindung von Endgeräten und TK-Anlage. Die Verbindung in das digitale Fernsprechnetz kann dabei über lokale Gateways oder über einen VoIP-Provider erfolgen. Bei so genannten "hybriden Anlagen" werden in herkömmliche TK-Anlagen VoIP-Baugruppen integriert, die den Anschluss von IP-Telefonen, meist proprietären Systemtelefonen, ermöglichen.

Ziel dabei ist die Integration der Daten- und Telefonienetze. Den möglichen Einsparungen an Leitungen, Netzkomponenten, Management, Administration und Wartung stehen allerdings zusätzliche Bedrohungen gegenüber wie z. B. das mit geringen Kenntnissen durchführbare Abhören der Datenverbindung, denen Rechnung zu tragen ist. Die erforderlichen Sicherheitsmaßnahmen relativieren einen Teil der Einsparpotenziale, insbesondere bei der Anpassung eines vorhandenen Datennetzes für den VoIP-Einsatz, sind jedoch zwingende Voraussetzung für den sicheren und verlässlichen Einsatz dieser Technologie.

Einsatz von VoIP zur TK-Anlagen-Kopplung

Traditionell werden TK-Anlagen überwiegend über separate Wähl- oder Standleitungen miteinander verbunden.

Eine zunehmend realisierte Anwendung von VoIP ist die Kopplung von lokalen Telekommunikationsanlagen (Trunking) über IP-Verbindungen. Dabei werden traditionelle TK-Anlagen an verschiedenen Standorten unter Nutzung eines WAN-Datennetzes gekoppelt. Die Zusammenführung von Telefonie- und Datennetz in der Standortvernetzung bietet dabei erhebliche Flexibilität, eine effizientere Bandbreitennutzung und damit auch ein Einsparpotenzial.

Einsatz von VoIP zur Internet-Telefonie

Ein weiteres Szenario ist die Sprachübertragung über öffentliche IP-Netze, vor allem über das Internet. Die zunehmend größeren Bandbreiten im Backbone- und Endanschlussbereich, die zu einer mittlerweile akzeptablen Sprachqualität führen, beschleunigen den Trend zur Internet-Telefonie im privaten Bereich.

Dabei können Softphones eingesetzt werden, die meist, ähnlich zu Messaging-Diensten, über zentrale Verzeichnisse registriert sind. Zunehmende Verbreitung finden kompakte und kostengünstige VoIP-Gateways, die es ermöglichen, mit herkömmlichen Telefonen (analog oder ISDN) Internet-Telefonie-Dienste zu nutzen. Es werden aber auch kostengünstige Hardphones für eine private Nutzung von den Herstellern angeboten.

Unternehmen und Behörden nutzen die Sprachübertragung über öffentliche IP-Netze dagegen derzeit kaum. Der Hauptgrund ist, dass hier keine Mechanismen zur Verfügung stehen, um eine bestimmte Sprach- oder Übertragungsqualität zu garantieren.

Beim Einsatz von VoIP werden die Steuerinformationen und die eigentlichen Sprachdaten in der Regel getrennt voneinander, mittels unterschiedlicher Übertragungsprotokolle transportiert. Steuerinformationen, wie beispielsweise der Zustand "besetzt", werden über Signalisierungsprotokolle, zum Beispiel H.323 oder SIP (Session Initiation Protocol), übermittelt. Für die Übertragung der Sprachdaten ist hingegen ein Medientransportprotokoll, in der Regel RTP (Real-Time Transport Protocol), zuständig. Nur bei sehr wenigen Protokollen, wie IAX (InterAsterisk eXchange), erfolgt keine Trennung von Steuer- und Medieninformationen.

Es gibt verschiedene Signalisierungsprotokolle. Da diese Protokolle untereinander nicht kompatibel sind, spielt die Auswahl für den Aufbau eines VoIP-Netzes eine wichtige Rolle. VoIP-Komponenten, die kein gemeinsames Protokoll unterstützen, können ohne ein Gateway nicht miteinander kommunizieren. Der Einsatz eines Gateways, das die Anweisungen von einem Protokoll in ein anderes übersetzt, ist sehr aufwendig und umständlich. Daher ist darauf zu achten, dass möglichst nur ein Signalisierungsprotokoll eingesetzt wird.

Die Auswahl der eingesetzten VoIP-Komponenten beeinflusst stark die Auswahl des Signalisierungsprotokolls, da viele VoIP-Komponenten nur ein bestimmtes Signalisierungsprotokoll unterstützen. Bezüglich der Sicherheit spielen die Unterschiede zwischen den Protokollen nur eine geringe Rolle. Es sollte dokumentiert werden, welches Signalisierungsprotokoll ausgewählt wurde.

Im Folgenden werden die verbreiteten Signalisierungsprotokolle H.323 und SIP betrachtet. Neben diesen Protokollen werden auch jeweils alle Arten von VoIP-Komponenten, die für einen Gesprächsaufbau mindestens benötigt werden, vorgestellt.

H.323

Die Protokollgruppe um H.323 beschreibt die Übertragung von Echtzeitinformationen (Video, Audio, Daten) in paketorientierten Transportnetzen. H.323 wurde ursprünglich als Umsetzung des ISDN D-Kanal Protokolls Q.931 auf ein IP-basiertes Netz entwickelt. Innerhalb von dieser Protokollgruppe sind die Protokolle H.225.0, H.245 und H.450 und H.235 definiert. H.323 beschreibt den Rahmen der Signalisierungsprotokolle, H.225.0 die eigentliche Signalisierung, H.245 die Kontrolle der Übertragung der Sprachinformationen und H.450 die eigentliche Telefonie-Funktion. Die optionale Unterstützung von H.235 bietet Schutz der Integrität und Vertraulichkeit der Signalisierung. Vertiefende Informationen sind bei der International Telecommunications Union (ITU) zu finden, von der die Protokolle festgelegt wurden. Audio- und Videodaten werden per UDP, Faxdaten per UDP oder TCP übertragen. Vor der Übertragung dieser Echtzeitdaten werden so genannte logische RTP- und RTCP-Kanäle zwischen den Endpunkten (Terminals) aufgebaut.

An einer H.323-Kommunikation können folgende Komponenten beteiligt sein:

- Terminals stellen die Endpunkte einer H.323-Kommunikation beim Benutzer dar. Diese Endgeräte verfügen in der Regel über einen Lautsprecher und ein Mikrofon und bieten dem Benutzer die Möglichkeit, mit einem anderen Gesprächsteilnehmer eine Verbindung aufzubauen. Eine direkte Verbindung zwischen den Endgeräten ist nur bei bekannter IP-Adresse möglich.
- Gatekeeper werden zur Verwaltung eingesetzt. Da die direkte Verbindungsaufnahme zwischen Terminals nur bei bekannten IP-Adressen möglich ist, agiert ein Gatekeeper als zentrale Steuerkomponente in H.323-Netzen.
- Die Multipoint Control Unit (MCU) ermöglicht Konferenzen, also Gespräche zwischen mehr als zwei Anwendern. In der optionalen MCU laufen sämtliche Medienströme von den Teilnehmern zusammen.
- Gateways realisieren die Übergänge in andere Netze und nehmen dabei die Anpassung der Nutzdaten und der Signalisierungsinformation vor. Beispielsweise vermitteln Gateways zwischen IP- und leitungsvermittelnden Telefonnetzen.

Der größte Nachteil von H.323 ist die Komplexität des Protokolls. Die Vielzahl der verschiedenen Protokolle lässt H.323 sehr unübersichtlich und aufwendig wirken. Diese Komplexität erschwert die Fehlersuche und kann zu Mehrkosten führen. Erschwerend kommt hinzu, dass das im Folgenden vorgestellte SIP von vielen Herstellern bei neueren Produkten priorisiert wird.

Session Initiation Protocol (SIP)

SIP ist ein textbasierendes Client-Server-Sitzungssignalisierungsprotokoll der IETF (Internet Engineering Task Force), das zur Steuerung des Verbindungsauf- und -abbaus von Multimediadiensten verwendet und in RFC 3261 beschrieben wird. Weitere Funktionalitäten, wie Videokonferenzen, Instant Messaging, verteilte Computerspiele und anderen Applikationen benötigen eine Erweiterung der SIP-Spezifikation. Diese sind in separaten RFCs zu finden. Der Multimedia-Nachrichtenstrom, wie die Sprachinformationen bei einem Telefonat, wird mit RTP gebildet. Die Signalisierung wird in der Praxis oft mit SSL bzw. TLS (Transport Layer Security) oder IPSec geschützt.

Das Adressierungsschema von SIP ähnelt stark dem einer E-Mail-Adresse (sip:benutzername@providername.org). Die Lokalisierung erfolg über DNS (Domain Name System). SIP unterstützt Punkt-zu-Punkt- und Punkt-zu-Mehrpunkt-IP-Verbindungen. Durch das einfache Klartextdesign der SIP-Pakete und der geringen Komplexität erfährt SIP eine immer größere Verbreitung.

Folgende VoIP-Komponenten können bei einer Kommunikation über SIP beteiligt sein:

- Die Endgeräte (Telefon, Softphone, Gateway) werden als User Agents (UA) bezeichnet. Ein User Agent kann die Rolle eines Clients bzw. eines Servers einnehmen. Der Initiator eines Gesprächs arbeitet als User Agent Server (UAS), der Gerufene als User Agent Client (UAC). Ein SIP-Endsystem beinhaltet immer beide Funktionen.
- Der Location Server liefert bei einer entsprechende Nachfrage die IP-Adresse des gewünschten Gesprächspartners. Dieser kann über den Benutzernamen identifiziert werden.
- Ein Registrar ermöglicht den Benutzern die Anmeldung und Registrierung. Hierfür meldet sich das Endgerät mit einer Kennung (Benutzername, Kennwort) und seiner SIP-Adresse an den Registrar an. Der Registrar gibt die Adresse (IP-Adresse) des Endgeräts dem Location Server bekannt, unter der er öffentlich erreichbar ist. Aufgrund dieser Registrierung kann das Endgerät lokalisiert werden.
- Ein SIP-Proxy nimmt die Rolle eines Vermittlers ein, der die Signalisierungsnachrichten bearbeitet oder weiterleitet. Ein User Agent sendet eine Anfrage an den SIP-Proxy. Der SIP-Proxy interpretiert die Anfrage und adressiert sie, nach entsprechender Bearbeitung, an den User Agent. Wenn nötig, wird eine Nachricht durch den SIP-Proxy verändert.

Obwohl SIP standardisiert wurde, wird es oft von den Herstellern von VoIP-Komponenten unterschiedlich interpretiert. Diese fehlende Interoperabilität führt dazu, dass nicht alle VoIP-Funktionen bei VoIP-Netzen, an denen Komponenten von verschiedenen Herstellern beteiligt sind, vollständig zur Verfügung stehen. Hiervon ist meist die Authentisierung zwischen den Systemen, die Verschlüsselung und die Bereitstellung von Mehrwertdiensten betroffen. Bei der Beschaffung von VoIP-Komponenten sollte daher deren Interoperabilität mit vorhandenen Komponenten überprüft werden.

Beim Einsatz von SIP in Firewall- bzw. NAT-Umgebungen sind weiterhin einige Besonderheiten zu beachten. Endgeräte, die sich in NAT-Umgebungen befinden, können beispielsweise nur mit hohen Aufwand mit VoIP-Systemen außerhalb der NAT-Umgebung kommunizieren.

Einsatz von NAT für VoIP

NAT (Network Address Translation) ermöglicht das Übersetzen von privaten/internen IP-Adressen in öffentliche/externe IP-Adressen. Bei dieser Adressumwandlung werden durch ein entsprechendes NAT-Gateway private Quell-IP-Adressen und die dazugehörigen privaten Quell-Ports in öffentliche Quell-IP-Adressen mit öffentlichen Quell-Ports übersetzt. Damit das NAT-Gateway Rückpakete bzw. eingehende Pakete, die an die öffentliche IP-Adresse gerichtet sind, an den richtigen internen Host weiterleiten kann, unterhält es eine entsprechende Zuordnungstabelle zwischen öffentlichen IP-Adressen/Ports und privaten IP-Adressen/Ports.

Durch NAT werden im UDP- bzw. TCP-Header des Medienstroms die Quell-IP-Adresse und die Quell-Portnummer modifiziert. Die Angaben über die Quell-IP-Adresse und den Quell-Port im Nachrichtenteil der Signalisierungsnachricht bleiben dagegen unverändert. Als Folge können keine Medienströme an ein VoIP-Telefon, das sich hinter einem NAT-Gateway befindet, gesendet werden. VoIP-Geräte, die sich im Internet befinden, können keinen Medienstrom zu einem VoIP-Telefon senden, das sich hinter einem NAT-Gateway befindet, da die private IP-Adresse nicht ins Internet geroutet wird.

In den folgenden Abschnitten werden Möglichkeiten aufgezeigt, die einen VoIP-Betrieb in einer NAT-Umgebung ermöglichen.

MIDCOM

MIDCOM steht für Middlebox Commmunications und ist ein Entwurf der IETF, der eine Lösung für die NAT- und Firewall-Problematik im Zusammenhang mit VoIP bietet. Ein MIDCOM-System besteht aus einer Middlebox und einem Server, der die Middlebox steuert bzw. konfiguriert. Der Steuerungsserver ist ein VoIP-Server (H.323-Gatekeeper, SIP-Proxy, etc.), der sich im Signalisierungspfad befindet und den Austausch der SDP-Daten (Session Description Protocol) verfolgt. Anhand dieser Daten steuert der Server über das MIDCOM-Protokoll die Middlebox (NAT-Gateway, Firewall), die die Zuordnungen in die NAT-Tabelle einträgt und die entsprechenden Ports öffnet. In der folgenden Abbildung ist die MIDCOM-Architektur skizziert.

Abbildung: Darstellung der MIDCOM-Architektur

Da der Steuerungsserver selbst mit dem Internet kommunizieren muss, ist dieser Server ebenfalls durch eine Firewall zu schützen. Ein erfolgreicher Angriff auf den Steuerungsserver ermöglicht unter Umständen weitere Angriffe, insbesondere auf die von ihm kontrollierte Middlebox (NAT-Gateway, Firewall). Dies kann weitere erhebliche Gefährdungen nach sich ziehen.

Session Border Controller

Da sich MIDCOM noch im Entwurfsstadium befindet, haben Hersteller begonnen, proprietäre Lösungen auf den Markt zu bringen, die die NAT- und Firewall-Problematik lösen. Diese Session Border Controller bieten häufig Zusatzfunktionen, wie beispielsweise die Überwachung von Service Level Agreements (SLA), Rufannahmesteuerung (Call Admission Control) und Gebührenermittlung (Billing). Die Systeme werden als Appliances oder Server angeboten. Die folgende Abbildung zeigt ein Beispiel des Einsatzes eines Session Border Controllers, der aus einem Signalisierungs- und einem RTP-Proxy besteht.Abbildung: Beispiel für den Einsatz eines Session Border Controllers

Sämtlicher Verkehr (Signalisierung und Medienstrom) läuft in diesem Beispiel über den Session Border Controller. Dem VoIP-Telefon B ist die tatsächliche IP-Adresse des VoIP-Telefons A nicht bekannt.

UPnP

UPnP (Universal Plug and Play) ist ein Industriestandard, der vor allem im Heimbereich immer größere Verbreitung findet. Mit der UPnP-Architektur soll die Vernetzung von PCs und Endgeräten (beispielsweise Drucker, Scanner, WLAN Access Points) vereinfacht werden. Durch UPnP können Applikationen die öffentliche IP-Adresse des NAT-Gateways lernen, die zu verwendenden NAT-Zuordnungen vorgeben und nach der Beendigung einer Sitzung wieder entfernen. Es kann auch eine so genannte Lease Time vorgegeben werden, die die Dauer der Gültigkeit einer NAT-Zuordnung festlegt. Werden mehrere NAT-Gateways hintereinander geschaltet, kann mit UPnP kein NAT-Durchgang erzielt werden.

STUN

Mit Hilfe von STUN (Simple Traversal of User Datagram Protocol (UDP) Through NATs) wird Endsystemen, die sich hinter einem NAT-Gateway befinden, ermöglicht, ihre öffentliche IP-Adresse zu ermitteln und die NAT-Zuordnung des Gateways zu lernen. Symmetric NAT wird von STUN jedoch nicht unterstützt. Die NAT-Zuordnungen werden bei VoIP im Signalisierungsprotokoll übertragen, so dass eingehende RTP-Ströme an die entsprechende NAT-Zuordnung adressiert werden, um so das VoIP-Telefon zu erreichen, das sich hinter dem NAT-Gateway befindet. Die STUN-Technologie wird bereits von vielen VoIP-Telefonen unterstützt und von den meisten VoIP-Providern angeboten.

TURN

TURN (Traversal Using Relay NAT) erlaubt Systemen hinter einem NAT-Gateway bzw. einer Firewall, eingehende TCP- und UDP-Verbindungen zu empfangen. Gleichzeitig wird verhindert, dass diese Möglichkeit für den Betrieb von öffentlich erreichbaren Servern, wie Webserver oder E-Mail-Server, genutzt werden kann, indem je Kombination aus IP-Adresse und Port nur eine Sitzung zu einem Peer erlaubt wird. Im Gegensatz zu STUN können mit TURN auch Systeme hinter symmetrischen NAT-Gateways eingehende Verbindungen empfangen. TURN ist ein einfaches Client/Server-Protokoll, wobei die Authentisierung auf der Basis von Passwörtern erfolgt.

ICE

Da bei TURN sämtliche Medienströme über den TURN-Server geführt werden, ist es sinnvoll, einen TURN-Server nur dann einzusetzen, wenn mit STUN der Empfang eingehender Verbindungen nicht möglich ist. ICE (Interactive Connectivity Establishment) stellt eine Methode für SIP dar, um einen NAT-Durchgang auf Grundlage mehrerer über SDP bekannt gegebener Adressen zu ermöglichen, wobei auf die Protokolle STUN, TURN, RSIP und MIDCOM zurückgegriffen wird. Es wird davon ausgegangen, dass einem Client mehrere Adressen (beispielsweise von STUN oder TURN gelernte Adressen) zur Verfügung stehen, über die er Medienströme empfangen kann. Da die Endsysteme nicht wissen, welche Adresse funktioniert, werden die Adressen nacheinander nach ihrer Priorität geprüft, wobei die Adresse mit der höchsten Priorität als erstes getestet wird. Die Prioritäten werden anhand der geringsten Kosten und dem Maximum an QoS (Quality of Service) festgelegt und dann nacheinander innerhalb des SDP aufgeführt. ICE ist für SIP konzipiert, funktioniert jedoch auch mit RTSP und H.323 und ermöglicht, dass ein Endgerät unabhängig von der NAT-Umgebung betrieben werden kann.

Wird das LAN über einen NAT-Gateway an das Internet angeschlossen, ist zu empfehlen, eine der vorgestellten Mechanismen auszuwählen. Die Entscheidung ist zu dokumentieren.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "VoIP" finden sich unter anderem in folgenden Veröffentlichungen:

[NITS80058] Security Considerations for Voice Over IP Systems

NIST Special Publication 800-5

[TL2103] Technische Leitlinie für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf

BSI-TL-02103 - Version 2.0, Bundesamt für Sicherheit in der Informationstechnik, 2014, https://www.bsi.bund.de/DE/Publikationen/TL-sichere-TK-Anlagen/TL02103_htm.html , zuletzt abgerufen am 05.10.2018

NET.4: Telekommunikation

Umsetzungshinweise zum Baustein NET.4.3 Faxgeräte und Faxserver

1 Beschreibung

1.1 Einleitung

Stand-Alone-Faxgeräte oder auch Faxserver sind seit langem ein fester Bestandteil der Standardausstattung der IT im Büroumfeld, auch wenn immer mehr Dokumente per E-Mail versendet werden. Oft werden nur noch ausgewählte Inhalte per Fax versendet, wenn der Versand per E-Mail nicht möglich ist. Dadurch, dass auch vertrauenswürdige Informationen und Inhalte per Fax versendet werden, können Faxgeräte auch als Angriffsweg genutzt werden.

Daher sollte für einen sicheren Einsatz von Faxgeräten, dem Schutzbedarf der jeweiligen Institution entsprechend angemessene Maßnahmen zur Sicherheit geplant und umgesetzt werden.

1.2 Lebenszyklus

Für Faxgeräte sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Beschaffung über den Betrieb bis zur Notfallvorsorge. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Beschaffung

Bei der Beschaffung von neuen Faxgeräten und Faxservern sollte im Vorfeld eine Anforderungsliste erstellt werden in der alle, an das Gerät benötigte Funktionen notiert werden. Nach diesen Kriterien sollten dann geeignete Faxgeräte und Faxserver beschafft werden (siehe NET.4.3.M6 *Beschaffung geeigneter Faxgeräte und Faxserver*).

Planung und Konzeption

Die beschafften Faxgeräte und Faxserver müssen geeignet aufgestellt werden (siehe NET.4.3.M1 *Geeignete Aufstellung eines Faxgerätes*). Um die korrekte Faxnutzung, die Einsatzart und den korrekten Umgang mit Faxein- und Faxausgängen festzulegen, sollte eine Sicherheitsrichtlinie erstellt werden (siehe NET.4.3.M4 *Erstellung einer Sicherheitsrichtlinie für die Faxnutzung*).

Umsetzung

Bei der Installation von Faxgeräten ist darauf zu achten, dass es unter den Gesichtspunkten der Nutzbarkeit, Bedienbarkeit und Verwendung zweckmäßig aufgestellt wird. Die Mitarbeiter, die das Gerät benutzen sollen, sind in seine Bedienung einzuweisen (siehe NET.4.3.M2 *Informationen für alle Mitarbeiter über die Faxnutzung*). Um Unregelmäßigkeiten bei der Übertragung festzustellen und schnellstmöglich handeln zu können, sollten die Sende- und Empfangsprotokolle regelmäßig ausgedruckt werden (siehe NET.4.3.M9 *Nutzung von Sende- und Empfangsprotokollen*). Faxsendungen können nur zugestellt werden, wenn das Faxgerät in Betrieb ist. Sollte dieses aufgrund von Überlastung nicht zur Verfügung stehen, können Faxsendungen nicht zugestellt werden und sich somit Geschäftsprozesse verzögern (siehe NET.4.3.M11 *Schutz vor Überlastung des Faxgerätes*). Um zu vermeiden, dass Unternehmen mit Werbe-Fax-Sendungen das Gerät überlasten, sollten Rufnummern gesperrt bzw. zugelassen werden (siehe NET.4.3.M12 *Sperren bestimmter Faxempfänger-Rufnummern und Absender-Rufnummern*).

Betrieb

Um einen sicheren Betrieb zu gewährleisten, sollten die Konfigurationsparameter und alle Änderungen an der Konfiguration dokumentiert werden (siehe NET.4.3.M3 *Sicherer Betrieb eines* Faxservers). Im laufenden Betrieb ist darauf zu achten, dass notwendige Verbrauchsgüter geeignet bevorratet werden, damit keine Nachrichten nur deshalb verloren gehen, weil zu einem bestimmten Zeitpunkt kein Papier oder kein Toner vorhanden ist (siehe NET.4.3.M5 *Ernennung eines Fax-Verantwortlichen*). In der Regel ist es zweckmäßig, alle Sendungen durch ein geeignetes Faxvorblatt zu kennzeichnen und leichter identifizierbar zu machen (siehe NET.4.3.M7 *Nutzung eines geeigneten Faxdeckblattes*). Durch regelmäßige Kontrollen der Sende- und Empfangsprotokolle lässt sich ein eventueller Missbrauch des Faxgeräts leichter aufdecken und eine gelegentliche Kontrolle programmierter Zieladressen hilft zu vermeiden, dass Sendungen versehentlich an den falschen Empfänger gehen (siehe NET.4.3.M10 *Kontrolle programmierbarer Zieladressen, Protokolle und Verteilerlisten*).

Aussonderung

Bei der Entsorgung von Verbrauchsgütern und Ersatzteilen ist zu beachten, dass bei bestimmten Geräten, Abbildungen gesendeter oder empfangener Faxsendungen auf Zwischenträgerfolien, Belichtungstrommeln oder auch auf Papier vorhanden sind, so dass diese Materialien nicht so entsorgt werden dürfen, dass später Unbefugte darauf zugreifen können (siehe NET.4.3.M8 *Geeignete Entsorgung von Fax-Verbrauchsgütern und -Ersatzteilen*).

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Faxgeräte und Faxserver" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

NET.4.3.M1 Geeignete Aufstellung eines Faxgerätes [Haustechnik]

Ein Faxgerät muss so aufgestellt werden, dass eingegangene Faxsendungen nicht von Unberechtigten eingesehen oder entnommen werden können. Daher sollte es in einem Bereich aufgestellt werden, der nicht frei öffentlich zugänglich ist. Eine Kontrolle des Zutritts zu diesem Bereich oder der Nutzung des Faxgerätes ist sinnvoll.

Sinnvollerweise kann dies durch die Aufstellung in einem ständig besetzten Raum (z. B. Geschäftszimmer, Sekretariat, Poststelle) erreicht werden. Außerhalb der Dienstzeiten oder bei Abwesenheit der berechtigten Benutzer muss das Gerät eingeschlossen werden (Raum oder Schrank).

NET.4.3.M2 Informationen für alle Mitarbeiter über die Faxnutzung [Informationssicherheitsbeauftragter (ISB)]

Alle Mitarbeiter sind auf die Besonderheiten der Informationsübermittlung per Fax hinzuweisen, außerdem sollten sie darüber informiert werden, dass die Rechtsverbindlichkeit einer Faxsendung stark eingeschränkt ist. Eine verständliche Bedienungsanleitung muss am Faxgerät zur Verfügung stehen. Die Benutzer sollten eine Kurzanleitung zur eingesetzten Faxclient-Software und des Faxserver erhalten. An jedem Faxgerät muss zudem eine Anweisung zur korrekten Faxnutzung ausliegen.

In der Anweisung sollten die folgenden Punkte enthalten:

- wer der Fax-Verantwortliche ist und damit für die manuelle Verteilung eingehender Faxsendungen und als Ansprechpartner in Fax-Problemfällen zuständig ist,
- wer das Faxgerät bzw. den Faxserver benutzen darf,
- dass ein einheitliches Faxdeckblatt benutzt werden soll,
- dass Faxgeräte mit Verschlüsselungsoption zum Übertragen von vertraulichen Informationen benutzt werden sollten, wenn diese zur Verfügung stehen,
- dass Einzelsendenachweise bzw. Übertragungsprotokolle für die korrekte Übertragung zu kontrollieren und diese den Unterlagen beizufügen und bei Bedarf zu archivieren sind,
- dass beim Einsatz eines Faxservers mit automatischer Eingangs-Fax-Verteilung für die Akten ein Ausdruck von Eingangs-Faxsendungen zu fertigen ist, bzw. diese elektronisch zu archivieren sind,
- dass bei Ausgangsfaxen, die über einen Faxserver versendet werden, für die Papierakten ein Ausdruck zu erstellen ist bzw. diese elektronisch zu archivieren sind sowie
- dass die Adressbücher und Verteillisten regelmäßig kontrolliert werden, damit die Faxe nicht versehentlich an falsche Empfänger gesendet werden.

NET.4.3.M3 Sicherer Betrieb eines Faxservers [IT-Betrieb]

Der sichere Betrieb eines Faxservers setzt voraus, dass sowohl die lokale Kommunikation als auch die Kommunikation auf Seiten des öffentlichen Netzes abgesichert wird. Eingehende Faxsendungen nimmt der Faxserver von anderen Faxservern oder Faxgeräten entgegen und leitet sie, wenn die Funktion des automatischen Fax-Routing aktiviert ist, an die angeschlossenen Benutzer weiter. Ausgehende Faxsendungen der angeschlossenen Benutzer werden vom Faxserver entgegengenommen und an den Empfänger weitergeleitet. Der Faxserver muss zudem sicherstellen, dass lokale Faxsendungen, d. h. Faxsendungen von einem Arbeitsplatz zu einem anderen innerhalb der gleichen Organisation(seinheit), nur intern und nicht über das öffentliche Netz weitergeleitet werden.

Zum sicheren Betrieb eines Faxservers ist es u. a. erforderlich, dass nach der Beschaffung und Installation die Konfiguration des Betriebssystems und der Faxserver-Applikation ausgiebig getestet wird. Auf evtl. auftretende Fehlermeldungen ist, soweit dies möglich ist, mit Änderungen an der Konfiguration zu reagieren. An die Testphase sollte sich ein Pilotversuch anschließen. Erst wenn der Faxserver auch in dieser Phase fehlerfrei arbeitet, sollte er für den Wirkbetrieb freigegeben werden. Die Konfigurationsparameter sollten, ebenso wie alle Änderungen an der Konfiguration, sorgfältig dokumentiert werden.

Faxserver speichern alle eingehenden und ausgehenden Faxsendungen. Die Dauer der Speicherung hängt von den Leistungsmerkmalen der Faxserver-Applikation und der Konfiguration ab. So ist es z. B. möglich, dass ausgehende Faxsendungen nur bis zur Erledigung des Sendeauftrages zwischengespeichert und dann gelöscht werden. Ebenso kann es sein, dass eingehende Faxsendungen nur bis zur Weiterleitung an den Empfänger zwischengespeichert werden und anschließend gelöscht werden. Denkbar ist aber auch, dass grundsätzlich alle ein- und ausgehenden Faxsendungen auf dem Faxserver solange gespeichert werden, bis die Sendungen durch den jeweiligen Benutzer oder durch den Fax-Verantwortlichen bzw. den IT-Betrieb gelöscht werden. Die Löschung kann bei einigen Faxservern auch automatisch nach einer gewissen Zeitspanne erfolgen. So können z. B. alle Faxsendungen, die älter als 3 Monate sind, automatisch gelöscht werden. In Abhängigkeit vom Einsatzkonzept sind Regelungen für die Löschung von Faxdaten auf dem Faxserver zu treffen. Gleichzeitig ist zu regeln, wo und in welchem Umfang die Faxdaten archiviert werden sollten. Generell sollten Faxdaten nicht länger als unbedingt nötig auf dem Faxserver verbleiben. Auf Faxservern können oftmals an Benutzer und Benutzergruppen folgende Berechtigungen für eingehende Faxsendungen vergeben werden:

- lesen,
- weiterleiten sowie
- löschen.

Für ausgehende Faxsendungen können oftmals folgende Rechte vergeben werden:

- senden,
- anhalten,
- löschen sowie
- ändern der Sendeoptionen.

Die Berechtigungen sind gemäß den Festlegungen in der Sicherheitsrichtlinie zu vergeben (siehe auch NET.4.3.M4 *Erstellung einer Sicherheitsrichtlinie für die Faxnutzung*).

Sofern nicht durch technische Maßnahmen sichergestellt wird, dass Faxsendungen sofort weitergeleitet werden, ist zudem durch die Vergabe entsprechender Zugriffsrechte sicherzustellen, dass nur berechtigte Benutzer auf die entsprechenden "Postfächer" auf dem Server zugreifen können.

Generell sollte ein Zugriff auf temporäre Bereiche, in denen die Faxserver-Applikation Faxsendungen vor Abgang beziehungsweise vor Verteilung an den Empfänger zwischenspeichert, nur privilegierten Benutzern und dem IT-Betrieb vorbehalten bleiben.

Regelmäßig sind die Verbindungen des Faxservers mit der Telekommunikationsanlage bzw. mit dem öffentlichen Telefonnetz auf Funktion zu überprüfen. Sofern der Faxserver mit internen Kommunikationssystemen, wie z. B. einem E-Mail-System oder einem Workflow-System, zusammenarbeitet, ist ebenfalls regelmäßig die Funktion dieser Verbindungen zu überprüfen. Vorbehalte gegen den Einsatz eines Faxservers bestehen häufig aufgrund der Tatsache, dass dabei ein IT-System, das in das LAN integriert ist, über das öffentliche Telekommunikationsnetz erreicht werden kann. Durch sorgfältige Auswahl und Konfiguration von Kommunikationskarten, Betriebssystem und Faxserver-Applikation sowie durch eine sichere netztopologische Anordnung des Servers kann die Gefahr eines Einbruchs in das Netz bzw. in den Faxserver bis auf ein geringes Restrisiko minimiert werden.

Die Leistungsmerkmale von aktiven ISDN-Karten, die nicht zum Empfang und Senden von Faxen notwendig sind, sollten deaktivert werden. Sofern dedizierte Fax-Karten eingesetzt werden, sind auch zunächst die entsprechenden Leistungsmerkmale genau zu untersuchen. Auch hier gilt, dass nicht benötigte Merkmale, soweit dies möglich ist, abzuschalten sind.

Der Faxserver sollte keine anderen Dienste als den Faxdienst anbieten. Insbesondere sollte ein Faxserver nicht gleichzeitig als Daten-, Drucker-, E-Mail- oder Internet-Server bzw. als Remote-Access-Rechner verwendet werden. Um einem Einbruch über das Telekommunikationsnetz entgegenzuwirken, muss das Betriebssystem so "schlank" wie möglich installiert werden. Dies bedeutet, dass auf die Installation von für den Betrieb nicht zwingend notwendigen Diensten und Protokollen verzichtet wird. Hierzu ein Beispiel: Wenn auf einem Faxserver der Telnet-Dienst nicht gestartet ist, kann auch kein entsprechender Angriff zum Erfolg führen. Bei der Festlegung der benötigten Dienste und Protokolle darf nie vergessen werden, dass Gefährdungen häufig erst durch die Kombination von verschiedenen Diensten und Protokollen entstehen.

Die sichere netztopologische Anordnung des Faxserver ist unter anderem davon abhängig, ob und ggf. welche Art von Firewall in der Institution eingesetzt ist. Ein Faxserver hat jeweils mindestens eine Schnittstelle zum Telekommunikationsnetz und zum LAN. Der Faxserver sollte im Netz so angeordnet werden, dass im Falle eines erfolgreichen Angriffs auf den Faxserver nicht in das gesamte Netz eingebrochen werden kann. Andererseits sollte es auch nicht möglich sein, den Faxserver von innerhalb des Netzes aus erfolgreich zu attackieren. Denkbar wäre hier z. B. ein Angriff eines Außentäters aus dem Internet. Gelingt solch ein Angriff, so ist der Täter in der Lage, über den Faxserver der angegriffenen Institution Fax-Dokumente zu versenden. Dies kostet Gebühren und, was ggf. noch schlimmer ist, führt unter Umständen zu Ansehensverlust. Auch ist ein Angreifer im Falle eines erfolgreichen Angriffs in der Lage, unbefugt Kenntnis von den auf dem Faxserver (zwischen-) gespeicherten Faxsendungen zu nehmen. Angriffe eines Innentäters über das LAN sind in vergleichbarer Weise denkbar. Da ein Faxserver meistens nicht die einzige IT-Komponente mit Anschluss an ein externes Netz ist, ist in der Regel zum Schutz des internen Netzes ohnehin eine Abschottung gegenüber externen Netzen vorhanden (siehe auch Baustein *NET.3.2 Firewall*).

Sofern als Internet-Firewall ein Screened Subnet vorhanden ist, sollte der Faxserver zwischen dem inneren Paketfilter und dem Application Gateway (siehe Abbildung "Einbindung eines Faxserver in ein Firewall-System") eingebunden werden. Die Schutzwirkung gegenüber Angriffen aus dem unsicheren Netz ist durch den Application Gateway und den äußeren Paketfilter hinreichend groß. Gegen Angriffe aus dem internen Netz wird der Faxserver durch den inneren Paketfilter geschützt.

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich NET.4.3 *Faxgerät*.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Faxgeräte und Faxserver".

NET.4.3.M4 Erstellung einer Sicherheitsrichtlinie für die Faxnutzung [Informationssicherheitsbeauftragter (ISB)]

Vor der Installation, Konfiguration und Freigabe von Faxgeräten sollte zunächst eine Sicherheitsrichtlinie für die Faxnutzung festgelegt werden. Folgende Punkte werden üblicherweise mit solch einer Sicherheitsrichtlinie geregelt:

Einsatzkonzept

Bevor ein Faxserver für die Nutzung freigegeben wird, muss zunächst festgelegt werden, in welcher Einsatzart das System betrieben werden soll. So ist z. B. denkbar, dass ein Faxserver nur dazu dient, Faxe über das LAN entgegenzunehmen und dann nach außen zu versenden. Ein Faxserver kann aber auch von außen eingehende Faxsendungen entgegennehmen. In diesem Fall muss festgelegt werden, wie die eingehenden Faxsendungen an die Empfänger weitergeleitet werden. Die erste Möglichkeit besteht dabei in der Weiterleitung durch den Faxserver selbst, ggf. mit Anbindung an bereits bestehende E-Mail oder Workflow-Systeme. Eine andere Möglichkeit ist die manuelle Weiterleitung der eingehenden Faxsendungen durch den Fax-Verantwortlichen. Hier besteht einmal die Möglichkeit der Weiterleitung per E-Mail. Denkbar ist aber auch, dass die Poststelle eingehende Faxe ausdruckt und diese Ausdrucke an den Empfänger weiterleitet.

Integration in den Geschäftsablauf

Von der Betriebsart hängt auch ab, wie bei Benutzung eines Faxservers versandte oder empfangene Faxe in den Geschäftsablauf integriert werden. Sofern der Fax-Verantwortliche alle Faxeingänge ausdruckt und die Ausdrucke an den jeweiligen Empfänger weiterleitet, entspricht dies dem Ablauf, wie er auch bei herkömmlichen Faxgeräten üblich ist. Werden aber Faxe direkt aus einer Applikation vom Arbeitsplatzrechner des Benutzers versandt oder werden Faxeingänge direkt vom Faxserver an den Empfänger übermittelt, unterscheiden sich diese Verfahren erheblich von denen bei der Benutzung herkömmlicher Faxgeräte. Daher sollte in diesem Fall in der Richtlinie für die Faxnutzung festgelegt werden, von welchen Faxeingängen und Faxausgängen Ausdrucke für die Akten gefertigt werden müssen.

Inhaltliche Restriktionen

Weiterhin sollte in der Sicherheitsrichtlinie festgelegt werden, welche Informationen überhaupt per Fax weitergegeben werden dürfen. Es sollte in der Sicherheitsrichtlinie zudem beschrieben werden, welche Kommunikationspartner welche Informationen erhalten dürfen.

Damit wird erreicht, dass der Empfänger auch die notwendigen Berechtigungen zum Weiterverarbeiten der Information besitzt. Beispielsweise kann festgelegt werden, dass Preislisten nur an Einkäufer oder Projektunterlagen nur an Projektbeteiligte per Fax versendet werden dürfen.

Notfallvorsorge und Ausfallsicherheit

Außerdem sollten in der Sicherheitsrichtlinie Aussagen zur Notfallvorsorge und zur Ausfallsicherheit des Faxbetriebes enthalten sein. Abhängig von den Anforderungen an den Wert Verfügbarkeit ist ggf. der Einsatz redundanter Faxserver sinnvoll. In diesen Bereich fallen auch Überlegungen an, ob für den Notfall noch herkömmliche Faxgeräte verfügbar gehalten werden.

Datensicherung

Der Faxserver sollte in das Datensicherungskonzept der Institution aufgenommen werden (siehe Baustein CON.3 *Datensicherungskonzept*). Insbesondere ist dabei festzulegen, wer für die Durchführung der Datensicherungen zuständig ist und was zu sichern ist. Gegenstand der Datensicherung können dabei die Software, Konfigurationsdaten, gespeicherte bzw. archivierte Faxdaten oder auch Protokolldateien sein. Außerdem sind Festlegungen hinsichtlich des Sicherungsintervalls und der Anzahl der aufzubewahrenden Generationen notwendig. Es muss festgelegt werden, wer für die Überprüfung der bei der Datensicherung anfallenden Protokolle zuständig ist. Schließlich sollten sowohl die Durchführung der Datensicherung als auch die Auswertung der Protokolle dokumentiert werden.

Schulung

Die Sicherheitsrichtlinie sollte zudem um ein institutionsweites Schulungskonzept ergänzt werden. Zunächst ist das Personal, dass das IT-System und die Faxserver-Applikation administriert, entsprechend zu schulen. Dann sollten die Benutzer für die Gefährdungen sensibilisiert werden, die durch einen Faxserver im Vergleich zu einem herkömmlichen Faxsystem entstehen (siehe Baustein ORP.3 *Sensibilisierung und Schulung*).

NET.4.3.M5 Ernennung eines Fax-Verantwortlichen [IT-Betrieb, Vorgesetzte]

Um den reibungslosen Betrieb des oder der Faxgeräte und Faxserver zu gewährleisten, muss ein Fax-Verantwortlicher benannt werden. Der Fax-Verantwortliche hat dabei diverse organisatorische und technische Aufgaben wahrzunehmen, die auch von der Betriebsart des Faxservers abhängen.

Der Fax-Verantwortlich muss außerdem mit den Verantwortlichen der sonstigen Kommunikationsdienste (insbesondere E-Mail und Telekommunikationsanlage) eng zusammenarbeiten.

Im Rahmen von Vertretungsregelungen ist sicherzustellen, dass der Vertreter des Fax-Verantwortliche, ebenso wie der Fax-Verantwortliche während der Arbeitszeit zu erreichen ist.

Typische Aufgaben des Fax-Verantwortlichen sind:

- Administration der Faxserver-Applikation. Dazu gehört:
  - Einrichtung neuer Benutzer,
  - Vergabe von Berechtigungen an Benutzer und Benutzergruppen,
  - Rücksetzen von Passwörtern,
  - Überprüfung der Kommunikationsverbindungen,
  - Auswertung der anfallenden Protokolle,
  - Anlaufstelle der Benutzer bei Problemen,
  - Pflege der zentralen Adressbücher und Verteilerlisten,
  - Durchführung von Datensicherungen, sofern dies nicht Aufgabe der Administration des Betriebssystems ist,

- Faxzustellung und Archivierung,
- Fehlerbehebung bei der Faxzustellung sowie
- Koordination der Zusammenarbeit mit TK-Anlagen- und E-Mail-Verantwortlichen.

Manuelle Weiterleitung von Faxeingängen

Sofern eingegangene Faxsendungen nicht automatisch an den Empfänger zugestellt werden, müssen diese durch den Fax-Verantwortlichen manuell weitergeleitet werden.

Dies kann z. B. in der Form erfolgen, dass durch den Fax-Verantwortlichen von den Faxeingängen ein Ausdruck gefertigt wird, der dann an den Empfänger auf dem üblichen Weg weitergeleitet wird. Dieses Verfahren unterscheidet sich nicht wesentlich von dem beim Einsatz eines herkömmlichen Faxgerätes. Denkbar ist allerdings, dass eingegangene Faxsendungen digital auf externen Datenträgern archiviert werden.

Automatische Weiterleitung von Faxeingängen

Bei der automatischen Weiterleitung von eingegangene Faxsendungen an den Empfänger (automatisches Fax-Routing) ist es ebenfalls möglich, dass durch den Fax-Verantwortlichen Ausdrucke zum Zwecke der Archivierung gefertigt werden. Auch hier besteht die Möglichkeit, eingehende Faxsendungen digital auf externen Datenträgern zu archivieren.

Sofern Faxsendungen nicht zugestellt werden können, sollte der Fax-Verantwortliche hiervon Kenntnis erlangen und versuchen, die Fehlerquelle zu beheben. Sofern die Zustellung endgültig scheitert, ist der Absender entsprechend zu informieren. Gründe dafür, dass Faxeingänge unzustellbar sind, können sein:

- Der Absender hat eine falsche Durchwahl benutzt.
- Der Empfänger ist nicht mehr Mitglied der Institution.
- Die automatische Weiterleitung von Faxeingängen erfolgt aufgrund der Absenderkennung und der Absender ist in der Institution noch nicht bekannt oder es existiert keine entsprechende Zuordnungsregel.

In all diesen Fällen muss von dem Fax-Verantwortlichen die Weiterleitung von Faxeingängen manuell erfolgen. Sofern Faxeingänge endgültig nicht zugestellt werden können, muss der Absender benachrichtigt werden.

Für jedes Faxgerät hat der Fax- Verantwortlicher, folgende Aufgaben zu übernehmen:

- Verteilung der eingehenden Faxsendungen an die Empfänger,
- Koordination der Versorgung des Faxgerätes mit notwendigen Verbrauchsgütern,
- geeignete Entsorgung von Fax-Verbrauchsgütern,
- Löschen von Restinformationen im Faxgerät vor Wartungs- und Reparaturarbeiten,
- Beaufsichtigung von Wartungs- und Reparaturarbeiten
- gelegentliche Kontrolle programmierter Zieladressen und Protokolle, insbesondere nach Wartungs- und Reparaturarbeiten sowie
- Ansprechpartner bei Problemen bei der Faxnutzung.

NET.4.3.M6 Beschaffung geeigneter Faxgeräte und Faxserver [Beschaffungsstelle, Informationssicherheitsbeauftragter (ISB)]

Bei Neuanschaffungen von Faxgeräten sollte darauf geachtet werden, dass übliche Standardsicherheitsfunktionen implementiert sind wie:

- Austausch einer Teilnehmerkennung,
- Sendebericht sowie
- Journalführung.

Unter Beachtung des Preis-/Leistungsverhältnisses sind darüber hinaus folgende zusätzliche Sicherheitsfunktionen zu begrüßen:

- passwortgeschützter Zugang,
- passwortgeschützter Pufferspeicher,
- Einrichten einer geschlossenen Benutzergruppe sowie
- Ausschließen bestimmter Faxanschlüsse von Versendung oder Empfang.

NET.4.3.M7 Geeignete Kennzeichnung ausgehender Faxsendungen [Benutzer]

Um Dokumente geordnet und nachvollziehbar per Fax auszutauschen, sollte ein standardisiertes Faxdeckblatt genutzt werden. Damit kann insbesondere geprüft werden, ob eine erhaltene Faxsendung vollständig empfangen und ausgedruckt wurde.

Das Faxdeckblatt sollte beinhalten:

- Name des Absenders und Institution (mit Telefonnummer und vollständiger Adresse),
- Name des Empfängers (mit Rufnummer des Faxgerätes und ggf. vollständiger Adresse),
- Datum
- Seitenanzahl sowie
- ggf. Dringlichkeitsvermerk (evtl. gestuft).

Die Bitte, fehlgeleitete Sendungen weiterzuleiten oder den Absender zu informieren, ist sinnvoll.

NET.4.3.M8 Geeignete Entsorgung von Fax-Verbrauchsgütern und -Ersatzteilen

Alle Fax-Verbrauchsgüter, aus denen Informationen über Faxdokumente gewonnen werden könnten, wie z. B. Zwischenträgerfolien oder fehlerhafte Ausdrucke, sollten vor der Entsorgung vernichtet oder durch eine zuverlässige Fachfirma entsorgt werden. Das Gleiche gilt beim Austausch informationstragender Ersatzteile, wie z. B. photo-elektrische Trommeln.

Wartungsfirmen, die Faxgeräte periodisch warten oder reparieren, sind auf eine entsprechende Handhabung zu verpflichten und zu kontrollieren.

NET.4.3.M9 Nutzung von Sende- und Empfangsprotokollen [Informationssicherheitsbeauftragter (ISB)]

Bei der Nutzung von Faxdiensten ist bei der Verwendung von Sende- und Empfangsprotokollen zwischen herkömmlichen Faxgeräten und Faxserver zu unterscheiden.

Einsatz eines herkömmlichen Faxgerätes

Listenmäßige Protokolle von Übertragungsvorgängen, die automatisch vom Faxgerät geführt werden (Kommunikationsjournal), sind regelmäßig auszudrucken. Es sollte festgelegt werden, wer diese Ausdrucke veranlasst, wo und wie lange sie aufbewahrt werden und in welcher Weise sie stichprobenartigen Prüfungen auf Unregelmäßigkeiten unterzogen werden. Auf die Erfordernisse des Bundesdatenschutzgesetzes (BDSG) ist Rücksicht zu nehmen. Insbesondere ist der Zugriff Unbefugter zu verhindern.

Eine weitere Kontrollmöglichkeit besteht, wenn das Faxgerät an eine moderne TK-Anlage angeschlossen ist. Dann ist es u. U. möglich, die Gebührendatensätze der Faxnummer in der TK-Anlage auszuwerten.

Einsatz eines Faxserver

Auch auf Faxservern ist es möglich, die Übertragungsvorgänge zu protokollieren. Diese Protokolle sollten regelmäßig ausgewertet und archiviert werden. Die Rahmenbedingungen und Zuständigkeiten für die Auswertung und Archivierung der Protokolle sollte festgelegt werden.

Der Fax-Verantwortliche ist für die Tätigkeiten zuständig, wie die Auswertung der Protokolle aber nur im Beisein eines Betriebs- oder Personalratsmitgliedes bzw. eines Angehörigen der Revision oder des Datenschutzes erfolgen darf. Auch hier gilt, dass die Erfordernisse des BDSG zu berücksichtigen sind und insbesondere der Zugriff Unbefugter zu verhindern ist.

NET.4.3.M10 Kontrolle programmierbarer Zieladressen, Protokolle und Verteilerlisten

Bei programmierbaren Kurzwahltasten oder Zieladressenspeicherung sollte regelmäßig überprüft werden, ob die gewünschte mit der einprogrammierten Faxnummer übereinstimmt und ob sie noch benötigt wird. Damit wird verhindert, dass eine von einem Unberechtigten eingegebene fremde Faxnummer längere Zeit statt der korrekten Nummer genutzt wird. Außerdem werden eventuell übersehene Änderungen der gewünschten Zielrufnummern frühzeitig entdeckt.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

NET.4.3.M11 Schutz vor Überlastung des Faxgerätes [IT-Betrieb] (A)

Ein Faxserver kann sowohl durch eingehende als auch durch ausgehende Faxsendungen überlastet werden. Eine Überlastung des Faxservers kann dazu führen, dass zeitweilig keine weiteren Faxsendungen mehr empfangen oder versandt werden können. Es ist auch denkbar, dass im Falle der Überlastung das Betriebssystem oder die Faxserver-Applikation abstürzt und der Faxserver vorübergehend gar nicht mehr verfügbar ist.

Eine Art der Überlastung des Faxservers liegt vor, wenn alle Kanäle, die durch die Kommunikationskarten bereitgestellt werden, durch eingehende und ausgehende Faxsendungen blockiert werden. Folge ist, dass weitere Faxe erst dann wieder empfangen oder gesendet werden können, wenn ein Kanal frei wird. Dieser Effekt tritt auch auf, wenn alle von der Telekommunikationsgesellschaft zur Verfügung gestellten Leitungen durch eingehende und ausgehende Faxsendungen belegt werden.

Vor der Beschaffung eines oder mehrerer Faxserver ist zunächst das voraussichtliche Faxvolumen abzuschätzen. Sodann sind ausreichend leistungsfähige Komponenten zu beschaffen. Außerdem sollte darauf geachtet werden, dass genügend Telekommunikationsleitungen zur Verfügung stehen.

Außerdem sollten die Protokolle des Faxservers regelmäßig kontrolliert werden, um feststellen zu können, ob der Server zu bestimmten Zeiten überlastet oder die Grenze der Belastbarkeit erreicht wird.

Eine Überlastung des Faxservers kann dadurch erfolgen, dass intern versucht wird, eine große Anzahl von Faxen zu versenden. Unter ungünstigen Umständen kann dies zum Absturz der Faxserver-Applikation oder des Betriebssystems führen. Auslöser kann z. B. eine sehr große Anzahl von Serienfax-Sendungen sein. Es sollte daher schon in der Test- oder in der Pilotierungsphase versucht werden, die Belastungsgrenze zu ermitteln. Um diese Belastungsgrenze nicht zu überschreiten, sollte den Benutzern z. B. mittels geeigneter Dienstanweisung der maximale Umfang einer Serien-Faxsendung vorgegeben werden. Umfangreiche Serien-Faxsendungen sind dann auf mehrere Sendungen aufzuteilen. Zu Zeiten hoher Belastung des Faxservers sollte durch eine entsprechende Dienstanweisung oder durch eine entsprechende Vergabe von Berechtigungen am Faxserver sichergestellt werden, dass Faxe nur in dringenden Fällen gesendet werden. Sinnvoll kann auch die Vorgabe sein, Faxe möglichst nur zeitversetzt in der Nacht zu senden, was zudem noch Gebühren spart.

Wenn festgestellt wird, dass der Faxserver immer durch die gleichen Senderrufnummern mittels einer entsprechenden Anzahl von Faxsendungen zu ganz bestimmten Zeiten blockiert wird, ist zunächst zu ermitteln, wer die Absender sind und um welche Art von Faxsendungen es sich handelt. Sofern die Faxsendungen von der Institution benötigt werden, kann versucht werden, mit den Absendern Zeiten auszuhandeln, in denen problemlos Faxsendungen entgegengenommen werden können. Sofern die Faxsendungen nicht benötigt werden (z. B. nicht angeforderte Werbe-Faxsendungen), kann versucht werden, die Absenderrufnummern über die Faxserver-Applikation oder über die Telekommunikationsanlage zu sperren. Dies ist aber nur möglich, sofern die Absenderkennung (Caller Sender Identification) nicht verschleiert bzw. bei Verwendung von die Rufnummernübermittlung seitens des Absenders nicht unterdrückt wurde. Sofern die Faxnummer des Absenders nicht zu ermitteln sind, bleibt nur noch die Möglichkeit, die vorhandenen Kapazitäten, wie oben beschrieben, zu erweitern.

Problematisch kann auch die Festplattenkapazität eines Faxservers sein. Dabei ist die Gefahr, die Festplattenkapazität durch einen Angriff von außen gezielt zu erschöpfen, eher gering. Eine gefaxte A4 Seite ist ca. 70 kB groß. Geht man von heute üblichen Festplattengrößen von mehreren Giga- bis Terabyte aus, so ist auch angesichts der anfallenden Gebühren ein entsprechender Angriff eher unwahrscheinlich. Grundsätzlich werden alle eingehenden und ausgehenden Faxsendungen auf der Festplatte des Faxservers (zwischen-) gespeichert. Der weitere Ablauf hängt dann von der Faxserver-Applikation und ggf. auch von der Konfiguration ab. So ist z. B. denkbar, dass alle Faxsendungen dauerhaft auf der Festplatte des Faxservers gespeichert bzw. archiviert werden. Bei dieser Betriebsart kann, abhängig vom Faxvolumen, sehr schnell die Festplattenkapazität erschöpft werden. Es sollte in diesem Fall sichergestellt werden, dass Ausgangs-Faxsendungen und bereits gelesene Eingangs-Fax-Sendungen möglichst zeitnah auf externe Datenträger archiviert und auf dem Faxserver gelöscht werden. Dazu sollte der den Benutzern auf dem Faxserver zur Verfügung gestellte Speicherplatz begrenzt werden. Außerdem sollte z. B. durch Dienstanweisung sichergestellt werden, dass Faxsendungen, die nicht mehr benötigt werden, zu löschen sind. Dies gilt insbesondere für unverlangt erhaltene Werbe-Fax-Sendungen. Durch den Fax-Verantwortlichen ist regelmäßig der freie Speicherplatz auf der Festplatte des Faxservers zu überprüfen.

NET.4.3.M12 Sperren bestimmter Faxempfänger-Rufnummern und Absender-Faxnummern (CIA)

Besteht die Notwendigkeit, das zufällige oder absichtliche Versenden von Informationen oder Unterlagen per Fax an eine nicht gewünschte Empfängerrufnummer zu verhindern, so bietet die heutige Technik dazu mindestens drei Lösungen:

Bei einigen Faxgeräten bzw. Faxservern ist es möglich, die Versendung von Faxen an bestimmte Faxempfänger-Rufnummern zu unterbinden (positiver Ausschluss) oder alternativ alle Empfängerrufnummern außer einigen ausgewählten Rufnummern zu sperren (negativer Ausschluss).

Die gleiche Art der Berechtigungsvergabe kann auch in modernen TK-Anlagen erreicht werden, vorausgesetzt, das Faxgerät ist über eine solche Anlage ans Telefonnetz angeschlossen.

Wenn ein Faxgerät oder die TK-Anlage eine solche Möglichkeit nicht bietet, so kann zum Beispiel vom Betreiber des öffentlichen Netzes eine Zusatzeinrichtung gemietet werden, die den Verbindungsaufbau zu bestimmten Rufnummern (positiver und negativer Ausschluss) verhindert.

Netzbetreiber können entsprechende Rufnummern ebenfalls unterbinden.

Damit bestimmte Faxsendungen das eigene Faxgerät nicht blockieren können, z. B. bei Überlastung durch spezielle Faxaktionen von Werbeagenturen, kann ggf. eine Sperre bestimmter Sender-Faxnummern realisiert werden.

Einige moderne Faxgeräte (Gruppe 4) sind in der Lage, die übermittelte Senderrufnummer auszuwerten und den Empfang von Faxsendungen ausgewählter Rufnummern zu verweigern. Dies gilt auch für einige Faxserver, sofern diese an das -Netz angeschlossen sind. Daneben kann auch die Faxabsenderkennung (Call Subscriber ID) zur Auswertung herangezogen werden. Nachteilig ist allerdings, dass der Faxabsender die Rufnummernübermittlung unterdrücken und die übermittelte Rufnummer sowie die Absenderkennung manipulieren kann.

Eine weitere Möglichkeit besteht darin, dass beim Telefon-Netzbetreiber kostenpflichtig eine geschlossene Benutzergruppe eingerichtet wird, wenn Empfänger und Sender an digitalen Vermittlungsstellen angeschlossen sind. Teilweise wird diese Möglichkeit auch von modernen TK-Anlagen angeboten.

NET.4.3.M13 Festlegung berechtigter Faxbediener [Benutzer] (A)

Die Berechtigung zur Bedienung des Faxgerätes sollte auf einen ausgewählten Kreis zuverlässiger Mitarbeiter beschränkt werden. Diese Mitarbeiter sind in die korrekte Handhabung des Gerätes einzuweisen und mit den erforderlichen Sicherheitsmaßnahmen vertraut zu machen. Jeder berechtigte Benutzer sollte darüber unterrichtet werden, wer das Gerät bedienen darf und wer der Fax-Verantwortliche ist. Darüber hinaus sollte am Faxgerät eine verständliche Bedienungsanleitung ausliegen.

Durch die Einschränkung des Faxbedienerkreises auf die für den operativen Einsatz notwendige Mindestzahl wird erreicht, dass die Anzahl der Personen, die eingehende Faxsendungen mitlesen können, begrenzt ist.

NET.4.3.M14 Fertigung von Kopien eingehender Faxsendungen [Benutzer] (A)

Ein Fax auf Thermopapier kann nach einiger Zeit stark verblassen oder schwarz werden. Daher sollten von Faxen auf Thermopapier, deren Informationsgehalt länger benötigt wird, Kopien auf Normalpapier erstellt werden.

NET.4.3.M15 Ankündigung und Rückversicherung im Umgang mit Faxsendungen [Benutzer] (CIA)

Wichtige Faxsendungen mit vertraulichen Inhalten (z. B. Angebote) oder termingebundene Faxsendungen sollten vor Absendung beim Empfänger (zum Beispiel per Telefon) angemeldet werden. Der Empfänger hat dann die Möglichkeit, zum entsprechenden Faxgerät zu gehen und dort das für ihn eingehende Fax direkt entgegenzunehmen, so dass kein anderer das Fax entnehmen kann.

Die Benutzer sollten von Vorgesetzten angewiesen werden, vertrauliche oder wichtige Faxsendungen anzukündigen.

Ebenso sollte beim Empfänger nachgefragt werden, ob die Faxsendung vollständig empfangen, ausgedruckt und ihm übergeben wurde. Die Mitarbeiter sollten hierzu angewiesen werden. Die telefonische Bestätigung kann auch auf dem Faxdeckblatt erbeten werden.

Hilfreich sind in diesem Zusammenhang die von einigen Faxgeräten als Leistungsmerkmal angebotenen Einzelsendeberichte, die Fehler beim Versand anzeigen können.

Bei wichtigen oder ungewöhnlichen Faxsendungen sollte in Erwägung gezogen werden, sich beim Faxabsender zu vergewissern, dass das Fax von ihm abgesandt und nicht von einem Dritten gefälscht wurde. Dies kann auf einfache Weise durch einen telefonischen Rückruf erfolgen. Die erforderliche Rufnummer ist im Allgemeinen auf dem Faxdeckblatt dokumentiert, sollte aber, da sie gefälscht sein könnte, verifiziert werden.

3 Weiterführende Informationen

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Faxgeräte und Faxserver" finden sich unter anderem in folgenden Veröffentlichungen:

[FAXNRW] Datensicherheit beim Telefaxverkehr

Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/Kommunikation/Inhalt/070402_Datensicherheit_beim_Telefaxverkehr/Datensicherheit_beim_Telefaxverkehr.php zuletzt abgerufen: 20.07.2018

Umsetzungshinweise für die Bausteinschicht INF

INF: Infrastruktur

Umsetzungshinweise zum Baustein INF.1 Allgemeines Gebäude

1 Beschreibung

1.1 Einleitung

Gebäude bilden den äußeren physischen Rahmen für die Durchführung von Geschäftsprozessen. Ein Gebäude umfasst die stationären Arbeitsplätze, die verarbeiteten Informationen sowie die aufgestellte Informationstechnik und gewährleistet für diese somit einen äußeren Schutz. Zudem ermöglichen die Infrastruktureinrichtungen eines Gebäudes häufig erst die Durchführung von Geschäftsprozessen und den IT-Betrieb. Daher ist nicht nur das Bauwerk an sich, also Wände, Decken, Böden, Dach, Fenster sowie Türen zu betrachten, sondern auch alle gebäudeweiten Infrastruktur- und Versorgungseinrichtungen wie Strom, Wasser, Gas, Heizung und Kühlung. Aufbauend auf den Schutzzielen müssen die verschiedenen Aufgaben und Sicherheitsmaßnahmen abgestimmt werden.

Betrachtet wird ein Gebäude, das von einer oder mehreren Organisationseinheiten einer Institution genutzt wird. Diese können durchaus unterschiedliche Sicherheitsansprüche haben. Zudem muss in alle Überlegungen einfließen, dass ein Gebäude fast immer auch von Institutionsfremden (Bürgern, Kunden, Lieferanten) betreten werden kann und soll. Wenn ein Gebäude von verschiedenen Parteien in derartiger Weise genutzt wird, so müssen Gestaltung und Ausstattung des Gebäudes und das Nutzungskonzept für das Gebäude zueinander passen. Es soll eine optimale Umgebung für die im Gebäude tätigen Menschen sichergestellt werden. Unberechtigte sollen dort keinen Zutritt erhalten, wo sie die Sicherheit beeinträchtigen könnten und die im Gebäude stationierte Technik soll sicher und effizient betrieben werden können.

1.2 Lebenszyklus

Bei der Absicherung eines Gebäudes müssen technische und nicht-technische Sicherheitsaspekte bei der Planung und Nutzung umgesetzt werden. Dabei muss der gesamte Lebenszyklus von Gebäuden betrachtet werden, beginnend von der Erstellung eines Anforderungskataloges, über Konzeption, Einrichtung, Nutzung bis hin zu Umbauten oder Auszug.

Die Verkabelung in einem Gebäude wird in den Bausteinen INF.3 Elektrotechnische Verkabelung und INF.4 IT-Verkabelung gesondert betrachtet, spezielle Räumlichkeiten wie Serverräume oder Archivräume in den jeweiligen Bausteinen der Schicht INF.

Bei der Nutzung von Gebäuden für den Geschäftsbetrieb von Behörden oder Unternehmen sind hinsichtlich der Informationssicherheit bei bestimmten Maßnahmen unterschiedliche Vorgehensweisen zu verfolgen. Bei einem Neubau können erforderliche Maßnahmen zu einem großen Teil schon in der Planungsphase durchgeführt werden.

Wenn es sich dagegen um eine Anmietung oder die Nutzung eines bestehenden Gebäudes handelt, was eventuell mit Erweiterungs- und Umbaumaßnahmen verbunden sein kann, sind die Möglichkeiten zur Realisierung einer adäquaten Informationssicherheit oft viel stärker eingeschränkt.

Planung und Konzeption

Die geplante Nutzung eines Gebäudes und der Schutzbedarf der dort betriebenen Geschäftsprozesse bestimmen, wie das Gebäude zu gestalten und unter Sicherheitsaspekten auszustatten ist. Beginnend bei einer Bewertung der Lage und Art des Grundstücks ist zu prüfen, ob das Gebäude dem vorgesehenen Zweck angemessen ist oder angemessen gestaltet werden kann.

Empfehlenswert bei der weiteren Planung oder Prüfung eines Bestandsgebäudes ist die Bildung eines Zonenmodells (siehe INF.1.M 23 Bildung von Sicherheitszonen), anhand dessen dann eine am Schutzbedarf orientierte Planung der Nutzung des Gebäudes vorgenommen werden kann (siehe INF.1.M1 Planung der Gebäudenutzung). Daraus werden dann die Organisation von Zutrittsberechtigungen, beschrieben in Kapitel 3.1 Zutrittskontrollsystem und Berechtigungsmanagement, die Ausführung von Türen und Fenstern und die weiteren Maßnahmen zur Sicherung und Überwachung abgeleitet.

Bei der Raumbelegungsplanung ist INF.1.M 3 Einhaltung von Brandschutzvorschriften sowie, im Falle einer Nutzung eines bestehenden Gebäudes, INF.1.M 34 Anordnung schützenswerter Gebäudeteile anzuwenden. Stets erforderlich ist auch, entsprechend der geplanten Raumnutzung, die zu erwartenden elektrischen Anschlusswerte zu bestimmen (siehe INF.1.M 2 Angepasste Aufteilung der Stromkreise).

Beschaffung

Sowohl bei der Auswahl eines Standortes für einen Neubau, als auch bei der Bewertung einer Bestandsimmobilie sind die Maßnahmen INF.1.M 25 Geeignete Standortauswahl und INF.1.M 31 Auswahl eines geeigneten Gebäudes in Betracht zu ziehen.

Bauphase und Vorbereitung für Nutzung

Während der Bauphase sind alle in der Planungsphase als erforderlich bewerteten Schutzmaßnahmen umzusetzen. In der Bauphase sind in jedem Fall die Maßnahmen INF.1.M 10 Einhaltung einschlägiger Normen und Vorschriften und INF.1.M 3 Einhaltung von Brandschutzvorschriften anzuwenden. INF.1.M 13 Regelungen für Zutritt zu Verteilern sowie INF.1.M 12 Schlüsselverwaltung sind spätestens beim Einzug in ein Gebäude festzulegen. Ebenso ist eine Zutrittsregelung und ein Zutrittskontrollkonzept gemäß INF.1.M 7 Zutrittsregelung und -kontrolle erforderlich.

Gebäudenutzung

Während der Gebäudenutzungsphase ist insbesondere die regelmäßige Anwendung von INF.1.M 18 Brandschutzbegehungen vorzusehen, womit die Einhaltung der vorgegebenen Vorschriften zum Brandschutz überwacht wird. Durch die Anwendung und regelmäßige Überwachung der Maßnahme INF.1.M 6 Geschlossene Fenster und Türen ist sicherzustellen, dass sich nur befugte Personen im Gebäude aufhalten und dass zumindest eine elementare Vorsorge gegen Einbrüche getroffen wird.

Notfallvorsorge

Um für den Notfall gerüstet zu sein, ist ein Alarmierungsplan zu erstellen, und in regelmäßigen Abständen sind auch Notfallübungen durchzuführen, da andernfalls zu erwarten ist, dass bei einem Notfall falsche Entscheidungen getroffen werden oder Unklarheit über die notwendigen Operationen herrscht (siehe INF.1.M 20 Alarmierungsplan und Brandschutzübungen).

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Allgemeines Gebäude" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

INF.1.M1 Planung der Gebäudeabsicherung [Informationssicherheitsbeauftragter (ISB), Planer]

Um praxistaugliche und wirtschaftliche Sicherheitsmaßnahmen für die Nutzung eines Gebäudes zu erarbeiten, sind der Schutzbedarf der dort betriebenen Geschäftsprozesse und die grundsätzlichen Schutzziele, die sich häufig aus der Geschäftstätigkeit ergeben, zu ermitteln. Über den selbstverständlichen Schutz von Personen im Gebäude und dem Schutz der Wirtschaftsgüter sind im Rahmen der Informationssicherheit besonders die Schutzbelange der IT, also der Hardware und der Software, zu beachten. Dabei sind neben der klassischen IT-Hardware die Bereiche der gesamten Support-Technik, also Stromversorgung, Kühlung/Klimatisierung etc. zu berücksichtigen.

Bei einem Gebäude müssen viele verschiedene Sicherheitsaspekte beachtet werden, von Brandschutz über Elektrik bis hin zur Zutrittskontrolle. Je nach Größe der Institution und der Gebäude kann es hierfür unterschiedliche Zuständige geben. Daher müssen die verschiedenen Rollen und Aufgaben abgestimmt werden. Die zuständigen Personen sollten sich untereinander abstimmen, um aufbauend auf den Schutzzielen angemessene Sicherheitsmaßnahmen für die verschiedenen Bereiche auszuwählen.

Es ist bewährte Praxis, zur Planung von Gebäuden zunächst Zonen zu betrachten (siehe INF.1.M 23 Bildung von Sicherheitszonen). Viele Schutzziele lassen sich dadurch erreichen, dass es weder nötig noch möglich ist, von einer Zone mit geringem Sicherheitsniveau direkt in eine mit höherem Sicherheitsniveau zu gelangen. Dabei sollte zunächst die räumliche Aufteilung mit der vorgesehenen Nutzung des Gebäudes abgestimmt werden (siehe INF.1.M 1.13 Anordnung schützenswerter Gebäudeteile). Zwischen verschiedenen Sicherheitszonen sollten klar erkennbare und möglichst einfach abzusichernde Übergänge geschaffen werden. Zulässige Übergänge zwischen den Zonen werden dann angepasst an den Schutzbedarf ausgeführt. Unzulässige Übergänge werden entweder unterbunden oder besonders abgesichert. So müssen Fluchttüren aus Sicherheitszonen mit höherem Sicherheitsniveau in den Außenbereich so gesichert werden, dass der unberechtigte Zutritt von außen nach innen verhindert wird. Fenster und Zugänge müssen entsprechend ihres Schutzbedarfs abgesichert sein (siehe INF.1.M 22 Sichere Türen und Fenster).

INF.1.M2 Angepasste Aufteilung der Stromkreise

Häufig wird schon bei der Erstinstallation dahingehend unsauber gearbeitet, dass eine der drei Außenleiter im 3-Phasen-Netz deutlich stärker mit Verbrauchern belegt und damit belastet wird, als die anderen beiden (Gefahr der Sternpunktverschiebung). Des weiteren stimmen erfahrungsgemäß nach einiger Zeit die Raumbelegung und die Anschlusswerte, für die eine Elektroinstallation ausgelegt wurde, nicht mehr mit den tatsächlichen Gegebenheiten überein. Es ist also unerlässlich, bei Änderungen der Raumnutzung und bei Änderungen und Ergänzungen der technischen Ausrüstung (IT, Klimageräte, Beleuchtung, etc.) die Elektroinstallation zu prüfen und gegebenenfalls anzupassen. Das kann in einfachen Fällen durch Umrangierung von Leitungen geschehen. Teilweise kann es aber auch erforderlich werden, zusätzliche oder vollkommen neue Einspeisungen, Leitungen, Verteiler etc. zu installieren.

Weitere Informationen zur IT-Verkabelung und der elektrotechnischen Verkabelung finden sich in den entsprechenden Bausteinen der Schicht INF.

INF.1.M3 Einhaltung von Brandschutzvorschriften

Die bestehenden Brandschutzvorschriften (z. B. nach der Norm DIN 4102 Brandverhalten von Baustoffen und Bauteilen) und die Auflagen der Bauaufsicht für Gebäude sind unbedingt einzuhalten. Die örtliche Feuerwehr sollte bei der Brandschutzplanung hinzugezogen werden.

Für Räume, in denen wichtige IT-Geräte und Datenträger (Server, Datensicherungen, etc.) untergebracht sind, sollten zudem die Regelungen der Norm EN 1047 Teil 2 beachtet werden. Ziel ist hier, durch besondere Maßnahmen wie dem Einbau von Türen mit Brand- und Rauchschutzqualität, der sorgfältigen Ausführung von Schottungen und eventuell sogar der Ertüchtigung von Wänden, die Wirkung eines Brandes auf die Inhalte solcher Räume möglichst gering zu halten.

Bei Besprechungs-, Schulungs- und Veranstaltungsräumen sind unter Umständen die entsprechenden Regelungen für den Brandschutz in Versammlungsstätten zu beachten. Da es hier je nach Nutzungsart unterschiedliche Zusatzforderungen wie beispielsweise hinsichtlich der Öffnungsart und -breite von Türen im Verlauf von Flucht- und Rettungswegen und Beschilderungen gibt, sollte auch hier bei der Planung die örtliche Feuerwehr befragt werden.

Es sollte eine Person benannt werden, die für die Einhaltung von Brandschutzvorschriften verantwortlich ist. Dies kann ein Brandschutzbeauftragter oder eine mit dem Aufgabengebiet betraute Person sein, die auch entsprechend geschult ist.

Es ist empfehlenswert, weitere Hinweise zum Brandschutz zu beachten, wie sie zum Beispiel in den Publikationen der VdS Schadenverhütung GmbH zu finden sind.

Besonders wichtig ist es, die Fluchtwege gut auszuschildern. Dafür sind die vorgeschriebenen Kennzeichen zu verwenden und die Vorschriften zu deren Anbringung einzuhalten. Die Fluchtwege müssen immer offen gehalten werden, das heißt insbesondere, dass sie nicht versperrt werden dürfen, z. B. durch im Flur abgestelltes Inventar oder indem die Fluchttüren abgeschlossen werden.

Brand- und Rauchschutztüren bieten nur im geschlossenen Zustand Schutz und dürfen deshalb keinesfalls durch Keile oder andere Vorrichtungen dauerhaft offen gehalten werden. Es dürfen keine Ausnahmen zugelassen werden.

Damit die Feuerwehr im Brandfall schnell mit der Brandbekämpfung beginnen kann, ist es wichtig, dass die Brandmeldezentrale, das Brandmeldetableau und die Einspeisepunkte für Löschwasser durch Beschilderung schnell gefunden werden können.

Zur Verwirklichung eines effizienten Brandschutzes ist die Zusammenarbeit aller zuständigen Verfahrensbeteiligten notwendig. Hierunter fallen die Funktionen des Brandschutzbeauftragten (Arbeitgeber ist für die Einhaltung der Brandschutzvorschriften verantwortlich), der Fachkraft für Arbeitssicherheit (in Deutschland erforderlich nach §§ 5, 6 Arbeitssicherheitsgesetz, diese ist zuständig für die Ausgestaltung des betrieblichen Brandschutzes) und des Sicherheitsbeauftragten (in Deutschland erforderlich nach § 22 SGB VII, dieser hat ausführende Tätigkeiten, z. B. zur Verhütung von Arbeitsunfällen und Berufskrankheiten, und arbeitet der Fachkraft für Arbeitssicherheit zu).

Vermeidung unnötiger Brandlasten

Eine Brandlast entsteht durch alle brennbaren Stoffe, die ins Gebäude eingebracht werden. Sie ist von der Menge und vom Heizwert der Stoffe abhängig. IT-Geräte und Leitungen stellen ebenso eine Brandlast dar wie Möbel, Fußbodenbeläge und Gardinen. Nähere Erläuterungen zur Brennbarkeit oder Nichtbrennbarkeit von Baustoffen (Baustoffklasse A oder B) sind in der DIN 4102- Teil 1 und Teil 4 zu finden.

Bei der Unterbringung von IT-Geräten, Datenträgern etc. sollte eine vorherige Beachtung der vorhandenen Brandlasten im gleichen Raum und in den benachbarten Räumen erfolgen. Zum Beispiel sollte das Datenträgerarchiv nicht in der Nähe von oder über einem Papierlager untergebracht sein.

Auch im laufenden Betrieb muss auf die Vermeidung unnötiger Brandlasten geachtet werden. Die regelmäßige Entsorgung von Müll, vor allem von Altpapier und von Verpackungsabfällen ist aktiver Brandschutz. Aus Büroräumen sollten nicht mehr benötigte Akten entfernt und in speziell dafür vorgesehenen Archiven gelagert werden. Eine der häufigsten Beispiele für unnötige Brandlasten in Räumen, die für die IT genutzt werden, ist Verpackungsmaterial, beispielsweise Pappe oder Styropor. Aus den IT-Räumen ist Verpackungsmaterial umgehend zu entfernen und in dafür vorgesehene Lagerräume zu transportieren, wenn es noch benötigt wird.

Bei Gebäuden sollte bereits in der Planungsphase die Reduzierung unnötiger Brandlasten berücksichtigt werden. Nicht brennbare Materialien sind für den Ausbau zu bevorzugen (Baustoffklasse A). Um den sicheren Betrieb unter Gesichtspunkten des Brandschutzes zu gewährleisten und Grenzwerte nicht zu überschreiten, sollte schon in der Planungsphase von Gebäuden eine überschlägige Berechnung der späteren Brandlasten erfolgen. Dabei sind die Brandklassen der Einrichtungen sowie die Baustoffklassen der Materialien zu berücksichtigen. Dadurch werden später Schwierigkeiten bei der brandschutztechnischen Abnahme durch Bauaufsichtsbehörden und Feuerwehr vermieden.

INF.1.M4 Branderkennung in Gebäuden [Planer]

Maßnahmen zum baulichen und technischen Brandschutz, Branderkennung und rechtzeitige Alarmierung im Brandfall sind elementare Maßnahmen, um Gesundheit und Leben aller Menschen, die sich in einem Gebäude aufhalten, zu schützen.

Welche Maßnahmen des baulichen und technischen Brandschutzes für ein Gebäude gefordert sind, geben in Deutschland die jeweils gültigen Bauordnungen vor. Um die verschiedenen Landesbauordnungen zu vereinheitlichen, wurde die Musterbauordnung (MBO) als Orientierungsrahmen erstellt. Zudem ist ein nach Größe und Nutzung des Gebäudes angemessenes Brandschutzkonzept aufzustellen.

Es gilt immer, dass es in Gebäuden, je nach Art der Nutzung und der Bauweise, aus verschiedenen Gründen zu Bränden kommen kann. Um Personen zu schützen und um einen Brand rechtzeitig eindämmen zu können, muss seine Entstehung schnellstmöglich detektiert und der Brand bekämpft werden.

Um die Entstehung eines Brandes schnellstmöglich detektieren, alarmieren und bekämpfen zu können, müssen unter Einhaltung der jeweils gültigen Normen und Herstellervorgaben ausreichend Rauchmelder installiert werden.

Lokale Melder können über eine Brandmeldezentrale (BMZ) gesteuert und ausgewertet werden. Melder aller Art und Brandmeldezentrale bilden gemeinsam die Brandmeldeanlage (BMA).

Empfehlenswert ist eine Mindestausstattung bestehend aus

- Rauchmeldern an der Decke aller Flure sowie
- Rauchmeldern an der Decke aller Technikräume und Räumen der Elektroversorgung (Verteilungen, USV).

Falls eine Raumlufttechnische Anlage (RLT) vorhanden ist, müssen auch deren Lüftungskanäle überwacht werden. Die RLT-Anlage muss zentral durch die BMZ abgeschaltet werden können, um zu verhindern, dass Brandrauch im Gebäude verteilt wird.

Es ist auf den korrekten Einbau der Rauchmelder entsprechend der Herstellervorgaben zu achten. Planung, Errichtung und Betrieb einer BMA sind nach Vorgaben der DIN 14675 "Brandmeldeanlagen - Aufbau und Betrieb" zu konzipieren und zwischen Auftraggeber, Bauaufsicht, Feuerwehr und gegebenenfalls Versicherer abzustimmen.

Falls eine Brandmeldezentrale vorhanden ist, sollten alle deren Meldungen inklusive der Störmeldungen auf einer ständig besetzten Stelle, z. B. der Pförtnerloge, auflaufen.

Die Funktionsfähigkeit aller Rauchmelder sowie aller weiteren Komponenten einer Brandmeldeanlage muss regelmäßig überprüft werden. Es sollten sporadisch einige der Melderlinien manuell auf ihre Funktionsfähigkeit getestet werden.

Bei Rauchdetektion muss eine Alarmierung im Gebäude ausgelöst werden, bei der sichergestellt ist, dass alle im Gebäude anwesenden Personen diese wahrnehmen können.

Um ein gefahrloses Verlassen des Gebäudes sicherzustellen, muss immer gewährleistet sein, dass die vorgesehenen Flucht- und Rettungswege benutzbar sind. Sie dürfen nicht durch Möbel oder gar elektrische Geräte wie Kopierer oder Drucker, die eine erhebliche Brandlast darstellen, in ihrer vorgeschriebenen Breite eingeschränkt werden. Die minimale Breite von Fluchtwegen ist in Deutschland in der Technischen Richtlinie für Arbeitsstätten ASR A2.3 "Fluchtwege und Notausgänge, Flucht- und Rettungsplan" vorgeschrieben. Es muss regelmäßig kontrolliert werden, dass die Fluchtwege benutzbar und frei von Hindernissen sind.

INF.1.M5 Handfeuerlöscher

Die meisten Brände entstehen aus kleinen, anfangs noch gut beherrschbaren Brandherden. Besonders in Büros findet das Feuer reichlich Nahrung und kann sich sehr schnell ausbreiten. Der Sofortbekämpfung von Bränden kommt also ein sehr hoher Stellenwert zu.

Diese Sofortbekämpfung ist nur möglich, wenn Handfeuerlöscher in der jeweils geeigneten Brandklasse (DIN EN 3 Tragbare Feuerlöscher) in ausreichender Zahl und Größe (Beratung durch die örtliche Feuerwehr) im Gebäude zur Verfügung stehen.

Alle Handfeuerlöscher müssen regelmäßig geprüft und gewartet werden, damit sie im Ernstfall funktionieren. Darüber ist ein Instandhaltungsnachweis zu führen. Es ist zudem darauf zu achten, dass Feuerlöscher in Bereichen mit besonderen Zutritts-Beschränkungen bei solchen regelmäßigen Inspektionen nicht vergessen werden.

Pulverlöscher, die die Brandklassen A (feste Stoffe), B (brennbare Flüssigkeiten) und C (Gase) abdecken, sollten in Bereichen mit elektrischen und elektronischen Geräten nicht eingesetzt werden, weil die Löschschäden in der Regel unverhältnismäßig hoch sind. Es wird daher dringend empfohlen, im direkten Umfeld von Serverräumen, Datenträgerarchiven, Räumen für technische Infrastruktur und Rechenzentren keine Pulverlöscher, sondern ausschließlich geeignete Gaslöscher bereit zu halten. Nur so kann verhindert werden, dass in der Ausregung eines Brandes fälschlicher Weise ein Pulverlöscher verwendet wird. Im Übrigen sind die geeigneten Handfeuerlöscher unter Berücksichtigung des Vorausgesagten im Brandschutzkonzept festzulegen.

Die Feuerlöscher müssen so angebracht werden, dass sie im Brandfall leicht erreichbar sind. Die Beschäftigten sollten sich den Standort des nächsten Feuerlöschers einprägen. Die Standorte von Löschern und Hydranten sind durch vorgeschriebene Schilder kenntlich zu machen. Tragbare Feuerlöscher sind zugelassen bis zu einem Gesamtgewicht von 20 kg. Mit den überwiegend eingesetzten Geräten von 6 und 12 kg lassen sich größere Brandherde löschen als von Laien üblicherweise angenommen wird, dies ist allerdings nur bei richtiger Anwendung des Löschers gegeben. Bis zur vollständigen Entladung des Löschmittels vergehen nur wenige Sekunden. Daher sind bei entsprechenden Brandschutzübungen die Mitarbeiter in die Benutzung der Handfeuerlöscher einzuweisen und die Bedienung der Löscher auch zu üben.

INF.1.M6 Geschlossene Fenster und Türen [Mitarbeiter]

Fenster und nach außen gehende Türen (Balkone, Terrassen) müssen in Zeiten, in denen ein Raum nicht besetzt ist, geschlossen werden. Außentüren sind abzuschließen. Im Keller- und Erdgeschoss und, je nach Fassadengestaltung, auch in den höheren Etagen, bieten offene Fenster und Türen Einbrechern ideale Einstiegsmöglichkeiten, die auch während der Betriebszeiten einer Institution genutzt werden.

Mitarbeiter sollten darauf hingewiesen werden, dass Fenster und Türen beim Verlassen von Räumen zu schließen sind. Wenn während normaler Arbeitszeiten sichergestellt ist, dass die Räume nur kurzzeitig leer stehen, kann von einer zwingenden Regelung für Büroräume sowie für Besprechungs-, Veranstaltungs- und Schulungsräumen abgesehen werden.

Keine Ausnahme darf bei Brand- und Rauchschutztüren zugelassen werden. Diese bieten nur im geschlossenen Zustand Schutz und dürfen deshalb keinesfalls durch Keile oder andere Vorrichtungen dauerhaft offen gehalten werden (siehe INF.1.M3 Einhaltung von Brandschutzvorschriften).

Es ist sinnvoll, wenn Pförtner oder Mitarbeiter der Haustechnik regelmäßig überprüfen, ob die Fenster und Türen nach Verlassen der Räume verschlossen wurden.

INF.1.M7 Zutrittsregelung und -kontrolle [Leiter Organisation]

Der Zutritt zu schutzbedürftigen Gebäudeteilen und Räumen ist zu regeln und zu kontrollieren (siehe ORP.4 Identitäts- und Berechtigungsmanagement). Die Maßnahmen reichen dabei von einer einfachen Schlüsselvergabe bis zu aufwendigen Identifizierungssystemen mit Personenvereinzelung.

Für eine Zutrittsregelung und -kontrolle ist es erforderlich, dass

- der von der Regelung betroffene Bereich eindeutig bestimmt wird,
- die Zahl der zutrittsberechtigten Personen auf ein Mindestmaß reduziert wird; diese Personen sollen gegenseitig ihre Berechtigung kennen, um Unberechtigte als solche erkennen zu können,
- der Zutritt anderer Personen (Besucher) erst nach vorheriger Prüfung der Notwendigkeit erfolgt,
- erteilte Zutrittsberechtigungen dokumentiert werden.

Die Vergabe von Rechten allein reicht nicht aus, wenn deren Einhaltung oder Überschreitung nicht kontrolliert wird. Die Ausgestaltung von Kontrollmechanismen sollte nach dem Grundsatz erfolgen, dass einfache und praktikable Lösungen oft ebenso effizient sind wie aufwendige Technik. Beispiele hierfür sind:

- Information und Sensibilisierung der Berechtigten,
- Bekanntgabe von Berechtigungsänderungen,
- sichtbares Tragen von Hausausweisen, ergänzt durch Vergabe von Besucherausweisen,
- Begleitung von Besuchern,
- Verhaltensregelungen bei erkannter Berechtigungsüberschreitung und
- Einschränkung des ungehinderten Zutritts für nicht Zutrittsberechtigte (z. B. Tür mit Blindknauf, Schloss für Berechtigte mit Schlüssel, Klingel für Besucher).

Bei der Zutrittskontrolle werden verschiedene bauliche, organisatorische und personelle Maßnahmen benötigt. Deren Zusammenwirken sollte in einem Zutrittskontrollkonzept geregelt sein, das die generellen Richtlinien für den Perimeter-, Gebäude- und Geräteschutz festlegt. Dazu gehören:

- Festlegung der SicherheitszonenZu schützende Bereiche können etwa Grundstücke, Gebäude, Serverräume, Räume mit Peripheriegeräten, Archive, Kommunikationseinrichtungen und die Haustechnik sein. Da diese Bereiche häufig sehr unterschiedliche Sicherheitsanforderungen aufweisen, kann es sinnvoll sein, diese in verschiedene Sicherheitszonen aufzuteilen (siehe INF.1.M 23 Bildung von Sicherheitszonen).
- Vergabe von Zutrittsberechtigungen (siehe ORP.4 Identitäts- und Berechtigungsmanagement)
- Bestimmung eines Verantwortlichen für ZutrittskontrolleDieser vergibt die Zutrittsberechtigungen an die einzelnen Personen entsprechend den in der Sicherheitspolitik festgelegten Grundsätzen.
- Definition von ZeitabhängigkeitenEs ist zu klären, ob zeitliche Beschränkungen der Zutrittsrechte erforderlich sind. Solche Zeitabhängigkeiten können etwa sein: Zutritt nur während der Arbeitszeit, Zutritt einmal täglich oder befristeter Zutritt bis zu einem fixierten Datum.
- Festlegung der BeweissicherungHier ist zu bestimmen, welche Daten bei Zutritt zu und Verlassen von einem geschützten Bereich protokolliert werden. Dabei bedarf es einer sorgfältigen Abwägung zwischen den Sicherheitsinteressen des Systembetreibers und den Schutzinteressen der Privatsphäre des Einzelnen.
- Behandlung von AusnahmesituationenAuch in Ausnahmesituationen sollten keine Unbefugten das Gebäude oder die Liegenschaften betreten können. Oberste Priorität ist allerdings sicherzustellen, dass im Brandfall alle Personen schnellstmöglich die gefährdeten Zonen verlassen können.

Ergänzend kann der Einbau von Ausweislesern verschiedenster Qualitäten, von Schleusen und Vereinzelungseinrichtungen sinnvoll sein. Zur Schlüsselverwaltung siehe INF.1.M 12 Schlüsselverwaltung.

Um ein umfassenderes Konzept umzusetzen, Flexibilität im Einsatz zu erhalten und um Transparenz und Nachprüfbarkeit sicherzustellen, ist der Einsatz eines IT-gestützten Systems zum Berechtigungsmanagement zu empfehlen (siehe Kapitel 3.1 Zutrittskontrollsystem und Berechtigungsmanagement).

Die Terminals zur Zutrittskontrolle müssen gegen Manipulationen geschützt werden. Dafür müssen diese so angebracht werden, dass Vertraulichkeit bei der Eingabe von Daten gewährleistet ist. Außerdem sollten alle zur Dateneingabe erforderlichen Einheiten in einem Gerät kombiniert sein, also beispielsweise eine Tastatur zur PIN-Eingabe.

Befinden sich nicht alle Einheiten in einem Gerät, muss die Datenübertragung zwischen diesen verschlüsselt erfolgen. Werden also z. B. berührungslose Ausweisleser eingesetzt, so muss die Datenübertragung zwischen Karte und Leser verschlüsselt erfolgen.

Im Betrieb muss die Wirksamkeit aller technischen und organisatorischen Maßnahmen stetig kontrolliert werden. Es empfiehlt sich, vor allem an bekannten problematischen Stelle regelmäßig zu überprüfen, ob keine Möglichkeiten entstanden sind, um die Zutrittskontrolle zu umgehen, z. B. in Liefer- oder Raucherzonen.

INF.1.M8 Rauchverbot [Mitarbeiter]

In erster Linie dient ein allgemeines Rauchverbot in Gebäuden natürlich dem Nichtraucherschutz. Daneben hat es aber auch Relevanz in der Informationssicherheit. So kann Tabak-Rauch empfindliche IT-Geräte ebenso schädigen wie der Rauch eines Schadfeuers. Daher und wegen der zusätzlichen Brandgefahr sollte in allen IT-Betriebsräumen (Serverraum, Datenträgerarchiv, aber auch Belegarchiv etc.), ein striktes Rauchverbot eingehalten werden. Dieses dient gleicherweise dem vorbeugenden Brandschutz wie der Betriebssicherheit von IT mit mechanischen Funktionseinheiten.

Leider erwächst aus dem Rauchverbot in Gebäuden durch die bereitzustellenden Raucherzonen in Außenbereichen ein anderes Risiko. Es ist häufig zu beobachten, dass Außentüren in mitunter schwer einsehbaren Bereichen ständig offen stehen, weil der Nahbereich der Tür die Raucherzone bildet und die Tür aus Bequemlichkeit während der Arbeitszeiten nie geschlossen wird.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Allgemeines Gebäude".

INF.1.M9 Sicherheitskonzept für die Gebäudenutzung [Informationssicherheitsbeauftragter (ISB), Planer]

Voraussetzung für Erstellung eines effektiven Sicherheitskonzepts ist die Ermittlung des Schutzbedarfs der in einem Gebäude betriebenen Geschäftsprozesse und die Definition der grundsätzlichen Schutzziele, die sich häufig aus der Geschäftstätigkeit ergeben. Anschließend wird ein praxistaugliches und wirtschaftliches Sicherheitskonzept für die Nutzung eines Gebäudes erarbeitet. Unter der Berücksichtigung verschiedener Sicherheitsaspekte eines Gebäudes, sollten aufbauend auf den Schutzzielen angemessene Sicherheitsmaßnahmen für die verschiedenen Bereiche bei Aufrechterhaltung eines definierten Sicherheitsniveaus festgelegt werden. Es soll sichergestellt werden, dass alle Zugänge so kontrolliert und abgesichert sind, dass keine unbefugten Personen die zu schützenden Bereiche betreten können.

Ergänzt werden muss diese Betrachtung fast immer um weitere Maßnahmen gegen unerlaubtes Eindringen oder Einschleichen. Einen Überblick dazu bildet die Maßnahme INF.1.M 27 Einbruchsschutz.

Wenn das Gebäude öffentliche oder halböffentliche Bereiche aufweist oder wenn z. B.durch Fensterfronten im Straßenbereich Einblick in das Gebäude möglich ist, ist die INF.1.M 16 Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile zu prüfen.

Überall wo der Schutz der Inhalte des Gebäudes, seien es Waren, sei es die technische Infrastruktur, in besonderer Weise gefordert ist, muss das Sicherheitskonzept den Schutz vor Wasser betrachten. Hinweise dazu gibt die Maßnahme INF.1.M 24 Selbsttätige Entwässerung.

Alle auf die Schutzziele abgestimmten vorbeugenden oder schadensmindernden Maßnahmen müssen schließlich noch um detektierende Maßnahmen (siehe M 1.18 Gefahrenmeldeanlage) ergänzt werden. Das Gebäude-Schutzkonzept ist erst dann vollständig, wenn durch Planung und Ausführung den relevanten Gefährdungen entgegengewirkt wird und durch überwachende Maßnahmen sichergestellt wird, dass schadenbringende Ereignisse oder zufällige oder vorsätzliche Versuche, Schutz- und Sicherungsmaßnahmen zu überwinden möglichst frühzeitig bemerkt werden. Nur dann ist es möglich, Gegenmaßnahmen einzuleiten.

Das Sicherheitskonzept für das Gebäude sollte mit dem Gesamt-Sicherheitskonzept der Institution abgestimmt sein. Es sollte regelmäßig aktualisiert werden, vor allem wenn sich Änderungen in der Gebäudenutzung ergeben, also beispielsweise nach organisatorischen Änderungen in der Institution.

INF.1.M10 Einhaltung einschlägiger Normen und Vorschriften [Bauleiter, Errichterfirma]

Für nahezu alle Bereiche der Technik gibt es Richtlinien, Normen und Vorschriften. Diese können von Standardisierungsorganisationen, Branchenvereinigungen, Anwendergruppen oder staatlichen Institutionen herausgegeben worden sein, z. B. DIN (Deutsches Institut für Normung), ISO (International Standards Organization), VDE (Verband der Elektrotechnik, Elektronik und Informationstechnik), VDMA (Verband Deutscher Maschinen- und Anlagenbau), VdS (Verband der Sachversicherer). Diese Regelwerke tragen dazu bei, dass technische Einrichtungen ein ausreichendes Maß an Schutz für die Benutzer und Sicherheit für den Betrieb gewährleisten.

Die Buchstaben-getreue Einhaltung von Normen allein führt nicht zu einer signifikanten Verbesserung der Informationssicherheit. Die intelligente Umsetzung normativer Vorgaben stellt aber eine unverzichtbare Grundlage für alle weiteren Sicherheitsmaßnahmen dar. Bei der Planung und Errichtung von Gebäuden, bei deren Betrieb und Umbau sowie beim Einbau technischer Gebäudeausrüstungen (z. B. interne Versorgungsnetze wie Telefon- oder Datennetze) und bei Beschaffung und Betrieb von Geräten sind entsprechende Normen und Vorschriften also unbedingt zu beachten.

INF.1.M11 Abgeschlossene Türen [Mitarbeiter]

Die Türen nicht besetzter Räume sollten abgeschlossen werden. Dadurch wird verhindert, dass Unbefugte Zugriff auf darin befindliche Unterlagen und IT-Einrichtungen erlangen. Das Abschließen einzelner Büros ist insbesondere dann wichtig, wenn sich diese in Bereichen mit Publikumsverkehr befinden oder der Zutritt nicht durch andere Maßnahmen kontrolliert wird.

Auf das Abschließen der Türen kann verzichtet werden, wenn diese flurseitig über einen Blindknauf verfügen. Voraussetzung hierfür ist allerdings, dass die befugten Mitarbeiter ihren Schlüssel stets mit sich führen.

Innentüren können auch Fluchttüren sein. Fluchttüren müssen ermöglichen, dass die Türen jederzeit durch beliebige Personen von innen geöffnet werden können, solange sich Personen auf der Innenseite befinden. Sie müssen so gesichert sein, dass ein unberechtigter Zutritt von außen nach innen verhindert wird.

In manchen Fällen, z. B. in Großraumbüros, können Büros nicht abgeschlossen werden. Dann sollte alternativ jeder Mitarbeiter vor seiner Abwesenheit seine Unterlagen ("Clear-Desk-Politik") und den persönlichen Arbeitsbereich verschließen: Schreibtisch, Schrank und PC (Zugriffsschutz aktivieren), Telefon.

In Besprechungs-, Veranstaltungs- und Schulungsräumen gibt es meistens keine Möglichkeit, Unterlagen, IT-Systeme und ähnliches gesondert einzuschließen. Daher sollte es möglich sein, solche Räume zumindest dann, wenn alle Teilnehmer einer Veranstaltung den Raum verlassen, abzuschließen oder ihn durch einen internen Mitarbeiter beaufsichtigen zu lassen.

Bei laufendem Rechner kann auf das Abschließen der Türen verzichtet werden, wenn Zugriffe nur nach erfolgreicher Authentisierung möglich sind, also z. B. ein passwortunterstützter Bildschirmschoner aktiviert ist. Bei ausgeschaltetem Rechner kann auf das Verschließen des Büros verzichtet werden, wenn das Booten des Rechners die Eingabe eines Passwortes verlangt. Die gleiche Funktion erfüllen Zugangsmechanismen, die auf Token oder Chipkarten basieren.

Es ist sinnvoll, wenn dafür beauftragte Mitarbeiter wie Pförtner oder Mitarbeiter der Haustechnik sporadisch überprüfen, ob die Vorgaben zum Verschließen von Räumen sowie zur sicheren Aufbewahrung von vertraulichen UNterlagen eingehalten werden.

INF.1.M12 Schlüsselverwaltung

Für alle Schlüssel des Gebäudes (von Etagen, Fluren und Räumen) ist ein Schließplan zu fertigen. Die Herstellung, Aufbewahrung, Verwaltung und Ausgabe von Schlüsseln ist zentral zu regeln. Reserveschlüssel sind vorzuhalten und gesichert aufzubewahren. Das gleiche gilt auch für alle Identifikationsmittel wie Magnetstreifen- oder Chipkarten. Zu beachten bleibt:

- Ist eine Schließanlage vorhanden, sind für schutzbedürftige Bereiche eigene Schließgruppen zu bilden. Je nach Anforderungen sind einzelne Räume aus der Schließgruppe herauszunehmen und mit Einzelschließung zu versehen.
- Nicht ausgegebene Schlüssel und die Reserveschlüssel sind gegen unbefugten Zugriff geschützt aufzubewahren.
- Die Ausgabe der Schlüssel erfolgt nur in begründeten und nachvollziehbaren Fällen an hierfür autorisierte Personen gegen Quittung und ist zu dokumentieren. Auch im Vertretungsfall darf ein Schlüssel nicht einfach weitergegeben werden, sondern hat über die Schlüsselausgabe zu erfolgen. Nur über diesen Umweg kann eine lückenlose Dokumentation als Nachweis über den Verbleib des Schlüssels erfolgen.
- Es sind Vorkehrungen zu treffen, wie bei Verlust einzelner Schlüssel zu reagieren ist (Meldung, Ersatz, Kostenerstattung, unter Umständen Regress wegen mangelnder Sorgfaltspflicht prüfen), Austausch des Schlosses, Austausch von Schließgruppen etc.).
- Wenn sich Rollen oder Zuständigkeiten von Mitarbeitern ändern, sind deren Schließberechtigungen zu prüfen und nicht mehr benötigte Schlüssel einzuziehen.
- Beim Ausscheiden von Mitarbeitern sind alle Schlüssel einzuziehen (Aufnahme der Schlüsselverwaltung in den Laufzettel der noch vor dem Ausscheiden zu erledigenden Stationen).
- Schlösser und Schlüssel zu besonders schutzbedürftigen Bereichen (zu denen nur sehr wenige Schlüssel ausgegeben werden sollten) können bei Bedarf auch ohne vorherige Ankündigung im Verdachtsfall getauscht werden, um so die Nutzung nicht autorisierter Schlüssel / Schließmittel zu verhindern.

INF.1.M13 Regelungen für Zutritt zu Verteilern

Die Verteiler (z. B. für Energieversorgung, Datennetze, Telefonie) sind nach Möglichkeit in Räumen für technische Infrastruktur (siehe Baustein INF.5 Raum für technische Infrastruktur) unterzubringen. Die dort genannten Sicherheitsanforderungen sind zu berücksichtigen.

Der Zutritt zu den Verteilern aller Versorgungseinrichtungen (Strom, Wasser, Gas, Telefon, Gefahrenmeldung, Fernwärme/-kälte, etc.) in einem Gebäude muss möglich und geordnet sein. Mit möglich ist gemeint,

- dass Verteiler nicht bei Malerarbeiten mit Farbe oder Tapeten so verklebt werden, dass sie nur noch mit Werkzeug zu öffnen oder unauffindbar sind,
- dass Verteiler nicht mit Möbeln, Geräten, Paletten etc. zugestellt werden,
- dass für verschlossene Verteiler die Schlüssel verfügbar sind und die Schlösser funktionieren.

Mit geordnet ist gemeint, dass festgelegt ist, wer welchen Verteiler öffnen darf. Verteiler sollten verschlossen sein und dürfen nur von den für die jeweilige Versorgungseinrichtung zuständigen Personen geöffnet werden. Die Zugriffsmöglichkeiten können durch unterschiedliche Schließungen und eine entsprechende Schlüsselverwaltung geregelt werden (siehe dazu INF.1.M 12 Schlüsselverwaltung und Kapitel 3.1 Zutrittskontrollsystem und Berechtigungsmanagement).

Sind in Verteilern des Stromversorgungsnetzes Schmelzsicherungen eingebaut, sollten entsprechende Ersatzsicherungen (im Verteiler) bereit liegen. Eine Dokumentation der Verteiler ist entsprechend INF.3 Elektrotechnische Verkabelung auszuführen.

Alle im Verteiler eingebauten Einrichtungen sind exakt und dauerhaft zu beschriften. Diese Beschriftung ist so anzubringen, dass auch bei entfernten Abdeckungen jedes Einbauelement unmittelbar sicher identifiziert werden kann.

INF.1.M14 Blitzschutzeinrichtungen

Die direkten Auswirkungen eines Blitzeinschlages auf ein Gebäude (Beschädigung der Bausubstanz, Brand u. ä.) lassen sich durch die Installation einer geeigneten Blitzschutzanlage weitestgehend verhindern. Da es aber nicht Aufgabe und Funktion des "Äußeren Blitzschutzes" ist, die im Gebäude vorhandenen elektrischen Betriebsmittel zu schützen, ist zudem auch ein "Innerer Blitzschutz", also der Überspannungsschutz, erforderlich (siehe dazu INF.3 Elektrotechnische Verkabelung).

Beispiel:

Durch Blitzschlag entstand in der süddeutschen Niederlassung eines Dienstleistungsunternehmens ein Schaden an IT-Geräten (PCs, Server, Laserdrucker) in Höhe von ca. 10.000 Euro. Aufgrund dieses Ereignisses wurde das Gebäude mit einem äußeren Blitzschutz ohne inneren Blitzschutz (Überspannungsschutz) ausgestattet. Ein erneuter Blitzschlag führte nun trotz äußeren Blitzschutzes zu Schäden in annähernd gleicher Höhe.

Die seit gültige Norm DIN EN 62305 "Blitzschutz" (entspricht den Normen VDE 0185-305 und IEC 62305) ordnet seit 2006 den gesamten Blitz- und Überspannungsschutz neu.

Jede Institution sollte auf Basis der neuen Norm DIN EN 62305 ein Blitz- und Überspannungsschutzkonzept erstellen. In Teil 2 "Risiko-Management" beschreibt diese Norm erstmals allgemeinverbindlich den Weg zu einem risikoorientierten Blitz- und Überspannungsschutz. Im Teil 3 wird darin der "Schutz von baulichen Anlagen und Personen", also der äußere Blitzschutz behandelt.

Der äußere Blitzschutz, die Fangeinrichtung (vulgo Blitzableiter), wird hinsichtlich ihrer Wirksamkeit in vier Schutzklassen (auch Lightning-Protection-Level, kurz LPL genannt) unterteilt. Die Schutzklasse IV (LPL IV) hat den geringsten Schutzwert, während eine Fangeinrichtung der Schutzklasse I den besten Schutz bietet. Leicht erkennbarer Unterschied zwischen den 4 Schutzklassen ist die Maschenweite der Fangeinrichtungen. Diese reicht von 20 x 20 m für die Schutzklasse IV in 5 m-Schritten hinunter bis 5 x 5 m für die Schutzklasse I. Für Gebäude mit umfangreicher IT-Ausstattung sollte die Fangeinrichtung mindestens der Schutzklasse II, besser Schutzklasse I entsprechen.

Der durch die Fangeinrichtung zur Erdung abfließende eingeprägte Blitzstrom bewirkt eine entlang der Fangeinrichtung vom Einschlagspunkt des Blitzes zum Erdungspunkt hin abnehmende Spannung. Am höchsten Punkt der Fangeinrichtung kann diese Spannung einige 100.000 Volt betragen. Es ist daher zu beachten, dass gerade in oberen Geschossen eines Gebäudes galvanisch leitende Installationen (Daten, Strom, Wasser etc.) einen ausreichenden Abstand von den Fangeinrichtungen haben müssen. Auch dieser Aspekt ist unter der Bezeichnung Trennungsabstand in der neuen Norm berücksichtigt. Mit Überlegungen zum Schutz gegen kompromittierende Einkopplung hat das nichts zu tun, auch wenn der Aspekt des Trennungsabstandes bisher häufig fälschlich mit dem Schutz gegen Einkopplung von den zu nahe am Blitzableiter liegenden Datenleitungen auf den Blitzableiter gleichgesetzt wurde.

Da der Spannungsabfall entlang der Fangeinrichtung am Erdungspunkt wegen des verbleibenden Erdübergangswiderstandes nie bis auf 0 V sinkt und der Fußpunkt der Fangeinrichtung mit dem Hauptpotentialausgleich des Gebäudes verbunden sein muss, wird das gesamte PE-System des Gebäudes und damit auch der N-Leiter auf diese Restspannung angehoben. Hier sind Spannungen im Bereich von immerhin noch weit über 10.000 Volt zu erwarten. Es werden also Spannungen zwischen N-/PE-Leitern und den Leitern L1/L2/L3 erreicht, die das betriebsübliche Maß von 230/400 V deutlich überschreiten. Damit diese Spannungen den innerhalb des Gebäudes betriebenen elektrotechnischen Einrichtungen nicht schaden, muss als unverzichtbare Folge aus dem Aufbau des äußeren Blitzschutzes der innere Blitzschutz, also der Überspannungsschutz aufgebaut werden (siehe INF.3 Elektrotechnische Verkabelung).

Das gesamte Blitzschutzsystem muss regelmäßig geprüft werden. Fangeinrichtungen der Schutzklassen I und II sind jährlich einer Sichtprüfung und alle 2 Jahre einer umfassenden Prüfung zu unterziehen. Für die Schutzklassen III und IV sind hier 2 bzw. 4 Jahre vorgesehen. Bei kritischen Systemen also solchen zum Schutz hoch- oder höchst verfügbarer Einrichtungen ist eine umfassende Prüfung sogar jährlich durchzuführen. Erkannte Mängel sind umgehend zu beheben. Selbstverständlich sind die Durchführung der Prüfung, die dabei getroffenen Feststellungen sowie durchgeführte Mängelbehebungen schriftlich zu dokumentieren.

INF.1.M15 Lagepläne der Versorgungsleitungen

Lagepläne kennzeichnen die Versorgungsleitungen (Strom, Wasser, Gas, Telefon, Gefahrenmeldung, Klimatisierung etc.) eines Gebäudes und von Gebäuden einer Liegenschaft in visueller Form, idealerweise mit einem erläuternden schriftlichen Teil. Aktuelle und gepflegte Pläne ermöglichen es, Arbeiten im Bereich von Leitungen so vorzubereiten, dass diese nicht beschädigt werden sowie sich im Schadensfall einfach und schnell ein genaues Bild der Situation zu machen, Schadstellen schnell zu lokalisieren, um Störungen dadurch schneller beheben zu können. Deshalb sollten genaue und jederzeit aktuelle Lagepläne aller Versorgungsleitungen, inklusive aller die Leitungen betreffenden Sachverhalte, im Gebäude und auf dem dazugehörenden Grundstück, geführt werden. Dazu gehören:

- genaue Führung der Leitungen (Einzeichnung in bemaßte Grundriss- und Lagepläne),
- genaue technische Daten (Typ und Abmessung),
- eventuell vorhandene Kennzeichnung,
- Nutzung der Leitungen, Nennung der daran angeschlossenen Netzteilnehmer,
- Gefahrenpunkte und
- vorhandene und zu prüfende Sicherheitsmaßnahmen.

Alle Arbeiten an Leitungen sollten vollständig und zeitnah dokumentiert werden. Die Pläne sollten gesichert aufbewahrt und so gelagert werden, dass ausschließlich berechtigte Personen darauf zugreifen können, sie aber zugleich im Bedarfsfall schnell verfügbar sind.

INF.1.M16 Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile

In jedem Gebäude gibt es Bereiche mit unterschiedlichen Nutzungsszenarien und unterschiedlichem Schutzbedarf. Schützenswerte Gebäudeteile sind z. B. Serverraum, Rechenzentrum, Datenträgerarchiv, Klimazentrale, Verteilungen der Stromversorgung, Schalt- und Rangierräume, Ersatzteillager.

Solche Bereiche sollten keinen Hinweis auf ihre Nutzung tragen. Türschilder wie z. B. RECHENZENTRUM oder ARCHIV geben einem potentiellen Angreifer, der zum Gebäude Zutritt hat, Hinweise, um seine Aktivitäten gezielter und damit Erfolg versprechender vorbereiten zu können.

Ist es unvermeidbar, geschäftsrelevante Informationen oder IT in Räumen oder Gebäudebereichen unterzubringen, die für Fremde leicht von außen einsehbar sind (siehe auch INF.1.M 34 Anordnung schützenswerter Gebäudeteile), so sind geeignete Maßnahmen zu treffen, um den Einblick zu verhindern oder so zu gestalten, dass die Nutzung nicht offenbar wird. Dabei ist darauf zu achten, dass z. B. nicht nur ein Fenster einer ganzen Etage mit einem Sichtschutz versehen wird.

INF.1.M17 Baulicher Rauchschutz [Planer]

Rauch stellt bei Bränden die größte Personengefährdung dar. Mehr als 90 % der Brandtoten sind durch Raucheinwirkungen (Vergiftungen) zu beklagen. Aber auch die IT-Hardware kann durch Rauch erheblich in Mitleidenschaft gezogen werden. Daher ist auf einen umfassenden Rauchschutz Wert zu legen.

Die folgenden Empfehlungen sollten zum Rauchschutz berücksichtigt werden:

- Brandschutztüren sollten Rauchschutzqualität aufweisen, erkennbar am Kürzel „RS“ in der Typenbezeichnung der Tür.
- Rauchschutztüren in Fluren sollten durch Rauchschalter gesteuert werden. Solche Türen können immer offen stehen, da sie bei Rauchdetektion selbsttätig schließen.
- Eine rasche Entrauchung von IT-Räumen muss möglich sein.
- In Klimakanälen (Zu- und Abluft) sollten Kanalmelder installiert sein. In der Frischluftansaugung sollten Melder installiert sein, die diese automatisch sperren, wenn Störgrößen (Rauch) erkannt werden.

Nach Installations- und Umbauarbeiten ist sicherzustellen, dass Rauchschutzmaßnahmen wirksam geblieben sind oder wieder hergestellt wurden.

Die Mitarbeiter müssen unterrichtet werden, welche Warnsignale die Rauchschutz-Komponenten haben und wie sie darauf zu reagieren haben.

Die Funktionsfähigkeit aller Rauchschutz-Komponenten muss regelmäßig überprüft werden. Dazu gehört es auch, zu überprüfen, ob Durchbrüche zur Durchführung von Verkabelungen im Doppelboden und in abgehängten Decken wirksam geschottet wurden.

INF.1.M18 Brandschutzbegehungen

Brandschutzbegehungen sollen Schwachstellen des vorbeugenden Brandschutzes aufdecken und sie unterstützen bei der Bewusstseinsbildung zur Etablierung präventiver Maßnahmen.

Bei Begehungen sollten typische Schwachstellen gezielt betrachtet werden, wie die Ansammlung brennbarer oder explosionsgefährlicher Stoffe außerhalb der dafür bestimmten Lager und Behältnisse oder Lagerung von Papiervorräten oder Möbeln innerhalb von Technik- und Serverräumen (nicht selten überschreiten diese Ansammlungen die zulässigen Brandlasten oder verstellen Fluchtwege). Hierbei wird überprüft, ob Rauchmelder funktionieren, Brandabschnitts- oder Rauchschutztüren durch Keile offen gehalten, Brandabschottungen bei Arbeiten geöffnet und/oder sogar beschädigt und nicht ordnungsgemäß wiederhergerichtet wurden. Neben angekündigten sollten auch unangekündigte Begehungen erfolgen, Feststellungen protokolliert und Mängel unverzüglich beseitigt werden.

Da die Handlungsweise der Mitarbeiter in der Regel nicht vom böswilligen Vorsatz, sondern von der betrieblichen Notwendigkeit oder Bequemlichkeit bestimmt wird, kann es nicht Sinn einer Brandschutzbegehung sein, Täter zu finden und zu bestrafen. Vielmehr sollten die vorgefundenen Mängel dazu Anlass geben, die Zustände und auch deren Ursachen unverzüglich zu beheben.

INF.1.M19 Frühzeitige Information des Brandschutzbeauftragten

Bei allen Arbeiten an Rohr- und Kabeltrassen, die in irgendeiner Form Wanddurchbrüche sowie notwendige Flure, Flucht- und Rettungswege berühren, ist der Brandschutzbeauftragte zu informieren. Diese Information muss schon so deutlich im Vorfeld der eigentlichen Arbeiten erfolgen, dass der Brandschutzbeauftragte ausreichend Gelegenheit hat, alle Aspekte des baulichen vorbeugenden Brandschutzes in die Planung und Durchführung der beabsichtigten Arbeiten einzubringen.

Dem Brandschutzbeauftragten muss, auch während laufender Arbeiten, durch rechtzeitige Information die Gelegenheit gegeben werden, die ordnungsgemäße Ausführung von Brandschutzmaßnahmen zu kontrollieren oder eine solche Kontrolle zu veranlassen, bevor diese durch den Baufortschritt nicht mehr zugänglich sind, z. B. weil eine abgehängte Decke bereits geschlossen worden ist.

Die Einbindung des Brandschutzbeauftragten ist durch entsprechende Organisationsanweisungen sicherzustellen und in den Planungs- und Abnahmeunterlagen der Baumaßnahme zu dokumentieren (siehe auch INF.1.M 3 Einhaltung von Brandschutzvorschriften).

INF.1.M20 Alarmierungsplan und Brandschutzübungen

Es ist erforderlich, Pläne für die im Brandfall zu ergreifenden Maßnahmen zu erstellen. In einem solchen Plan ist z. B. niederzulegen,

- welche Maßnahmen bei welchen Ereignissen zu treffen sind,
- ob und wie Gebäudeteile evtl. zu räumen sind (Personen und Geräte),
- wer zu informieren ist und
- welche hilfeleistenden Kräfte zu informieren sind.

Ergänzt werden kann der Alarmierungsplan um Verhaltensregeln für den Brandfall, die allen Mitarbeitern bekannt zu geben sind. Dazu siehe auch Baustein DER.4 Notfallmanagement.

Der beste Alarmierungsplan nützt allerdings wenig, wenn nicht sichergestellt ist, dass die darin aufgelisteten Maßnahmen richtig und praktikabel sind. Es ist also erforderlich, den Alarmierungsplan regelmäßig zu prüfen und zu aktualisieren. Eine dieser Prüfungsmaßnahmen ist die Durchführung von Brandschutzübungen.

Beispiel:

- Eine in einem 21?geschossigen Bonner Bürogebäude durchgeführte Brandschutzübung hat gezeigt, dass viele Mitarbeiter nicht wussten, wo ein Feuerlöscher oder wo das nächste Treppenhaus ist. Im Ernstfall kann diese Unkenntnis zu einer Katastrophe führen. Teilweise wurde die Übung ignoriert, man verließ aus Bequemlichkeit den Raum nicht.

Gerade in Brandschutzübungen soll das richtige Verhalten im Brandfall geschult und geübt werden, um Menschenleben zu schützen und Schäden u. a. für die IT zu vermeiden. Die Durchführung solcher Übungen ist vorher mit der Behörden- oder Unternehmensleitung abzustimmen.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

INF.1.M21 Unabhängige elektrische Versorgungsstränge (A)

Sobald hohe oder sehr hohe Anforderungen an die Verfügbarkeit der IT gestellt werden, ist eine Versorgung der IT über zwei voneinander unabhängige elektrische Versorgungsstränge und der Einsatz von IT-Geräten mit zwei Netzteilen sinnvoll und angemessen.

Die wichtigen Verbraucher (zentrale Speicherkomponenten, Netzknoten oder Server) werden an die unabhängigen Versorgungen "Netz 1" und "Netz 2" (auch „A-B-Versorgung“genannt) angeschlossen (siehe Abbildung). Andere IT-Komponenten, an die wenige hohe Anforderungen gestellt werden, werden gleichmäßig auf die Versorgungsstränge verteilt.

Unabhängige elektrische Versorgungsstränge

Hierbei ist besonders bei den nur einfach angeschlossenen Geräten darauf zu achten, dass Geräte, die sich gegenseitig Redundanz geben, nicht an der gleichen Versorgung angeschlossen werden. Zudem müssen die Geräte entsprechend ihrer Leistungsaufnahme gleichmäßig auf beide Stränge verteilt werden.

INF.1.M22 Sichere Türen und Fenster (CIA)

Wenn Türen und Fenster einen Übergang zwischen Sicherheitszonen bilden, müssen sie angemessenen Schutz bieten. Eine Außentür muss z. B. vor Einbrüchen schützen, ebenso müssen die erreichbaren Fenster gesichert werden. Im Innenbereich müssen Türen, die die Grenze eines Brandabschnitts bilden, selbst Brandschutzqualität haben, zudem können sie oder auch andere Innentüren eine zweite Linie des Einbruchschutzes bilden.

Sicherheitstüren und -fenster sind in Normen klassifiziert. Aus dem Schutzziel des zu sichernden Bereichs und dem Schutzbedarf der Institution lässt sich eine Auswahl der angemessenen Ausführung von Türen und Fenstern treffen:

- In der Norm DIN EN 1627:2011-09 "Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchhemmung - Anforderungen und Klassifizierung" sind die Bauelemente in Widerstandsklassen (RC, englisch Resistance Class) eingeordnet worden. Türen gemäß der Klassifizierungen RC1 bis RC4 bieten aufgrund ihrer Stabilität einen höheren Schutz gegen Einbruch (z. B. bei Serverräumen, Räumen mit technische Infrastruktur sowie bei Keller- und Lieferanteneingängen). Die Widerstandsklassen RC5 und RC6 sind in der Regel nur bei sehr speziellen Erfordernissen angemessen und spielen daher bei IT-Grundschutzbetrachtungen keine Rolle.
- Selbstschließende feuerhemmende und gegebenenfalls rauchdichte Türen (z. B. Feuerschutztüren T30 oder T30-RS, nach DIN 18082 "Feuerschutzabschlüsse") verzögern die Ausbreitung eines Brandes und in der RS-Ausführung auch von Rauch.

Sie schützen in der Ausführung als selbstschließende Rauchschutztür (DIN 18095-1 "Türen; Rauchschutztüren; Begriffe und Anforderungen") die Ausbreitung von Brandrauch. Brandrauch ist so feinkörnig, dass er problemlos durch Druckausgleichs- und Lüftungsöffnungen von Festplatten hindurch kommt. Für die geringen Flughöhen von Festplattenleseköpfen ist er aber immer noch viel zu groß und verursacht dort enorme Schäden.

Es können auch mehrere Schutzeigenschaften in einer Tür kombiniert werden, es gibt beispielsweise rauchdichte Brandschutztüren, die zudem Schutz gegen Einbruch bieten.

Die Sicherungsmaßnahmen aller raumumschließenden Bauelemente müssen gleichwertig sein:

- Bei Verwendung einbruchhemmender Türen ist im Fassadenbereich die Verwendung einbruchhemmender Fenster oder Fassadenelemente (siehe DIN EN1627-1630:2011 "Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchhemmung") zu erwägen.
- Weiterhin ist es z. B. nicht zweckmäßig, eine einbruchhemmende Tür der höchsten Widerstandsklasse in eine Gipskartonwand einzubauen.
- Beim Einbau einer feuerhemmenden oder rauchdichten Tür ist darauf zu achten, dass auch die umgebende Wand gleichwertig feuerhemmend und rauchdicht ist und nicht durch offene Oberlichter oder ungeschottete Kabeldurchführungen ein Bypass besteht.

Anforderungen zur Ausführung von Sicherheitstüren finden sich in INF.2 Rechenzentrum und INF.1.M 27 Einbruchsschutz.

Der Einsatz von Sicherheitstüren ist hinsichtlich der Brandschutzes über den von der Bauaufsicht und der Feuerwehr vorgeschriebenen Bereich hinaus (siehe INF.1.M 3 Einhaltung von Brandschutzvorschriften) besonders bei schutzbedürftigen Räumen wie Serverraum, Beleg- oder Datenträgerarchiv sinnvoll. Bei hochschutzbedürftigen Räumen ist ein ausgewogenes Schutzkonzept zu erstellen, welches den Einbau von Sicherheitstüren und die Gefahrenmeldung und Alarmierung zur Prüfung und Intervention berücksichtigt. Denn hat ein potentieller Angreifer ein ganzes Wochenende Zeit für einen Einbruchsversuch, wird ihn auch eine hochwertige einbruchhemmende Tür nicht von seinem Ziel abhalten, Daten oder Einrichtung zu entwenden oder zu zerstören.

Für die Ausstattung von Rechenzentren sollte für die Türen inklusive deren Einbausituation die Widerstandsklasse RC3 gemäß DIN EN 1627-1630:2011 als Mindestwert angesetzt werden. Lediglich wenn für die Sicherheit ganz besonders günstige Bedingung vorliegen, insbesondere falls die Interventionszeit hilfeleistender Kräfte kurz ist (maximal 2 Minuten), kann in Ausnahmefällen eine RC2-Tür ausreichen. Liegt die Interventionszeit hilfeleistender Kräfte hingegen bei 5 Minuten und höher, ist sogar eine RC3-Tür als unzureichend anzusehen und es empfiehlt sich der Einbau von RC4-Türen. Sinngemäß gelten die gleiche Überlegungen natürlich auch für alle anderen, die RZ-Hülle bildenden Bauelemente.

Hinweis: Ziel eines Einbruches könnte es auch sein, Daten oder IT-Systeme zu manipulieren. Daher sollten zentrale IT-Systeme nach Einbrüchen auf ihre Integrität überprüft werden (siehe dazu auch M 6.60 Festlegung von Meldewegen für Sicherheitsvorfälle).

Es ist dafür zu sorgen, dass Brand- und Rauchschutztüren auch tatsächlich geschlossen und nicht (unzulässigerweise) z. B. durch Keile offen gehalten werden. Alternativ können Türen mit einem automatischen Schließmechanismus, der im Alarmfall aktiviert wird, eingesetzt werden.

Außerdem ist regelmäßig zu prüfen, dass die Sicherheitstüren und -fenster funktionstüchtig sind. Sie müssen in einem ordentlichen mechanischen Zustand sein, sicher öffnen und schließen und überwachende Installationen wie Schließkontakte müssen funktionieren.

INF.1.M23 Bildung von Sicherheitszonen [Planer] (C)

Der Schutzbedarf von Räumen in einem Gebäude hängt von ihrer Nutzung ab. Die erforderlichen Sicherheitsmaßnahmen müssen diesem Schutzbedarf angepasst sein. Entsprechend muss die bauliche Ausführung von Wänden, Fenstern und Türen sein und die ergänzende Ausstattung mit Sicherheits- und Überwachungstechnik. Bei der Planung eines neuen Gebäudes oder der Bewertung eines Bestandsgebäudes sollten deshalb Räume ähnlichen Schutzbedarfs in Zonen zusammengefasst werden. Damit lassen sich vergleichbare Risiken einheitlich behandeln und die Kosten der Umsetzung von Maßnahmen werden reduziert.

Um z. B. nicht jeden einzelnen Raum im Gebäude permanent abschließen oder überwachen zu müssen, sollten Zonen mit Besucherverkehr von schutzbedürftigen Bereichen getrennt werden. Öffentliche Räume wie eine Kantine, die externes Publikum anzieht, oder halb-öffentliche Räume wie Besprechungs-, Schulungs- oder Veranstaltungsräume sollten in der Nähe des Gebäudeeingangs angeordnet sein. Der Zugang zu Gebäudeteilen mit internen Bereichen wie den Büros kann dann z. B. von einem Pförtner einfach überwacht werden. Besonders sensitive Bereiche wie eine Entwicklungsabteilung, Räume der Gebäudetechnik oder IT-Räume sollten mit einer zusätzlichen Zugangskontrolle abgesichert werden.

Zur physischen Sicherung eines Gebäudes und gegebenenfalls des umgebenden Grundstücks hat es sich bewährt, ein Sicherungskonzept mit tiefengestaffelten Sicherheitsmaßnahmen (Zwiebelschalenprinzip) zu planen und umzusetzen. Bewährt ist eine Aufteilung in vier Sicherheitszonen, Außenbereich, kontrollierter Innenbereich, interner Bereich und Hochsicherheitsbereich:

Abbildung: Bildung von Sicherheitszonen

Die Sicherheitszone 0, also der Außenbereich, wird von der Grundstücksgrenze umfasst. Wenn die Situation es zulässt, sollte diese juristische Grenze deutlich durch eine Einfriedung angezeigt werden. Hier kann bereits die erste Zutritts- und Zufahrtskontrolle vorgenommen werden. Öffentliche Gebäudebereiche sind dieser Zone zuzurechnen.

Die Sicherheitszone 1 ist der kontrollierte Innenbereich. Durch eine angemessene Zutrittskontrolle, z. B. einen Pförtner oder ein Zutrittskontrollsystem, erhalten nur Berechtigte (Mitarbeiter, geladene Besucher) Zutritt zu dieser Zone. Bei hohem Schutzbedarf sollte in dieser Zone bereits die Verpflichtung bestehen, stets sichtbar Ausweise zu tragen. Die Außenhaut der Zone 1 (Gebäudeaußenhaut) sollte durch bauliche und technische Maßnahmen gegen Sabotage und Einbruch geschützt werden.

Die Zone 2 als interner Bereich ist nur für einen eingeschränkten Kreis von Berechtigten zu betreten. Hier gibt es definierte Zutrittsberechtigungen. Räume oder Gebäudeabschnitte der Zone 2 sollten jeweils nur einen Zugang aufweisen. Weitere Zuwegungen dienen ausschließlich als Flucht- und Rettungswege und sind im Betrieb immer geschlossen zu halten. Sie sind permanent zu überwachen und durch elektromechanische Sicherungseinrichtungen (Fluchtwegsicherungssysteme) gegen missbräuchliche Nutzung zu sichern.

Die Zone 3 bildet den Hochsicherheitsbereich (z. B. Vorstandsbereiche, kritische IT-Räume). Der Kreis der Zutrittsberechtigten ist sehr eingeschränkt. Die Sicherheitsmaßnahmen sollten entsprechend hoch sein. Beispiel: Der Zutritt ist nur über eine Sicherheitsschleuse mit Zwei-Faktor-Authentisierung und Vereinzelung, der Austritt mit Ein-Faktor-Authentisierung und Vereinzelung möglich. Es erfolgt eine Bilanzierung des Zutritts, sobald keine Personen mehr als anwesend gemeldet sind, erfolgt die automatische Scharfschaltung der Einbruchmeldeanlage.

Poststellen, Anlieferungs- und Ladezonen sollten sich in Sicherheitszone 1 befinden. Sie sollten so gestaltet sein, dass Lieferungen angenommen werden können, ohne dass die Lieferanten weitere Bereiche des Gebäudes betreten müssen. Die Türen in diesen Bereichen sollten nicht über längere Zeit offenstehen. Bei höherem Schutzbedarf sollte sich entweder nur die Außentür oder die Tür zu den inneren Bereichen öffnen lassen. Eingehende Lieferungen sollten in der Lieferzone daraufhin untersucht werden, ob damit Risiken verbunden sein könnten. Die Art und Tiefe der Überprüfungen ist abhängig vom jeweiligen Gefährdungspotential (z. B. Briefbomben). Ein- und ausgehende Lieferungen sollten möglichst getrennt voneinander aufbewahrt werden.

INF.1.M24 Selbsttätige Entwässerung (A)

Alle Bereiche innerhalb von Gebäuden, in denen sich Wasser sammeln und stauen kann oder in denen fließendes oder stehendes Wasser nicht oder erst spät entdeckt wird und in denen das Wasser Schäden verursachen kann, sollten mit einer selbsttätigen Entwässerung und mit Wassermeldern ausgestattet sein. Zu diesen Bereichen gehören u. a.:

- Keller,
- Lufträume unter Doppelböden,
- Lichtschächte,
- Heizungsanlage.

Erfolgt die Entwässerung passiv, also durch Bodengullys direkt in das Abwassersystem des Gebäudes, sind Rückstauklappen unerlässlich. Ohne solche Klappen wird diese Entwässerung zur Wassereintrittsöffnung, wenn das Abwassersystem überlastet wird. Nach extremen Niederschlägen dringt in der Mehrzahl aller Fälle Wasser über diesen Weg in Keller ein. Die Rückstauklappen müssen regelmäßig auf ihre Funktionstüchtigkeit hin untersucht werden.

Ist eine passive Entwässerung nicht möglich, weil das Niveau des Abwassersystems zu hoch ist, können Pumpen eingesetzt werden, die über Schwimmerschalter oder Wassersensoren automatisch eingeschaltet werden. Beim Einsatz dieser Technik sind insbesondere folgende Punkte zu beachten:

- Die Pumpenleistung muss ausreichend bemessen sein.
- Die Druckleitung der Pumpe ist mit einem Rückstauventil auszustatten.
- Es sind Vorkehrungen zu treffen, damit die Pumpe nicht durch mitgeschwemmte Gegenstände blockiert werden kann (Ansaugfilter etc.).
- Das Anlaufen der Pumpe sollte automatisch (z. B. beim Hausmeister oder der Haustechnik) angezeigt werden.
- Die Funktion von Pumpe und Schalter ist regelmäßig zu testen.
- Die Druckleitung der Pumpe darf nicht an eine in unmittelbarer Nähe vorbeigeführte Abwasserleitung angeschlossen werden. Bei einem Leck dieser Leitung würde die Pumpe das Wasser nur "im Kreis pumpen".

Um zu verhindern, dass Wasser z. B. bei Starkregen von Außen in das Gebäude dringt, ist auch der Zustand der Grundstücksentwässerung zu prüfen und diese gegebenenfalls instand zu setzen. Falls die Lage oder das Profil des Grundstücks besondere Gefährdungen des Gebäudes durch Oberflächenwasser mit sich bringen, kann der Einbau besonderer Wasserschutztüren erwogen werden.

INF.1.M25 Geeignete Standortauswahl [Institutionsleitung] (A)

Bei der Auswahl und Planung des Standortes, an dem ein Gebäude angemietet werden oder entstehen soll, empfiehlt es sich, neben den üblichen Aspekten wie Raumbedarf und Kosten, auch Umfeldgegebenheiten, die Einfluss auf die Informationssicherheit haben, zu berücksichtigen:

- In Zusammenhang mit Schwächen in der Bausubstanz kann es durch Erschütterungen naher Verkehrswege (Straße, Eisenbahn, U-Bahn) zu Beeinträchtigungen der IT kommen.
- Gebäude, die direkt an Hauptverkehrstrassen (Eisenbahn, Autobahn, Bundesstraße, Flughafen) liegen, können durch Unfälle beschädigt werden.
- Die Nähe zu optimalen Verkehrs- und somit Fluchtwegen kann die Durchführung eines Anschlages erleichtern.
- In der Nähe von Sendeeinrichtungen kann es zu Störungen der IT kommen.
- In der Nähe von Eisenbahnlinien kann es zur Störung der IT kommen.
- In der Nähe von Gewässern und in Niederungen ist mit Hochwasser zu rechnen.
- In der Nähe von Kraftwerken oder Fabriken kann durch Unfälle oder Betriebsstörungen (Explosion, Austritt schädlicher Stoffe) die Verfügbarkeit des Gebäudes (z. B. durch Evakuierung oder großräumige Absperrung) beeinträchtigt werden.

Es kann auch möglich sein, Gefährdungen aus der Nachbarschaft z. B. durch passende Anordnung schützenswerter Gebäudeteile zu kompensieren. Dies sollte bei der Auswahl und Planung berücksichtigt werden.

Die standortbedingten Gefährdungen und die erforderlichen schadensvorbeugenden oder -reduzierenden Maßnahmen sollten im Sicherheitskonzept dokumentiert werden. Außerdem sollten sie ins Notfallkonzept einfließen.

INF.1.M26 Pförtner- oder Sicherheitsdienst (CIA)

Die Einrichtung eines Pförtner- oder Sicherheitsdienstes hat weitreichende positive Auswirkungen gegen eine ganze Reihe von Gefährdungen. Voraussetzung ist allerdings, dass bei der Durchführung des Pförtner- oder Sicherheitsdienstes einige Grundprinzipien beachtet werden. Der Fokus des Pförtnerdienstes liegt naturgemäß darauf, Zutritte während der Geschäftszeiten zu kontrollieren, während Sicherheitsdienste vor allem außerhalb der Geschäftszeiten die Liegenschaft überwachen und absichern.

- Die Pförtner sollten alle Personenbewegungen an der Pforte und an allen anderen Eingängen beobachten und kontrollieren.
- Unterstützt durch Videoüberwachung können entfernte Türen und Tore von den Pförtnern überwacht und auch gesteuert werden (siehe Kapitel 3.2 Videoüberwachung).
- Den Pförtnern müssen die Mitarbeiter bekannt sein. Es ist zu empfehlen, dass sich auch bekannte Personen bei den Pförtnern legitimieren, also z. B. einen Hausausweis vorzeigen. Scheidet ein Mitarbeiter aus der Institution aus oder ändert seine Position innerhalb der Institution, sind auch die Pförtner zu unterrichten, ab wann diesem Mitarbeiter der Einlass zu verwehren ist oder ob sich Zutrittsberechtigungen ändern.
- Unbekannte Personen ("selbst der neue Chef") haben sich bei den Pförtnern auszuweisen.
- In einem Besucherbuch kann der Zutritt von Fremdpersonen zum Gebäude dokumentiert werden. Die Ausgabe von Besucherausweisen oder Besucherbegleitscheinen ist zu erwägen.

- Besucher sollten zu den Besuchten begleitet oder an der Pforte abgeholt werden. Falls Besucher unbegleitet das Gebäude betreten dürfen, muss vorher verifiziert werden, dass dies ohne Sicherheitsbedenken möglich ist. Die jeweiligen Rahmenbedingungen sind vorab zu dokumentieren. Beispielsweise könnte eine Liste mit vertrauenswürdigen Dauerbesuchern geführt werden, die nach Erhalt eines Besucherausweises das Gebäude ohne Begleitung betreten dürfen.
- Wenn die Pforte rund um die Uhr besetzt ist, können dort immer oder nur außerhalb der normalen Dienstzeiten Meldungen der alarmierenden und überwachenden Technik auflaufen. Anhand von Alarmlisten zu den Meldungen leitet die Pforte die Meldungen an zuständige Mitarbeiter in Bereitschaft oder zuständige externe Stellen weiter.

Die Arbeitsbedingungen der Pförtner und des Sicherheitspersonals sind für die Aufgabenwahrnehmung geeignet auszugestalten. Die Aufgabenbeschreibung muss verbindlich festschreiben, welche Aufgaben den Pförtnern oder den Mitarbeitern des Sicherheitsdienstes im Zusammenspiel mit weiteren Schutzmaßnahmen zukommt (z. B. Gebäudesicherung nach Dienst- oder Geschäftsschluss, Scharfschaltung der Alarmanlage, Kontrolle der Außentüren und Fenster).

Bei der Definition der Aufgaben muss beachtet werden, dass die zugewiesenen Aufgaben keine Sicherheitslücken aufreißen. Wenn eine Pforte mit nur einem Pförtner besetzt ist und dieser keine Möglichkeit hat, die Pforte vorübergehend zu verschließen, so darf er nicht die Anweisung haben oder erhalten, Besucher selbst zu bestimmten Besuchten zu begleiten.

In vielen Institutionen werden Pförtner- und Wachdienste durch externe Sicherheitsdienstleister übernommen, siehe hierzu OPS 4.2 Sonstige Dienstleistungen.

INF.1.M27 Einbruchsschutz (CIA)

Erfahrungsgemäß wählen Einbrecher ihre Ziele danach aus, wie hoch das Risiko und Aufwand im Verhältnis zum erwarteten Gewinn sind. Daher sollten alle Maßnahmen zum Einbruchsschutz darauf zielen, die Erfolgsaussichten von Tätern zu minimieren. Die gängigen Maßnahmen zum Einbruchsschutz sollten den örtlichen Gegebenheiten entsprechend angepasst werden. Dazu gehören:

- einbruchhemmende Türen und Fenster, beispielsweise mit der Widerstandsklasse RC2 (nach DIN EN 1627:2011-09 "Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchhemmung - Anforderungen und Klassifizierung") oder höherwertig, wenn die Gefährdungslage es erforderlich macht,
- Rollladensicherungen bei einstiegsgefährdeten Türen oder Fenster,
- besondere Schließzylinder, Zusatzschlösser und Riegel,
- Sicherung von Kellerlichtschächten,
- Verschluss von nicht benutzten Nebeneingängen,
- einbruchgesicherte Notausgänge,
- Verschluss von Personen- und Lastenaufzügen außerhalb der Dienstzeit.

Empfehlungen hierzu geben die örtlichen Beratungsstellen der Kriminalpolizei.

Alle Maßnahmen zum Einbruchsschutz sollten sinnvoller Weise eine durchgehend gleichwertige Hülle um den Bereich bilden, der gegen unbefugten Zutritt geschützt werden soll. Türen sind in ausreichend feste Wände einzubauen. Lüftungsöffnungen sind in geeigneter Form zu vergittern (maximale Gitterweite 10x20 cm). Auch in Doppelbodenbereichen und über abgehängten Decken sind Maßnahmen zum Zutrittsschutz umzusetzen. Die Gleichwertigkeit und Durchgängigkeit des Einbruchsschutzes sollte durch eine fachkundige Person während der Planung, bei der Umsetzung und später im Betrieb regelmäßig begutachtet werden.

Bei der Planung materieller Sicherungsmaßnahmen ist darauf zu achten, dass Bestimmungen des Brand- und Personenschutzes, z. B. die Nutzbarkeit von Fluchtwegen, nicht verletzt werden. Dies gilt insbesondere für Änderungen an Brandschutzelementen, die einer Typenfreigabe unterliegen.

Den Mitarbeitern ist bekanntzugeben, welche Regelungen und Maßnahmen zum Einbruchsschutz beachtet werden müssen, also beispielsweise dass Türen, Fenster oder Rollladensicherungen abends abgeschlossen werden müssen.

Auch innerhalb eines Gebäudes kann der Einbau von einbruchhemmenden Elementen sinnvoll sein. Die Absicherung ist zu erwägen bei besonderen zutrittskontrollierten Bereichen wie den Räumen der Geschäftsleitung, Serverräumen oder den Kerneinheiten eines Rechenzentrums.

INF.1.M28 Klimatisierung für Menschen (IA)

In größeren Gebäuden sollte die Luftversorgung durch raumlufttechnische (RLT-) Anlagen geleistet werden. RLT-Anlagen sorgen für den Transport (Lüftung) und die Konditionierung (Klimatisierung) der Luft. RLT-Anlagen sollen ein für Menschen günstiges Raumklima schaffen. Zudem müssen sie eine hygienisch einwandfreie Qualität der Innenraumluft sicherstellen. Das heißt, dass die durch eine RLT-Anlage aufbereitete Luft keine Gefährdung der Gesundheit oder Störungen der Befindlichkeit mit sich bringt, Geruchsbelästigungen unterbleiben und die thermische Behaglichkeit erhalten bleibt.

Eine gute Luftqualität kann nicht ausschließlich durch die RLT-Anlage erzeugt werden. Auch bei der Auswahl der Bauwerkstoffen, Bodenbelägen und Möbeln muss auf den Einsatz von Materialien geachtet werden, die die Raumluft nicht zusätzlich und unnötig mit Schadstoffen belasten.

Die Planung von Lüftungs- und Klimaanlagen nach Stand der Technik für Nichtwohngebäude ist in der DIN EN 13779 "Lüftung von Nichtwohngebäuden - Allgemeine Grundlagen und Anforderungen für Lüftungs- und Klimaanlagen und Raumkühlsysteme" beschrieben. Zusammen mit der Arbeitsstättenverordnung legt sie fest, in welchen Räumen des Gebäudes welche Anforderungen an die Luftqualität zu erfüllen sind. Die DIN EN 13779 enthält detaillierte Festlegungen für

- die operative Temperatur
- das Zugluftrisiko
- die relative Raumluftfeuchte
- die bewerteten Schalldruckpegel
- und weitere für Menschen relevante Faktoren.

Während für Büros und sonstige ständig besetzte Räume hohe Anforderungen an die Luftqualität bestehen, ist der Anspruch in nicht ständig besetzten Räumen geringer. Umso wichtiger ist, dass, wie auch in der Norm gefordert, die Vorgaben für die Klimaplanung vom Bauherrn oder dem zukünftigen Nutzer vorgegeben werden.

Während Kälte fast nie ein Problem bei Erzeugung eines behaglichen Raumklimas darstellt, kann sommerliche Hitze ein größeres Problem sein. Die Arbeitsstättenverordnung fordert für Arbeitsräume gesundheitlich zuträgliche Raumtemperaturen und den Schutz gegen übermäßige Sonneneinstrahlung. Um an warmen Sommertagen ein erträgliches Raumklima zu erhalten, muss die RLT-Anlage durch eine wirkungsvolle Beschattung der Fenster unterstützt werden.

RLT-Anlagen müssen regelmäßig gewartet werden. Bei RLT-Anlagen dienen Wartungsarbeiten nicht nur dazu, den zuverlässigen Betrieb zu sichern, sondern auch dazu, Hygiene und damit die Gesundheit aller Nutzer des Gebäudes zu garantieren. Die Einhaltung von Wartungsintervallen und die sorgfältige Durchführung von Reinigungsarbeiten und Filterwechseln muss kontrolliert und dokumentiert werden.

RLT-Anlagen dürfen nicht für jedermann zugänglich sein und müssen gegebenenfalls gegen Sabotage materiell geschützt werden. Die RLT-Anlagen müssen auch bei der Notfallplanung (siehe Baustein DER.4 Notfallmanagement), insbesondere bei Abschalt- und Wiederanlaufplanungen, berücksichtigt werden.

INF.1.M29 Organisatorische Vorgaben für die Gebäudereinigung (CIA)

Mit der Durchführung von Reinigungsarbeiten werden fast ausschließlich externe Unternehmen beauftragt, siehe auch OPS.4.2 Sonstige Dienstleistungen. Das nicht zur eigenen Institution gehörende Reinigungspersonal muss alle Räume und Bereiche des Gebäudes betreten, auch Gebäudeteile, wie Technikräume oder Vorstandsetagen, zu denen nur bestimmte Mitarbeitergruppen Zutritt haben. Desweiteren benutzen die externen Reinigungskräfte häufig eigenes Arbeitsgerät und bringen je nach Vertrag auch Reinigungsmittel und andere Verbrauchsstoffe mit. Damit werden Schwachstellen geschaffen, da beispielsweise so auch internes Material auf dem Rückweg mitgenommen werden könnte.

Neben allgemeinen Merkmalen eines Leistungsverzeichnisses für Reinigungsarbeiten wie Art, Name und Lage des Objektes sind Raumnutzungsgruppen, aktuelle Raumverzeichnisse sowie die einzelnen Leistungsarten detailliert zu beschreiben. Leistungsarten können z. B. die Reinigung nichttextiler und textiler Beläge, die Reinigung und Pflege von Gegenständen der Raumausstattung und Einrichtung sowie Entsorgungsaufgaben sein. Darauf aufbauend werden die einzelnen Anforderungen mit Angabe des Umfanges in den einzelnen Räumen beschrieben.

Um den Arbeitsprozess nicht zu stören, werden Reinigungsarbeiten oft in die arbeitsfreien Zeiten verlegt. Damit muss aber auch geklärt werden, ob das Reinungspersonal beaufsichtigt werden sollte. Vorstellungen zu den Reinigungszeiten sowie die Sonderbehandlung einzelner besonders schutzbedürftiger und nicht unkontrolliert begehbarer Bereiche sind in der Leistungsbeschreibung aufzuführen.

Reinigungspersonal sollte vor Aufnahme ihrer Tätigkeit in die Aufgaben eingewiesen werden. Hierzu gehört vor allem eine Einweisung, welche Bereiche unter welchen Voraussetzung betreten werden dürfen, wie IT-Systeme zu reinigen sind und was in der Umgebung von IT-Systemen zu beachten ist und wie sie mit vertraulichen Informationen umzugehen haben, die sie während ihrer Arbeit erhalten. Dies können z. B. Unterlagen sein, die sich auf Schreibtischen oder in Papierkörben finden, oder mitgehörte Gespräche.

Der Zutritt von Reinigungspersonal kann insbesondere in Bereichen mit höheren Sicherheitsanforderungen wie Rechenzentren, Serverräumen, Technikräumen oder Kommunikationszentralen problematisch sein und daher zusätzliche Sicherheitsmaßnahmen erfordern. In solchen Bereichen kann es sinnvoll sein, die Vertrauenswürdigkeit des Reinigungspersonals zu überprüfen oder diese während ihrer Tätigkeit zu beaufsichtigen.

Wenn Vertrauen in die Reinigungsfirma besteht, sollte der Zutritt der Reinigungskräfte über die vorhandene Zutrittskontrolle oder das Schließsystem geregelt werden. Das kann jedoch nur dann eine wirksame Sicherungsmaßnahmen sein, wenn z. B. Ausweis oder Schlüssel gegen Unterschrift und nur zeitlich begrenzt an benannte und bekannte Mitarbeitern der Reinigungsfirma ausgegeben werden. Bei der Vereinbarung über die Verwendung von Stammpersonal kann über das Ausweissystem eine wirksame Kontrolle der Vertragseinhaltung erreicht werden.

Für die Koordination, aber auch bei auftretenden Problemen ist vom Auftragnehmer ein Objektverantwortlicher zu benennen, der jederzeit ansprechbar ist. Er muss Entscheidungsbefugnis über das einzusetzende (vor allem auch über nicht mehr einzusetzendes, weil unerwünschtes) Personal haben.

Bereits in der Ausschreibung und der Vertragsformulierung ist die Sonderbehandlung sensitiver Bereiche einzubeziehen. Zum Beispiel sind bei Rechenzentren stichprobenartige Kontrollen von Taschen oder Transportgut im Zugangs- oder Zufahrtsbereich für betriebsfremdes Personal in den Verträgen festzuschreiben.

Da bei Reinigungskräften IT-Kenntnisse nicht vorausgesetzt werden können, sollten diese daher in allen Bereichen mit geschäftskritischen IT-Systemen dahingehend eingewiesen werden, welche Tätigkeiten zu Schäden an IT-Einrichtungen oder Problemen beim IT-Betrieb führen können. Beispiele für solche Problemfelder sind:

- Bei der Reinigung von Tastaturen können unbeabsichtigt Eingaben an Servern oder anderen zentralen Komponenten erfolgen, die den IT-Betrieb beeinträchtigen.
- IT-Systeme können versehentlich ausgeschaltet werden.
- Stromversorgungs- oder Kommunikationskabel können durch Staubsauger beschädigt oder aus den Endpunkten gerissen werden.
- Durch Wasser oder Reinigungsflüssigkeit können Kurzschlüsse in Hardware-Komponenten verursacht werden.

Bereiche mit einem erhöhten Sicherungsbedarf wie Maschinensaal oder Datenträgerarchiv sind nur unter Anwesenheit von Verantwortlichen des Auftraggebers oder in einigen Fällen auch unter Anwesenheit einer Vertrauensperson des Auftragnehmers, z. B. im Vier-Augen-Prinzip, zu reinigen.

INF.1.M30 Auswahl eines geeigneten Gebäudes (CIA)

Neben der Standortplanung (siehe INF.1.M 25 Geeignete Standortauswahl), die das Umfeld eines Gebäudes betrachtet, muss ein Gebäude hinsichtlich seiner inneren Eignung beurteilt werden. Grundsätzlich ist natürlich schon bei der Gebäudeauswahl zu prüfen, ob alle für die spätere Nutzung relevanten Maßnahmen dann auch umgesetzt werden können.

Für einige dieser Maßnahmen können die Voraussetzung nachträglich jedoch nur mit extrem hohem Aufwand oder gar nicht geschaffen werden. Diese Maßnahme soll daher bei der Auswahl eines bestehenden Gebäudes helfen, typischerweise erst später auftretende Probleme im Vorfeld so weit wie möglich zu vermeiden. Sie kann aber auch bei der Planung eines Neubaus hilfreich sein.

Einzelne Aspekte sind je nachdem, ob das Gebäude gekauft oder gemietet wird, unterschiedlich relevant. Aus Sicht der Informationssicherheit ist unter anderem Folgendes hinsichtlich des Zustandes der Bausubstanz zu beachten:

- Ermöglicht die Statik (maximale Deckentraglast, tragende Wände) die Einrichtung von Räumen mit hoher Flächenlast (Serverraum, RZ, USV etc.) dort, wo sie arbeitsökonomisch und aus Sicht der Informationssicherheit sinnvoll anzuordnen wären (siehe auch INF.1.34 Anordnung schützenswerter Gebäudeteile)?
- Lassen sich die vorhandenen oder zusätzlich erforderlichen Erschließungswege (Flure, Treppenhäuser, Aufzüge) so nutzen und einrichten, dass Maßnahmen wie z. B. INF.1.M7 Zutrittsregelung und -kontrolle auch sinnvoll umzusetzen sind?
- Ist es auf Grund der Erschließungswege möglich, Bereiche mit hohen Sicherheitsanforderungen von solchen mit niedrigen zu trennen, so dass z. B. Schulungsräume außerhalb von sensitiven Bereichen wie der Produktentwicklung liegen?
- Lassen sich die vorhandenen oder zusätzlich erforderlichen Erschließungswege (Flure, Treppenhäuser, Aufzüge) jederzeit für den Transport auch größerer IT-Komponenten nutzen? Ist dies nicht gewährleistet, kann der Wiederanlauf nach einem Hardwareschaden unter Umständen stark verzögert werden.
- Gibt es (Bau-)Auflagen (Wegerechte, Denkmalschutz etc.), die einer bedarfsgerechten Nutzung des Gebäudes hinderlich sein können? Besonders auf Wegerechte Dritter ist hier zu achten, da diese mit erforderlichen zutrittsgeschützten Bereichen kollidieren können.
- Ist eine Raumverteilung möglich, so dass die INF.1.M 3 Einhaltung von Brandschutzvorschriften umgesetzt werden kann?
- Lassen sich INF.1.M 2 Angepasste Aufteilung der Stromkreise und INF.4 IT-Verkabelung umsetzen?
- Gibt es einen äußeren Blitzschutz? Wenn ja, hat das Einfluss auf Details der Umsetzung der Anforderungen INF.3 Elektrotechnische Verkabelung und INF.4 IT-Verkabelung.

Bei Mietobjekten sind zusätzlich folgende Aspekte zu berücksichtigen:

- Erhält der Mieter alle für die geeignete Herrichtung des Gebäudes erforderlichen Rechte? Welche Rechte und Einspruchsmöglichkeiten behält sich der Vermieter vor?
- Müssen Sicherheitseinrichtungen nach Ende des Mietverhältnisses zurückgebaut werden? Es muss in der Planungsphase sichergestellt werden, dass wegen solcher Zusatzkosten nicht auf erforderliche Sicherheitsmaßnahmen verzichtet wird.
- Wenn das Gebäude gleichzeitig von Dritten genutzt wird, ist zu klären, in wie weit dadurch die Umsetzung von Maßnahmen erschwert oder gar verhindert wird.
- Erhält man als Mieter ein Mitspracherecht bei einer späteren Neuvermietung dritt-genutzter Gebäudeteile? Es kann durchaus sein, dass ein neuer Mitnutzer des Gebäudes als sicherheitskritischer angesehen werden muss als der bisherige.Beispiel: Die Personalabteilung eines kleinen Schulbuch-Verlages zieht aus und als Nachmieter richtet dort eine politisch oder gesellschaftlich sehr umstrittene Organisation ein Büro ein.

Es sollte dokumentiert werden, welche Sicherheitsanforderungen bei der Gebäudeauswahl betrachtet wurden. Vor allem sollten eventuell vorhandene Sicherheitsrisiken und die ergriffenen Maßnahmen, um diesen vorzubeugen oder Auswirkungen zu reduzieren, festgehalten werden.

INF.1.M31 Auszug aus Gebäuden [Innerer Dienst] (C)

Wenn ein Gebäude ganz oder teilweise wegen Auszug geräumt wird, sind folgende Dinge zu beachten:

- Im Vorfeld des Auszugs ist ein Bestandsverzeichnis aller für die Informationssicherheit relevanten Dinge (Hardware, Software, Datenträger, Ordner, Schriftstücke etc.) zu erstellen.
- Jeder Beschäftigte ist schriftlich darüber zu informieren, für welche Dinge er zuständig ist. Dadurch wird vermieden, dass sich ein Mitarbeiter sehr wohl um seine eigenen Dinge kümmert, Dinge für die vermeintlich jemand anderer zuständig ist, hingegen liegen bleiben.
- Nicht mehr benötigte Alt-Geräte, Datenträger etc. sind vor dem Auszug entsprechend OPS.1.1.8 Löschen und Vernichten zu entsorgen. Keinesfalls dürfen alte Betriebsmittel einfach zurückgelassen werden, auch wenn der Vermieter, Nachmieter oder Käufer deren weitere Verwendung wünscht oder eine Entsorgung zusagt.
- Nach absolviertem Auszug sind alle Räume daraufhin zu überprüfen, ob auch tatsächlich keine sicherheitskritischen Dinge zurückgelassen wurden. Besonders in entlegenen Abstellbereichen wie Keller und Dachböden werden häufig Dinge vergessen.Alle Gegenstände der dienstlichen Nutzung sind konsequent einzusammeln, zu entfernen und gegebenenfalls nachträglich einer sicheren Entsorgung zuzuführen.

Die Empfehlungen zur Sicherheit bei Umzügen aus ORP.1 Organisation sollten berücksichtigt werden.

INF.1.M32 Brandschott-Kataster (A)

Es sollte ein Brandschott-Kataster geführt werden, das mindestens folgende Anforderungen erfüllt:

- Im Kataster sind alle Schotts aufzunehmen, also reine Kabelschotts, Rohrleitungsschotts, Kombischotts etc.
- Jedes Brandschott im Gebäude bzw. in der Liegenschaft ist im Kataster individuell zu führen.(Die Aufnahme von Schotts in das Kataster kann für solche Schotts entfallen, deren Versagen nachweislich keinerlei nachteiligen Einfluss auf den IT-Betrieb des Gebäudes bzw. der Liegenschaft hat.)
- Jedes Brandschott wird im Kataster unter einer individuellen eindeutigen Kennzeichnung geführt. Diese Kennung ist im unmittelbaren Umfeld des betreffenden Schotts (soweit irgend möglich auf beiden Seiten) gut lesbar anzubringen.
- Im Kataster ist für jedes Schott individuell der Nachweis einer mindestens jährlichen Sichtkontrolle mit den sich dabei ergebenden Feststellungen zu führen.
- In das Kataster sind für Schotts, die zum Zeitpunkt der Erstellung des Katasters schon eingebaut sind, alle verfügbaren Informationen strukturiert aufzunehmen, also mindestens:
- Einbauort
- Hersteller des Schotts
- Produktbezeichnung
- die zum Zeitpunkt der Errichtung gültigen Allgemeinen bauaufsichtlichen Zulassungen (AbZ) oder die allgemeinen bauaufsichtlichen Prüfzeugnisse (AbP). Diese AbZ bzw. AbP sind in der Regel nur 5 Jahre gültig und werden danach entweder verlängert oder aufgehoben. Oft ist es sehr schwer, Hinweise auf abgelaufene AbZ oder AbP im Internet zu finden.
- Einbaudatum
- Einbaufirma und ein aktuelles Foto beider Seiten des eingebauten Schotts.

Bei Bestands-Schotts kann es in Einzelfällen bei unklarer Sachlage zwingend erforderlich sein, es durch ein neues zu ersetzen. Für ein solches Schott gelten dann auch die folgenden Vorgaben:

- Für alle nach der erstmaligen Erstellung des Katasters neu eingebauten oder veränderten Schotts sind über die oben genannten Informationen hinaus mindestens folgende weitere im Kataster aufzunehmen:
- Lückenlose Fotodokumentation aller wesentlichen Einzelschritte des Ein- oder Umbaus,Grund des Umbaus,
- Nachweis, dass die beim Umbau verwendeten Materialien vom Hersteller des Schotts für den Umbau zugelassen sind.
- Alle Eintragungen im Kataster sind unverzüglich vorzunehmen, spätestens 4 Wochen nach Beendigung der Arbeiten.

Nach einem Umbau ist das alte Zertifikat am Einbauort deutlich als ungültig zu kennzeichnen aber so, dass man noch alle relevanten technischen Informationen lesen kann, und durch ein neues, den Umbau berücksichtigende Zertifikat zu ergänzen.

INF.1.M33 Anordnung schützenswerter Gebäudeteile (CIA)

Schützenswerte Räume oder Gebäudeteile sollten nicht in exponierten oder besonders gefährdeten Bereichen untergebracht sein:

- Kellerräume sind eventuell durch Wasser gefährdet.
- Räume im Erdgeschoss - zu öffentlichen Verkehrsflächen hin - sind durch Anschlag, Vandalismus und höhere Gewalt (Verkehrsunfälle in Gebäudenähe) gefährdet.
- Räume im Erdgeschoss mit schlecht einsehbaren Höfen sind durch Einbruch und Sabotage gefährdet.
- Gut einsehbare Räume im Erdgeschoss oder in Bereichen mit Publikumsverkehr sind gefährdet, da dadurch Spontandiebstähle oder unerwünschte Einsichtnahmen in geschäftsrelevante Informationen ermöglicht werden können.
- Räume unterhalb von Flachdächern sind durch eindringendes Regenwasser gefährdet.
- Tiefgaragen können eine ganze Reihe von Risiken mit sich bringen: schlecht einsehbare Hintereingänge, offen zugängliche Versorgungsleitungen oder IT-Verkabelungen, sie bieten aber auch häufig Unbefugten die Möglichkeit, aus Autos heraus auf ungenügend gesicherte WLANs zuzugreifen. Aus Sicht des Brandschutzes sind auch Bereiche in Tiefgaragen problematisch, die als Lagerraum missbraucht werden.

Als Faustregel kann man sagen, dass schutzbedürftige Räume oder Bereiche im Zentrum eines Gebäudes besser untergebracht sind als in dessen Außenbereichen.

Optimal ist es, diese Aspekte schon in die Bauplanung für ein neues Gebäude oder in die Raumbelegungsplanung bei Einzug in ein bestehendes einzubeziehen. Bei bereits genutzten Gebäuden wird eine entsprechende Nutzungsanordnung oft mit internen Umzügen verbunden sein. Ersatzweise sollten die sich aus ohnehin erforderlichen Änderungen der Raumbelegung ergebenden Gelegenheiten konsequent genutzt werden.

Wenn schützenswerte Räume nicht anders als in exponierter Lage angeordnet werden können, so sollte das explizit im Sicherheitskonzept dokumentiert werden. Außerdem sind zusätzliche kompensierende Maßnahmen zu ergreifen, die der besonderen Gefährdung entgegenwirken. So kann z. B. bei elektrischen Betriebsräumen oder IT-Räumen im Keller eine bestehende Gefährdung durch Wasser durch umfassende Wasserdetektion, Schwellenbildung und Vorbereitung von Entwässerungsmaßnahmen beherrscht werden.

INF.1.M34 Gefahrenmeldeanlage (A)

Eine Gefahrenmeldeanlage (GMA) besteht aus einer Vielzahl lokaler Melder, die mit einer Zentrale kommunizieren, über die auch der Alarm ausgelöst wird. Ist eine Gefahrenmeldeanlage für Einbruch, Brand, Wasser oder auch Gas vorhanden und lässt sich diese mit vertretbarem Aufwand entsprechend erweitern, sollten zumindest die Kernbereiche der IT (Serverräume, Datenträgerarchive, Räume für technische Infrastruktur u. ä.) in die Überwachung durch diese Anlage mit eingebunden werden. So lassen sich Gefährdungen wie Feuer, Einbruch, Diebstahl frühzeitig erkennen und Gegenmaßnahmen einleiten.

Um dies zu gewährleisten, ist die Weiterleitung der Meldungen an eine ständig besetzte Stelle (Pförtner, Wach- und Sicherheitsdienst, Feuerwehr, etc.) unumgänglich. Dabei muss sichergestellt sein, dass diese Stelle auch in der Lage ist, technisch und personell auf den Alarm zu reagieren. Hierbei sind die Aufschaltrichtlinien der jeweiligen Institutionen und die Anforderungen der DIN EN 50518 "Notruf- und Serviceleitstellen" zu beachten.

Es sollte ein Konzept für die Gefahrenerkennung, Weiterleitung und Alarmierung für die verschiedenen Gebäudebereiche erstellt werden. Dieses muss an Veränderungen bei der Nutzung angepasst werden. Eine Gefahrenmeldeanlage ist ein komplexes Gesamtsystem, das dem Gebäude und dem Risiko entsprechend geplant und installiert werden muss. Planung, Installation und Wartung einer Gefahrenmeldeanlage sollte daher durch Experten durchgeführt werden. Falls diese nicht im eigenen Haus vorhanden sind, sollte auf externe Unterstützung zurückgegriffen werden. So gibt es beispielsweise eine Vielzahl unterschiedlicher Meldesysteme, die entsprechend der Sicherheitsanforderungen und der Umgebung ausgewählt werden müssen. Zur Einbruchserkennung können z. B. Bewegungsmelder, Glasbruchsensoren, Öffnungskontakte, Videokameras u. a. eingesetzt werden.

Die Melder können untereinander auf verschiedene Arten vernetzt werden. In Abhängigkeit von Art und Größe der zu schützenden Bereiche und der geltenden Richtlinien müssen passende Systeme ausgewählt und installiert werden. Bei der Planung oder Erweiterung einer GMA sollte darauf geachtet werden, dass die Trassen für die Vernetzung ausreichend dimensioniert sein müssen und möglichst wenig Änderungen an der Trassenbelegung vorgenommen werden sollten.

Um die Schutzwirkung der GMA aufrechtzuerhalten, ist eine regelmäßige Wartung und Funktionsprüfung (siehe DIN VDE 0833 Teil 1-3 "Gefahrenmeldeanlagen für Brand, Einbruch und Überfall") vorzusehen.

Ist keine GMA vorhanden oder lässt sich die vorhandene nicht nutzen, kommen als Minimallösung lokale Gefahrenmelder in Betracht. Diese arbeiten völlig selbständig, ohne Anschluss an eine Zentrale. Die Alarmierung erfolgt vor Ort oder mittels einer einfachen Zweidrahtleitung (eventuell Telefonleitung) an anderer Stelle.

Es gibt Räume wie Serverraum, Datenträgerarchiv, die einen erhöhten Schutzbedarf haben. Wenn keine zentrale GMA vorhanden ist, sind dort lokale Gefahrenmelder zu installieren. Bei der Verwendung lokaler Gefahrenmelder für die Früherkennung muss dafür gesorgt werden, dass ein Alarm auch außerhalb der betroffenen Räume wahrgenommen wird. Die Meldung kann über verschiedene Wege erfolgen und sollte an eine Stelle weitergeleitet werden, die rund um die Uhr besetzt ist. Beispielsweise gibt es Lösungen, die über die TK-Anlage oder Funk Mitarbeiter über ein Mobiltelefon alarmieren können.

Vor der Planung einer GMA muss ein konsistentes Schutzkonzept für das betrachtete Gebäude erarbeitet werden. Bei der Planung von Gefahrenmeldeanlagen für private bzw. gewerbliche Objekte sollte mit dem Sachversicherer geklärt werden, ob eine Minderung der Versicherungsprämie, insbesondere für die Einbruch-Diebstahlversicherung in Frage kommt.

3 Weiterführende Informationen

3.1 Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Allgemeines Gebäude" finden sich unter anderem in folgenden Veröffentlichungen:

[27001A11] ISO/IEC 27001:2013

Information technology - Security techniques - Information security management systems - Requirements, insbesondere Annex A, A.11 Physical and environmental security, International Organization of Standardization (Hrsg.), ISO/IEC JTC 1/SC 27, Oktober 2013

[DIN0185-3] DIN EN 62305-3:2011-10 Blitzschutz

Teil 3: Schutz von baulichen Anlagen und Personen, Oktober 2011

[DIN0298-4] DIN VDE 0298-4 Verwendung von Kabeln und isolierten Leitungen für Stromanlagen

Teil 4: Empfohlene Werte für die Strombelastbarkeit von Kabeln und Leitungen für feste Verlegung in und an Gebäuden und von flexiblen Leitungen, Juni 2013

[DIN0833-2] DIN VDE 0833-2:2017-10: Gefahrenmeldeanlagen für Brand, Einbruch und Überfall

Teil 2: Festlegungen für Brandmeldeanlagen, Oktober 2017

[DIN0833-4] DIN VDE 0833-4:2014-10: Gefahrenmeldeanlagen für Brand, Einbruch und Überfall

Teil 4: Festlegungen für Anlagen zur Sprachalarmierung im Brandfall, Oktober 2014

[DIN100-444] DIN VDE 0100-444:2010-10 Errichten von Niederspannungsanlagen

Teil 4-444: Schutzmaßnahmen - Schutz bei Störspannungen und elektromagnetischen Störgrößen, Oktober 2010

[DIN100-520] DIN VDE 0100-520:2013-06 Errichten von Niederspannungsanlagen

Teil 5-52: Auswahl und Errichtung elektrischer Betriebsmittel - Kabel- und Leitungsanlagen, Juni 2013

[DIN1047-1] DIN EN 1047-1:2006-01 Wertbehältnisse - Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Brand

Teil 1: Datensicherungsschränke und Diskettenseinsätze, Januar 2006

[DIN1047-2] DIN EN 1047-2:2013-05 Wertbehältnisse - Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Brand

Teil 2: Datensicherungsräume und Datensicherungscontainer, Mai 2013

[DIN1143-1] DIN EN 1143-1:2012-07 Wertbehältnisse - Anforderungen, Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Einbruchdiebstahl

Teil 1: Wertschutzschränke, Wertschutzschränke für Geldautomaten, Wertschutzraumtüren und Wertschutzräume, Juli 2012

[DIN12056] DIN EN 12056-1 bis 4: Schwerkraftentwässerungsanlagen innerhalb von Gebäuden

Januar 2001

[DIN12101-1] DIN EN 12101-1:2006-06 Rauch- und Wärmefreihaltung

Teil 1: Bestimmungen für Rauchschürzen, Juni 2006

[DIN13779] DIN SPEC 13779:2009-12 Lüftung von Nichtwohngebäuden - Allgemeine Grundlagen und Anforderungen für Lüftungs- und Klimaanlagen und Raumkühlsysteme

Dezember 2009

[DIN14073-2] DIN EN 14073-2:004-11 Büromöbel - Büroschränke

Teil 2: Sicherheitstechnische Anforderungen, November 2004

[DIN14096] DIN 14096:2014-05 Brandschutzordnung

Regeln für das Erstellen und das Aushängen, Mai 2015

[DIN15602] DIN EN 15602:2008-04 Sicherheitsdienstleister/Sicherungsdienstleister– Terminologie

April 2008

[DIN1627] DIN EN 1627:2011-09 Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchshemmung - Anforderung und Klassifizierung

September 201

[DIN18082] Verwaltungsvorschrift DIN18082T1EErl MV Einführung tehnischer Baubestimmungen

DIN 18082 Teil 1: Feuerschutzabschlüsse, Stahltüren T30-1, Dezember 1991

[DIN18095-1] DIN 18095-1:1988-10 Türen, Rauchschutztüren, Begriffe und Anforderungen

Oktober 1988

[DIN1986-100] DIN1986-100:2016-12 Entwässerung für Gebäude und Grundstücke

Teil 100: Bestimmungen in Verbindung mit DIN EN 752 und DIN EN 12056, Dezember 2016

[DIN1991] DIN EN 1991 Eurocode 1: Einwirkungen auf Tragwerke

[DIN1992] DIN EN 1992 Eurocode 2: Bemessung und Konstruktion von Stahlbeton- und Spannbetontragwerken

[DIN1993] DIN EN 1993 Eurocode 3: Bemessung und Konstruktion von Stahlbauten

[DIN1994] DIN EN 1994 Eurocode 4: Bemessung und Konstruktion von Verbundtragwerken aus Stahl und Beton

[DIN1995] DIN EN 1995 Eurocode 5: Bemessung und Konstruktion von Holzbauten

[DIN1996] DIN EN 1996 Eurocode 6: Bemessung und Konstruktion von Mauerwerksbauten

[DIN2425-1] DIN 2425-1:1975-08 Planwerke für die Versorgungswirtschaft, die Wasserwirtschaft und für Fernleitungen; Rohrnetzpläne der öffentlichen Gas- und Wasserversorgung

August 1975

[DIN3] DIN EN 3 Tragbare Feuerlöscher

[DIN4102] DIN 4102 Brandverhalten von Baustoffen und Bauteilen

[DIN54] DIN EN 54 Brandmeldeanlagen

[DIN60839-11-1] DIN EN 60839-11-1:2013-12: Alarmanlagen

Teil 11-1: Elektronische Zutrittskontrollanlagen – Anforderungen an Anlagen und Geräte, Dezember 2013

[DIN62305-1] DIN EN 62305-1:015-12; VDE 0185-305-1:2015-12- Entwurf Blitzschutz

Teil 1: Allgemeine Grundsätze (IEC 81/472/CD:2015), Dezember 2015

[DIN77200] DIN 77200:2008-05: Sicherungsdienstleistungen – Anforderungen

Mai 2008

[ISFCF19] The Standard of Good Practice for Information Security

Area CF19 Physical and Environmental Security, Information Security Forum (ISF), June 2018

[NIST80053PEP] Assesing Security and Privacy Controls for Federal Information Systems and Organizations

NIST Special Publication 800-53, Revision 4, insbesondere Appendix F-PS Page F-2013, Family: Physical and environmental protection, April 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf, zuletzt abgerufen am 05.10.2018

[VDI3551] VDI 3551:2011-01

Elektromagnetische Verträglichkeit (EMV) in der Technischen Gebäudeausrüstung, Januar 2011

INF: Infrastruktur

Umsetzungshinweise zum Baustein INF.3 Elektrotechnische Verkabelung

1 Beschreibung

1.1 Einleitung

Die elektrotechnische Verkabelung von IT-Systemen und anderen Geräten umfasst alle Kabel und Verteilungen im Gebäude vom Einspeisepunkt des Verteilungsnetzbetreibers bis zu den Elektro-Anschlüssen der Verbraucher.

Die ordnungsgemäße und normgerechte Ausführung der elektrotechnischen Verkabelung ist Grundlage für den sicheren IT-Betrieb.

1.2 Lebenszyklus

Für die elektrotechnische Verkabelung ist eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung über die Umsetzung bis zum Betrieb. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt. Wie beim Gebäude, so ist auch hier zu beachten, dass die Einflussmöglichkeiten beim Einzug in ein schon bestehendes Gebäude auch bei der Absicherung der Verkabelung wesentlich geringer sind als bei der Errichtung eines Neubaus.

Planung und Konzeption

In der Planungsphase werden die Grundlagen für eine leistungsfähige, gut abgesicherte Verkabelung gelegt. Hierfür sollte eine Anforderungsanalyse im Rahmen der Planung und Konzeption durchgeführt werden (siehe INF.3.M4 Anforderungsanalyse für die elektrotechnische Verkabelung).

Die mechanischen und elektrischen Eigenschaften der Verkabelung werden durch die Auswahl der einzusetzenden Kabeltypen (siehe INF.3.M1 Auswahl geeigneter Kabeltypen) und durch Kabelführung und -trassen und die Umgebungsbedingungen festgelegt (siehe INF.3.M2 Planung der Kabelführung). Durch Auswahl geeigneter Kabeltypen und die typgerechte Verlegung (siehe INF.3.M3 Fachgerechte Installation) muss die elektrotechnische Installation widerstandsfähig gegen Gefährdungen aus dem Umfeld gemacht werden (siehe z. B. INF.3.M6 Überspannungsschutz und INF.3.M12 Vermeidung elektrischer Zündquellen). Bei der Planung sollte nach Möglichkeit auch darauf geachtet werden, dass Leitungen und Haupt- und Unterverteilungen des Gebäudes gegen Missbrauch in geeigneter Weise physisch abgesichert werden (siehe INF.3.M14 Materielle Sicherung der elektrotechnischen Verkabelung und INF.3.M15 Nutzung von Schranksystemen).

Umsetzung

Ein wesentliches Element des Brandschutzes ist die richtige Installation von Kabelkanälen, die durch eine fehlende Brandabschottung erhebliche Risiken verursachen können (siehe INF.3.M8 Brandabschottung von Trassen). Beim Einbau der Verkabelung ist auch auf eine ausführliche und korrekte Dokumentation zu achten, da es im Nachhinein meist sehr schwierig oder sogar unmöglich ist, festzustellen, wo Kabel verlaufen und was sie verbinden (siehe INF.3.M9 Dokumentation und Kennzeichnung der elektrotechnischen Verkabelung und INF.3.M10 Neutrale Dokumentation in den Verteilern). Die elektrotechnische Verkabelung sollte nach Abschluss der Installation einem Abnahmeprozess unterzogen werden, der auch die Aspekte der Informationssicherheit umfasst (siehe INF.3.M5 Abnahme der elektrotechnischen Verkabelung).

Betrieb

Als Grundlage für einen sicheren und störungsfreien Betrieb müssen die Anlagen und ihre Nutzung regelmäßig geprüft werden (siehe INF.3.M11 Kontrolle elektrotechnischer Anlagen und Verbindungen). Bei Arbeiten an Trassen ist sicherzustellen, dass der Brandschutzbeauftragte rechtzeitig in Planung und Ausführung mit einbezogen wird (siehe INF.3.M8 Brandabschottung von Trassen).

Aussonderung

Auch Elektrokabel, die nicht mehr benötigt werden, sind zu entfernen oder fachgerecht außer Betrieb zu nehmen (siehe INF.3.M7 Entfernen und Deaktivieren nicht mehr benötigter Leitungen).

Notfallvorsorge

Sofern erhöhte Anforderungen an die Verfügbarkeit gestellt werden, sollte die Verkabelung, gegebenenfalls einschließlich der externen Anschlüsse, redundant ausgelegt werden (siehe INF.3.M13 Sekundär-Energieversorgung).

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Elektrotechnische Verkabelung" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

INF.3.M1 Auswahl geeigneter Kabeltypen

Bei der Auswahl von Kabeln sind neben den übertragungstechnischen Notwendigkeiten auch die Umgebungsbedingungen bei der Verlegung sowie im Betrieb zu berücksichtigen. Um diesen unterschiedlichen Anforderungen gerecht zu werden, bieten die Kabelhersteller unterschiedliche Arten von Kabeln am Markt an oder entwickeln entsprechende Lösungen.

In Bezug auf den Kabelmantel für Verlegung im Innen- oder Außenbereich müssen folgende Kriterien berücksichtigt werden:

- Temperatur,
- umgebendes Medium (Wasser, Abwasser, Säure, Gas, Licht, Erdreich),
- Nagetierschutz, Hieb- und Spatenstichfestigkeit, Steinschlagfestigkeit, Wasserdruckfestigkeit,
- Funktionserhalt in feuergefährdeten Bereichen,
- spezielle Zugkräfte durch z. B. Freileitungsverwendung.

Außerdem sind die vorgesehenen Trassensysteme zu beachten, wie Kabelpritschen, Kabelleiter, Kabelkanäle, Kabelzugrohre, Kabelformsteine, Steigbereiche und Freileitungsbau.

Der weitere Kabelaufbau muss folgende Faktoren berücksichtigen:

- Zugkräfte durch maschinelle Verlegung, z. B. Kabelzugwinde, Einblassystem oder Handverlegung,
- Biegeradius und Querdruckstabilität, entsprechend Verlegeart und Ruhezustand im Betrieb,
- Feucht- oder Nassbereiche durch Längswasserschutz,
- spezielle Zugkräfte im verlegten Zustand, die durch große Spann- oder Abfangweiten bei Freileitungen oder extremen Steigungen entstehen,
- starke elektrische und induktive Störfelder durch Kabelschirmung.

Die richtige und den Vorschriften gemäße Auswahl von Elektrokabeln und die Beachtung der einschlägigen Normen (DIN VDE 0100 "Bestimmungen für das Errichten von Starkstromanlagen mit Nennspannungen bis 1000 V", DIN 4102 "Brandverhalten von Baustoffen und Bauteilen") und Vorschriften sowie der anerkannten Regeln der Technik stellt die grundlegende Notfallvorsorge der elektrotechnischen Installation dar.

Individuelle Anforderungen für die Auswahl von Kabeln dürfen gerade bei Betriebsumgebungen, in denen Umwelteinflüsse oder besondere bauliche Gegebenheiten zu beachten sind, nicht ausschließlich durch die IT selbst definiert werden. Insbesondere Mitarbeiter der Haustechnik, die mit Betriebsabläufen und sonstigen besonderen Bedingungen vertraut sind, müssen zur geplanten Kabelführung, bei der Feststellung der relevanten Einflüsse und damit der besonderen Anforderung an die Ausführung von Kabeln beteiligt werden.

INF.3.M2 Planung der Kabelführung [Leiter IT]

Bei der Planung von Kabeltrassen ist darauf zu achten, dass erkennbare Gefahrenquellen umgangen werden. Grundsätzlich sollten Trassen nur in den Bereichen verlegt werden, die ausschließlich innerhalb der Räumlichkeiten einer Institution zugänglich sind. Ein übersichtlicher Aufbau der Trassen erleichtert die Kontrolle. Trassen und einzelne Kabel sollten immer so verlegt werden, dass sie vor direkten Beschädigungen durch Personen, Fahrzeuge und Maschinen geschützt sind.

Der Standort von Geräten sollte so gewählt werden, dass die daran angeschlossenen Kabel nicht im Lauf- oder Fahrbereich liegen. Ist dies nicht zu vermeiden, sind die Kabel den zu erwartenden Belastungen entsprechend durch geeignete Kanalsysteme zu schützen. Grundsätzlich ist bei Geräteanschlussleitungen auf eine ausreichende Zugentlastung der Kabel in den Steckern zu achten.

Tiefgaragen stellen ein großes Problem für eine schadensmindernde Kabelführung dar. Durch die Sicherheitsschaltungen und die langen Offenzeiten von Einfahrtstoren ist der Zutritt von Fremdpersonen zu Tiefgaragen nie auszuschließen. Durch die in der Regel geringen Deckenhöhen ist es mit einfachen Mitteln möglich, sich Zugriff zu dort verlaufenden Trassen zu verschaffen. Durch Trassen im Fahrbereich kann die zulässige Fahrzeughöhe unterschritten werden. Beschädigungen oder Zerstörungen der Trassen und Kabel durch zu hohe Fahrzeuge sind dann nicht auszuschließen.

Bei gemeinsam mit Dritten genutzten Gebäuden ist darauf zu achten, dass Kabel nicht in Fußboden-, Decken- oder Wandkanälen durch deren Bereiche führen. Alle Kanalsysteme sind gegenüber den fremd genutzten Bereichen mechanisch fest zu verschließen. Besser ist es, sie an den Bereichsgrenzen enden zu lassen.

Durch Bereiche mit hoher Brandgefahr sollten möglichst keine Kabel verlegt werden. Ist dies nicht möglich und ist der Funktionserhalt aller auf der Trasse liegenden Kabel erforderlich, ist der entsprechende Trassenbereich mit Brandabschottung zu versehen. Ist der Funktionserhalt nur für einzelne Kabel erforderlich, sollte dafür ein entsprechendes Kabel und die dazu gehörige Befestigung gewählt werden. Ein Funktionserhalt-Kabel kann nie allein die geforderte Funktion erfüllen. Die Kabelanlage ist als Ganzes zu betrachten, dazu gehört auch die Befestigung, wie Trassen, Schellen oder Rohre. Ebenso wichtig ist, dass die Kabelanlage nicht durch darüber befindliche Teile ohne Funktionserhalt zerstört werden kann, wenn diese im Brandfall herabfallen.

In Produktionsbetrieben ist mit hohen induktiven Lasten und daraus resultierenden Störfeldern zu rechnen. Auch diese sind bei der Trassen- und Kabelverlegung zu berücksichtigen. Für den Schutz der Kabel gilt sinngemäß das gleiche wie bei der Brandabschottung.

Bei Erdtrassen ist ca. 10 cm über der Trasse ein Warnband zu verlegen. Bei einzelnen Kabeln (ohne Rohr) ist der Einbau von Kabelabdeckungen sinnvoll.

Leitungen müssen so verlegt sein, dass ein Sturm sie nicht bewegen kann. Beispielsweise sollte dafür Sorge getragen werden, dass Leitungen auf freien Dachflächen in zweckmäßiger Weise befestigt sind. Hierbei sollte berücksichtigt werden, dass bei einem Sturm starke Kräfte auf die Kabel oder Kabelstränge wirken können. Außerdem müssen Leitungen geschützt gegen mechanische Beschädigungen verlegt werden, da Gegenstände darauf fallen könnten. Leitungen auf Dachflächen oder in Bereichen, die mit Lamellenwänden verkleidet sind, sollten daher immer in Schutzrohren verlegt sein.

Kabeltrassen (z. B. Fußbodenkanäle, Fensterbank-Kanäle, Pritschen, Rohrtrassen im Außenbereich) sind ausreichend zu dimensionieren. Es muss einerseits genügend Platz vorhanden sein, um eventuell notwendige Erweiterungen des Netzes vornehmen zu können. Andererseits sind zur Verhinderung des Übersprechens (gegenseitige Beeinflussung von Kabeln) eventuell Mindestabstände zwischen den Kabeln einzuhalten. Insbesondere ist bei der Nutzung von gemeinsamen Trassen für Energie- und IT-Verkabelung sicherzustellen, dass die Trassen durch einen Mittelsteg getrennt sind. Schon durch eine einfache getrennte Führung von Stromkabeln und IT-Kabeln lassen sich Störungen der IT meist vermeiden.

Ist es nicht möglich, Trassen mit ausreichenden Reserven zu errichten, sollte zumindest darauf geachtet werden, dass im Bereich der Trassenführung genügend Platz ist, um Erweiterungen unterzubringen. Werden Wand- und Deckendurchbrüche in hinreichender Größe ausgelegt, kann auf spätere lärm-, schmutz- und kostenintensive Arbeiten verzichtet werden. Bei Verwendung von nachinstallationsfähigen Brandschotten können Durchbrüche so gerüstet werden, dass der Schutz vor Feuer und Verrauchung stets gewährleistet ist, zugleich die Nachführung von Kabeln aber jederzeit problemlos möglich bleibt.

Zu beachten ist, dass Durchbrüche durch Wände mit einer Feuerwiderstandsklasse nur zu 60 % belegt werden dürfen, um eine wirksame Schottung dieser Öffnungen erreichen zu können. Gegebenenfalls sollten für spätere Erweiterungen bei der Errichtung Durchbrüche vorgesehen und diese vorerst mittels Weichschott oder Brandschutzkissen verschlossen werden.

Wichtig ist, dass die Trassendimensionierung immer im Zusammenhang mit der Auswahl der Kabeltypen geplant werden muss.

Die Raumbelegung und die Anschlusswerte, für die eine Elektroinstallation ausgelegt wurde, stimmen erfahrungsgemäß nach einiger Zeit nicht mehr mit den tatsächlichen Gegebenheiten überein. Es ist also unerlässlich, bei Änderungen der Raumnutzung und bei Änderungen und Ergänzungen der technischen Ausrüstung (IT, Klimageräte, Beleuchtung, etc.) die Elektroinstallation zu prüfen und gegebenenfalls anzupassen. Das kann in einfachen Fällen durch Umrangierung von Leitungen geschehen. Teilweise kann es aber auch erforderlich werden, zusätzliche bzw. vollkommen neue Einspeisungen, Leitungen, Verteiler etc. zu installieren.

Sowohl mit Blick auf die Sicherheit als auch mit in Betracht der immer schnelleren Datenverbindungen auf Kupferleitungen ist es sehr empfehlenswert, das Stromverteilnetz im gesamten Gebäude komplett als TN-S-System auszulegen. Das ist auch Vorgabe der DIN VDE 0100-444. Dabei werden der PE- und der N-Leiter ab der Potentialausgleichsschiene (PAS) getrennt geführt.

Um die Wirksamkeit des TN-S-Systems dauerhaft zu gewährleisten, muss sichergestellt werden, dass die Verbindung zwischen PE- und N-Leiter an der PAS (Zentraler Erdungspunkt die einzige im gesamten Netz ist. Es kann in der Praxis nicht ausgeschlossen werden, dass beim Anschluss neuer Geräte oder bei Schaltarbeiten im Netz versehentlich eine weitere Verbindung zwischen PE- und N-Leiter geschaffen wird. Daher sollten Änderungen im Datennetz mit der Haustechnik abgestimmt werden. Zudem sollte ein TN-S-System in regelmäßigen Abständen auf korrekte Funktion hin geprüft werden. Das kann bei den ohnehin durchzuführenden Prüfungen des Stromversorgungsnetzes und bei Verdachtsmomenten (beispielsweise länger andauernde unspezifische Störungen im Datennetz) erfolgen. Idealerweise wird ein TN-S-System mit einer permanenten Stromüberwachung des ZEP ausgestattet.

Sobald hohe oder sehr hohe Anforderungen an die Verfügbarkeit der IT gestellt werden, sind eine Versorgung der IT über zwei voneinander unabhängige elektrische Versorgungsstränge und der Einsatz von IT-Geräten mit zwei Netzteilen üblich und angemessen.

Die wichtigen Verbraucher (Speicherkomponenten, zentrale Netzknoten, wichtige Server) werden an die unabhängigen Versorgungen "Netz 1" und "Netz 2" angeschlossen. Andere IT-Komponenten, an die wenige hohe Anforderungen gestellt werden, werden gleichmäßig auf die Versorgungsstränge verteilt.

Hierbei ist besonders bei den nur einfach angeschlossenen Geräten darauf zu achten, dass Geräte, die sich gegenseitig Redundanz geben, nicht an der gleichen Versorgung angeschlossen werden. Zudem müssen die Geräte entsprechend ihrer Leistungsaufnahme gleichmäßig auf beide Stränge verteilt werden, um Netzschieflasten zu vermeiden.

Alle Arbeiten an Rohr- und Kabeltrassen, die in irgendeiner Form Wanddurchbrüche sowie notwendige Flure, Flucht- und Rettungswege berühren, sind ausschließlich im Einvernehmen mit dem Brandschutzbeauftragten durchzuführen Diese Kontaktaufnahme muss schon so deutlich im Vorfeld der eigentlichen Arbeiten erfolgen, dass der Brandschutzbeauftragte ausreichend Gelegenheit hat, alle Aspekte des baulichen vorbeugenden Brandschutzes in die Planung und Durchführung der beabsichtigten Arbeiten einzubringen.

Dem Brandschutzbeauftragten muss, auch während laufender Arbeiten, durch rechtzeitige Information die Gelegenheit gegeben werden, die ordnungsgemäße Ausführung von Brandschutzmaßnahmen zu kontrollieren, bevor diese durch den Baufortschritt nicht mehr zugänglich sind, z. B. weil eine abgehängte Decke bereits geschlossen worden ist.

Die Einbindung des Brandschutzbeauftragten ist durch entsprechende Organisationsanweisungen sicherzustellen und in den Planungs- und Abnahmeunterlagen der Baumaßnahme zu dokumentieren.

INF.3.M3 Fachgerechte Installation

Die Installationsarbeiten der elektrotechnischen Verkabelung müssen sorgfältig und fachkundig erfolgen. Gleichzeitig müssen alle relevanten Normen beachtet werden. Die entscheidenden Kriterien für eine fachgerechte Ausführung der elektrotechnischen Verkabelung müssen daher vom Auftraggeber in allen Phasen überprüft werden. Es ist Aufgabe der ausführenden Firma bei Anlieferung des Materials zu prüfen, ob die richtigen Kabel und Anschlusskomponenten geliefert wurden. Bei der Verlegung von Stromkabeln muss besondere Sorgfalt darauf gelegt werden, dass die Montage keine Beschädigungen hervorruft und dass die Kabelwege so gewählt sind, dass Beschädigungen der verlegten Kabel durch die normale Nutzung des Gebäudes ausgeschlossen sind. Zudem muss generell darauf geachtet werden, dass IT-Kabel getrennt von der elektrotechnischen Verkabelung geführt werden.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Elektrotechnische Verkabelung".

INF.3.M4 Anforderungsanalyse für die elektrotechnische Verkabelung

Anforderungen, die Einfluss auf eine zukunftssichere, bedarfsgerechte und wirtschaftliche Ausführung der elektrotechnischen Verkabelung haben könnten, sollte im Vorfeld größerer Verkabelungsarbeiten analysiert werden. In einer Anforderungsanalyse sollte zunächst abgeschätzt werden, welche Strommengen von welchen Verbrauchern kurzfristig durch die Anwender in der Institution genutzt werden sollen und wie darauf aufbauend die längerfristige Entwicklung der Nutzung aussehen wird.

INF.3.M5 Abnahme der elektrotechnischen Verkabelung

Die elektrotechnische Verkabelung ist entsprechend der relevanten DIN-VDE-Vorschriften nach Abschluss der Installation einem Abnahmeprozess zu unterziehen. Dabei sind grundsätzlich auch die Aspekte der Informationssicherheit (siehe auch INF.3.M11 Kontrolle elektrotechnischer Anlagen und Verbindungen) zu berücksichtigen.

Eine Abnahme sollte erst dann erfolgen, wenn alle durchzuführenden Aufgaben abgeschlossen sind, der Ausführende die Maßnahme zur Abnahme gemeldet hat und sich bei den Kontrollen durch den Auftraggeber keine inakzeptablen Mängel gezeigt haben. Der Abnahmetermin sollte zeitlich so gewählt werden, dass die Kontrollen zur Abnahme in ausreichender Zeit vorbereitet werden können. Neben der korrekten Abrechnung und dem tatsächlichen Umfang der Leistungen müssen bei der Abnahme die Einhaltung der unterschiedlichen Normen für elektrotechnische Verkabelungen kontrolliert werden. Bei der Abnahme sollte auch betrachtet werden, ob nach der Installation die Brandschottung wieder ordnungsgemäß hergestellt wurde.

Für das Abnahmeprotokoll kann eine Checkliste vorbereitet werden. Die Checkliste sollte auch Punkte zu allgemeinen Anforderungen an die Betriebsräume enthalten. Das Abnahmeprotokoll muss von den Teilnehmern und Verantwortlichen rechtsverbindlich unterzeichnet werden. Das Protokoll sollte Bestandteil der internen Dokumentation der Verkabelung sein.

INF.3.M6 Überspannungsschutz

In jedem elektrisch leitenden Netz, gleichgültig ob es der Energieversorgung oder der Datenübertragung dient, kann es zu jeder Zeit zu Überspannungen kommen. Überwiegend werden solche Überspannungen durch andere Stromverbraucher im gleichen Versorgungsnetz verursacht. Überspannungen durch Blitz sind dagegen zwar sehr viel seltener, haben aber ein ungleich höheres Schadenspotential.

Nicht nur über die im Haus verlegten Leitungen, sondern auch über alle elektrisch leitenden Außenanbindungen wie Telefon-, Wasser- oder Gasleitungen können Überspannungen in ein Gebäude und die dort betriebene IT gelangen. Darüber hinaus können Überspannungen auch auf interne Leitungen eingekoppelt werden.

Die erforderlichen Maßnahmen zum Schutz von IT-Geräten sind unabhängig von der Ursache der Überspannung im Wesentlichen die gleichen. Die seit Oktober 2006 gültige Norm DIN EN 62305 "Blitzschutz" (entspricht der Norm VDE 0185-305 und IEC 62305) ordnet den gesamten Blitz- und Überspannungsschutz neu.

Auf Basis der neuen Norm DIN EN 62305 ist ein Überspannungsschutzkonzept zu erstellen.

Die DIN EN 62305 beschreibt in ihrem Teil 2 "Risiko-Management" erstmals allgemeinverbindlich den Weg zu einem risikoorientierten Blitz- und Überspannungsschutz. Im Teil 3 wird der "Schutz von baulichen Anlagen und Personen" behandelt, in Teil 4 "Elektrische und elektronische Systeme in baulichen Anlagen".

Im Überspannungsschutzkonzept sind natürlich auch Netzersatzanlagen (NEA) und unterbrechungsfreier Stromversorgungen (USVen) zu berücksichtigen. Obwohl USVen einen gewissen Schutz der angeschlossenen Geräte bewirken, sind sie keinesfalls als Überspannungsschutzeinrichtung zu betrachten, sondern einzig und allein als zu schützendes elektronisches Gerät.

An die Stelle der früheren drei Stufen Grob-, Mittel- und Feinschutz ist das Konzept der energetischen Koordination getreten. Nach der Norm ist ein Überspannungsschutz im Gebäude und damit die Beachtung der energetischen Koordination zwar nur dann zwingend erforderlich, wenn es einen äußeren Blitzschutz gibt. Im Sinne der Informationssicherheit sollte auch in Fällen ohne äußeren Blitzschutz im Gebäude der Überspannungsschutz aufgebaut und folglich die energetische Koordination beachtet werden. Vereinfacht dargestellt bedeutet das folgendes:

- Hinter jedem Schutzelement (SPD - Surge Protecting Device) darf maximal so viel durch Überspannung verursachte Energie wirken, wie alle dahinter befindlichen elektrischen Einrichtungen (inklusive der folgenden SPDs) verkraften. Ein reines Leitungsnetz ist natürlich wesentlich robuster und verträgt deutlich mehr Energie als z. B. die Schnittstelle einer Netzwerkkarte in einem PC.
- Alle eingesetzten SPDs müssen sich miteinander vertragen. Der Ausgang eines vorgelagerten SPDs und der Eingang des folgenden müssen aufeinander angepasst sein. Der Nachweis der energetischen Koordination kann auf dreierlei Weise erbracht werden:

1 Einzelfallprüfung durch einen Fachprüfer,
2 Computersimulation mittels geeigneter Näherungsverfahren,
3 Einbau von SPDs aus einer Produktfamilie, für die der Hersteller den Nachweis erbringt.

Durch den Aufbau des Blitz- und Überspannungsschutzes werden wie Zwiebelschalen ineinander liegende Blitzschutzzonen (LPZ, Lightning Protection Zone) gebildet. Mit steigendem Schutz werden sie von außen nach innen mit LPZ 0, LPZ 1, LPZ 2 etc. bezeichnet. Dabei kann eine Zone nur dann gebildet werden, wenn es die nächst äußere gibt: So ist es nicht möglich, eine LPZ 2 zu realisieren, ohne auch die LPZ 1 zu haben.

Für einfache elektrische und elektromechanische Geräte ist die LPZ 1 meist ausreichend. Zum Schutz elektronischer Geräte (IT-Hardware, USV etc.) ist mindestens die LPZ 2 zu realisieren. Bei besonders empfindlichen Geräten, z. B. in der Medizin- oder Messtechnik kann durchaus die LPZ 3 erforderlich werden.

Hinweis:

Die LPZ (Blitzschutzzonen) sind nicht zu verwechseln mit den Schutzklassen des äußeren Blitzschutzsystems, das mit LPS (Lightning Protection System) bezeichnet wird.

Ob ein LPS erforderlich ist und mit welcher Schutzklasse, muss anhand der Risikobewertung (gemäß Teil 2 der DIN EN 62305) entscheiden werden. Der früher ausreichende Blick in eine Gebäudeliste genügt nicht mehr!

In vielen Fällen ist der gebäudeweite Aufbau einer LPZ 2 oder LPZ 3 gar nicht erforderlich. Während der Übergang von der LPZ 0 (das ist alles außerhalb eines Gebäudes, wo der Blitz also tatsächlich direkt einschlagen kann) zur LPZ 1 tatsächlich möglichst nah an der Gebäudehülle zu erfolgen hat, kann der Aufbau höherer LPZ an beliebiger Stelle und in beliebigem Umfang erfolgen. Wichtig ist dabei aber darauf zu achten, dass keine Leitung, die nur den Schutz der LPZ 1 genießt (z. B. Heizungsrohre) durch höherwertige LPZ hindurch läuft.

Die früher notwendigen Mindestleitungslängen zwischen den SPDs, also den Schutzelementen, und der unterschiedlichen LPZ sind heute nicht mehr zwingend. Es gibt SPDs, die in einem Bauteil den Übergang von der LPZ 0 direkt in die LPZ 2 realisieren.

Die Schutzwirkung eines SPDs reicht nach beiden Seiten (auf die kommende und die gehende Leitung) nur über eine bestimmte Kabelstrecke, die im Einzelnen vom Hersteller zu benennen ist. Wird die Kabellänge abgehend überschritten, sind wiederholt SPDs einzubauen, um den Schutz aufrecht zu erhalten.

Nach DIN EN 62305 müssen Blitzschutzsysteme (LPS) abhängig von der Schutzklasse in Abständen von 1 bis 4 Jahren überprüft werden. Für die Überspannungsschutzeinrichtungen sieht die Norm keine ausdrücklichen Prüfintervalle vor. Im Sinne der Informationssicherheit sollten aber alle SPDs periodisch (mindestens einmal pro Jahr) und nach bekannten Ereignissen geprüft und gegebenenfalls ersetzt werden. Um diese Prüfung überhaupt durchführen zu können, sollten, sofern verfügbar, ausschließlich solche SPDs eingebaut werden, die eine integrierte Defektanzeige oder (noch besser) eine Lebensdaueranzeige besitzen.

Neben dem Überspannungsschutz auf allen elektrisch leitenden Systemen müssen in Serverräumen und den Kerneinheiten eines Rechenzentrums Maßnahmen gegen elektrostatische Aufladung getroffen werden. Der Durchgangswiderstand der Bodenbeläge in solchen Räumen muss zwischen 10 und 100 Megaohm liegen. Die Einstufung nach DIN-Vorschrift 4102-1 "Brandverhalten von Baustoffen und Bauteilen" muss mindestens "B1 schwer entflammbar" erreichen. Dies gilt auch für einen Doppelboden oder Installationsboden.

Unabhängig von Umfang und Ausbau des Überspannungsschutzes ist zu beachten, dass ein umfassender Potentialausgleich aller in den Überspannungsschutz einbezogenen elektrischen Betriebsmittel erforderlich ist! Die Mehrzahl der Schäden an IT-Geräten durch Überspannungen ist auf nicht konsequent umgesetzten Potentialausgleich zurückzuführen.

Einige Störungen, die sich nachteilig auf die ordnungsgemäße Funktion der IT und damit negativ auf deren Verfügbarkeit und Integrität auswirken, erfolgen über elektrisch leitende Medien. Besonders relevant sind hier Einkopplungen von Störsignalen unterschiedlichster Herkunft sowie Überspannungen durch Blitz oder Schalthandlungen. Recht wirkungsvoll können diese Störungen dadurch unterbunden werden, wenn Außenleitungen galvanisch getrennt werden und somit der elektrische Ausbreitungsweg der Störung unterbrochen wird, allerdings ist dies nicht immer möglich.

In der normalen Stromversorgung wäre der Einsatz von Trenntransformatoren zwar tatsächlich eine galvanische Trennung. Störende Spannungsspitzen und andere Störsignale würden aber auch Eins-zu-Eins übertragen. Einzig die Bandpass-Wirkung eines Transformators würde die Störung ggf. etwas reduzieren.

Aufgrund der Tatsache, dass Trenntransformatoren nur begrenzt wirken und da diese in Datenleitungen in der Regel nicht einsetzbar sind, ist die oben erwähnte galvanische Trennung für die Praxis nicht relevant. Stattdessen lassen sich Risiken, die durch Spannungsspitzen und Überspannungen auf der Energieversorgung entstehen, ausreichend reduzieren, wenn die Maßnahmen des Überspannungsschutzes umgesetzt werden.

Sonstige Medienleitungen (Kühlmittel und Kondenswasser einer Kälteversorgung, normale Wasser oder Gasleitungen etc.) müssen natürlich auch betrachtet werden. Ist das geführte Medium selbst elektrisch leitend, also Wasser (auch Hauptbestandteil von Kühlflüssigkeiten), dann ist es kaum zielführend die ansonsten in Kupfer oder Stahl ausgeführte Verrohrung durch Kunststoff zu unterbrechen. Auch hierbei greifen dann nur die einschlägigen Maßnahmen des Überspannungsschutzes.

Einzig bei Gas-Leitungen kann ein nicht-leitendes Rohrstück eine echte galvanische Trennung bewirken.

INF.3.M7 Entfernen und Deaktivieren nicht mehr benötigter Leitungen

Nicht benötigte Leitungen sind solche Leitungen, die für die Funktion des Gebäudes aufgrund von Nutzungsänderungen oder Modernisierungsmaßnahmen nicht mehr erforderlich sind. Diese Leitungen sollten grundsätzlich vollständig entfernt werden, um die Brandlasten im Gebäude auf das notwendige Mindestmaß zu beschränken und um die vorhandenen Trassen nur im erforderlichen Rahmen zu befüllen. Bei der Entfernung von Leitungen ist darauf zu achten, dass die Brandschottungen nach der Entfernung der Kabel wieder fachgerecht verschlossen werden.

Welche Leitungen nicht mehr benötigt werden, darf erst nach sorgfältiger Prüfung durch die zuständige Organisationseinheit entschieden werden. Die Entscheidung ist zu dokumentieren.

Werden die Änderungen der Verkabelungsinfrastruktur parallel zum Dienstbetrieb durchgeführt, sind die Maßnahmen organisatorisch so zu unterstützen, dass die Beeinträchtigungen des Dienstbetriebes auf ein Minimum reduziert werden. Dazu müssen gegebenenfalls auch Wochenend- und Nachtarbeiten eingeplant werden. Wenn in den vorhandenen Trassen nicht genug Platz für die alten und neuen Kabel ist, so sind neue Trassen für die neuen Kabel zu installieren, um die Umschaltzeit von der noch immer betriebenen alten Infrastruktur auf die neue Infrastruktur so kurz wie möglich zu gestalten.

Trassen und Kabel, die mit der vorhandenen Technik sinnvoll als Reserve weiter genutzt werden können, sind explizit am Kabel selbst und in der Dokumentation als nicht im Betrieb befindliche Reserve zu kennzeichnen und in einem betriebsfähigen Zustand zu erhalten.

In der Betriebsdokumentation sind alle Änderungen revisionsfähig zu dokumentieren.

Es empfiehlt sich, in sinnvollen Zeitabständen und in jedem Fall nach Leitungsarbeiten die Änderungen fachkundig zu prüfen. Diese Prüfungen sind zu protokollieren.

INF.3.M8 Brandschutz in Trassen

Elektroleitungen werden typischerweise in Installationstrassen konzentriert. Es ist oft festzustellen, dass Trassen entlang von Flucht- und Rettungswegen, durch Tiefgaragen, Lager, Werkstätten oder als Transittrassen durch fremde Nutzungsbereiche führen.

Bei Gebäuden mit mehreren Brandabschnitten unterliegt die Ausführung von Elektroleitungen brandschutztechnischen Auflagen. Dies betrifft insbesondere Leitungen, die Brandabschnitte, Wände oder Decken durchqueren oder die in Verkehrswegen verlegt wurden. Speziell wenn die Trassen für Brandmelde-, Alarmierungs-, Löschtechnik oder Sicherheitsbeleuchtung genutzt werden, sind zusätzliche Forderungen nach Funktionserhalt von Elektroleitungen im Brandfall einzuhalten. Daher sollte bei der Planung der Trassen in jedem Fall der Brandschutzbeauftragte hinzugezogen werden. Trassen müssen sowohl Brandschutz als auch Schutz gegen Sabotage bieten. Beides lässt sich durch eine fachgerechte Schottung der Trassen erreichen.

Wenn Elektrokabel in erheblicher Packungsdichte im brandschutztechnisch abgetrennten Kabelkanal geführt sind, können größere Temperaturerhöhungen entstehen. Dies kann ein Ansteigen des elektrischen Leitungswiderstandes mit zusätzlicher Erwärmung nach sich ziehen. Daher sind die Vorgaben in DIN VDE 0100-520 "Errichten von Niederspannungsanlagen - Teil 5: Auswahl und Errichtung elektrischer Betriebsmittel - Kapitel 52: Kabel- und Leitungsanlagen" als deutsche Fassung der IEC 60364-5-52 in Abhängigkeit der Verlegeart zu beachten. Dies liegt im Verantwortungsbereich des Elektrofachplaners.

Durchbrüche sind nach Verlegung der Leitungen entsprechend der Feuerwiderstandsklasse der Wand oder Decke zu schotten. Um die Nachinstallation zu erleichtern, können geeignete Materialien wie Weichschotts oder Brandschutzkissen bei Maßnahmen mit temporärem Charakter verwendet werden. Entsprechende Normen und Richtlinien, wie die DIN 4102 "Brandverhalten von Baustoffen und Bauteilen", sind zu beachten. Kabeltrassen dehnen sich bei Erwärmung z. B. durch Brandeinwirkung aus und können ein Weich- oder Kissenschott zerstören, wenn sie durch Wände geführt werden.

Daher sollten Trassen nicht durch das Schott hindurch geführt werden, sondern beidseitig mindestens 10 cm vor der Wand enden. Diese Praxis erleichtert auch das Ausfächern der Kabel und Leitungen, die nicht als Bündel, sondern einzeln durch das Schott geführt werden müssen.

Häufig werden in einer Trasse unterschiedliche Kabel, z. B. für Telefon, LAN und Haustechnik, geführt. Falls Änderungen der Verkabelung anstehen, sollte bereits in der Planungsphase geklärt werden, ob in absehbarer Zeit auch andere Kabelsysteme ausgewechselt werden sollen. Eine entsprechende Zusammenlegung von Projekten minimiert Ausfallzeiten und erspart zusätzliche Kosten für eine mehrmalige Brandschottung.

Ist die geplante Trassenführung gemäß den brandschutztechnischen Auflagen nicht möglich, so ist eine alternative Trassenführung zu prüfen. Darüber hinaus sollten nach Abschluss der Installationsarbeiten die Brandabschottung in regelmäßigen Abständen, beispielsweise jährlich, kontrolliert werden.

INF.3.M9 Dokumentation und Kennzeichnung der elektrotechnischen Verkabelung

Für die Wartung, Fehlersuche, Instandsetzung und für eine erfolgreiche Überprüfung der Verkabelung sind eine gute Dokumentation und eine eindeutige Kennzeichnung aller zugehörigen Komponenten erforderlich. Die Güte dieser Revisionsdokumentation ist abhängig von der Vollständigkeit, der Aktualität und der Lesbarkeit der Unterlagen. In jedem Fall ist ein Verantwortlicher für die Dokumentation der Verkabelung zu benennen.

Da es mit zunehmender Größe eines Netzes nicht möglich ist, alle Informationen in einem Plan unterzubringen, ist eine Aufteilung der Informationen sinnvoll. Tatsächliche Lageinformationen sind immer in maßstäbliche Pläne einzuzeichnen. Andere Informationen können in Tabellenform oder Schemaplänen geführt werden. Wichtig dabei ist eine eindeutige Zuordnung aller Angaben untereinander. Die Dokumentation sollte somit aus beschreibenden Unterlagen, Listen und Plänen bestehen.

Die beschreibenden Unterlagen, wie z. B. eine Dokumentationsrichtlinie, enthalten die Informationen über die Abläufe zur Dokumentation, Bezeichnungs- und Kennzeichnungsregelungen. In dieser sollte beispielsweise in allgemeiner Form beschrieben werden, welche Listen und Pläne zu erstellen sind und wie diese auch revisionssicher zu führen sind.

Die Bestandspläne bestehen typischerweise aus:

- Standortübersichten und bemaßten Lageplänen mit der genauen Führung der Trassen und der Primärverkabelung,
- Gebäudeschnitten als Schemapläne und bemaßten Etagengrundrissplänen mit der genauen Lage und Führung der Verteilerräume, Trassen und Kabel sowie den Steckdosen pro Raum in z. B. Brüstungskanälen und/oder Bodenauslässen,
- Technikraumplänen mit Raumlayout, Doppelbodenraster und Schrankpositionierung, Stromverteilung und Potenzialausgleichsschiene sowie einer vorhandenen Klimatisierung sowie
- Schrankansichtsplänen zur lagerichtigen Beschreibung der eingebauten passiven und aktiven Komponenten inklusive der Steckdosenleisten.

Es muss möglich sein, sich anhand dieser Dokumentation einfach und schnell ein genaues Bild über die Verkabelung zu machen.

Die Art der Dokumentation ist ähnlich der bei der IT-Verkabelung. Es ist daher sinnvoll, beide zusamen zu führen.

Um die Aktualität der Dokumentation zu gewährleisten, ist sicherzustellen, dass alle Arbeiten an der Verkabelung rechtzeitig und vollständig demjenigen bekannt werden, der die Dokumentation führt. Es ist z. B. denkbar, die Ausgabe von Material, die Vergabe von Fremdaufträgen oder die Freigabe gesicherter Bereiche von der Mitzeichnung dieser Funktion abhängig zu machen.

Da diese Dokumentation schutzwürdige Informationen beinhaltet, ist sie sicher aufzubewahren und der Zugriff zu regeln.

Sinnvollerweise wird bereits bei der Planung von Verkabelungsmaßnahmen in einem Tool mit der Dokumentation begonnen und diese nach der Realisierung vom Planungsstatus in den Produktivstatus übernommen. Auf diesem Wege ist es leichter, die Nutzer der Dokumentation über bevorstehende Änderungen zu informieren und die Dokumentation aktuell zu halten.

INF.3.M10 Neutrale Dokumentation in den Verteilern

In jedem Verteiler sollte sich eine Dokumentation befinden, die den derzeitigen Stand von Rangierungen und Leitungsbelegungen wiedergibt. Diese Dokumentation ist möglichst neutral zu halten, sie muss aber zugleich sicheres Schalten in der Verteilung ermöglichen. Neben bestehenden und genutzten Verbindungen sind darin ggf. auch existierende Reserveleitungen aufzuführen. Es sollten, soweit nicht ausdrücklich vorgeschrieben (z. B. für Leitungen der Sicherheitsstromversorgung), keine Hinweise auf die Nutzungsart der Leitungen gegeben werden. Leitungs-, Verteiler-, und Raumnummern reichen in vielen Fällen aus. Alle weitergehenden Informationen sind in einer Revisionsdokumentation aufzuführen.

INF.3.M11 Kontrolle elektrotechnischer Anlagen und Verbindungen

Nach der Errichtung und anschließend in regelmäßigen Abständen müssen elektrotechnische Installationen überprüft werden.

Die Erstprüfung ist in der Norm DIN-VDE 0100-610 "Errichten von Niederspannungsanlagen - Teil 6-61: Prüfungen - Erstprüfungen" (Deutsche Fassung der IEC 60364-6-61) beschrieben. Die Prüfung muss durch einen staatlich anerkannten Sachverständigen erfolgen. Der Prüfer besichtigt die Installationen und ihre Ausführung vor Ort und führt Prüfmessungen durch. Hierbei wird geprüft, ob

- alle elektrischen Anlagen nach Herstellervorgaben errichtet worden sind,
- Brandschotts korrekt eingebaut wurden,
- eine richtige Auswahl der Leiter in Bezug auf Strombelastbarkeit, Auswahl und Einstellung der Schutzeinrichtungen und Übereinstimmung mit der Planung getroffen wurde,
- Schaltpläne vollständig und korrekt sind,
- Warnhinweise angebracht wurden,
- alle Leiter ordnungsgemäß verbunden sind,
- die Durchgängigkeit der Schutzleiter gegeben ist.

Zudem umfasst die Erstprüfung die Messung des Isolationswiderstands der gesamten Anlage und die Prüfung und den Nachweis des Schutzes durch automatische Abschaltung.

Ergebnis der Erstprüfung ist die Feststellung der Betriebssicherheit und Wirksamkeit der elektrotechnischen Anlagen.

Elektrische Anlagen müssen auch danach regelmäßig durch einen Sachkundigen auf Betriebssicherheit überprüft werden. Dabei muss neben dem vorrangigen Schutzziel der Unfallverhütung vor allem die Auswirkung von Änderungen der Nutzung (z. B. durch eine stark angestiegene Anzahl von Verbrauchern) überprüft und dokumentiert werden. Die Prüfprotokolle mit den Ergebnissen der Prüfungen und Messungen sollten archiviert werden.

Elektroverteilung

Die gesamte Elektroverteilung, hauptsächlich Schutzschalter sowie Verschraubungen und Klemmstellen, unterliegt wie alle technischen Geräte einer Alterung. Sie ist daher in regelmäßigen Abständen gemäß DIN VDE 0105-100:2005-06 "Betrieb von elektrischen Anlagen" zu überprüfen.

Im Schadensfall muss ein Gewerbetreibender den Nachweis über den einwandfreien Zustand der Elektroanlage gegenüber den Gewerbeaufsichtsämtern, den Berufsgenossenschaften und den Versicherungen führen.

In Deutschland schreibt die Berufsgenossenschaftliche Vorschrift für Sicherheit und Gesundheit bei der Arbeit (BGV, A3 - Elektrische Anlagen und Betriebsmittel) folgende regelmäßige Prüfungen vor:

- elektrische Anlagen und ortsfeste Geräte: mindestens alle 4 Jahre,
- ortsveränderliche Geräte: je nach Gerätetyp mindestens alle 6 Monate bis zu mindestens alle 2 Jahre.

Zu den ortsveränderlichen Geräten gehören unter anderem Steckdosenleisten, aber auch viele IT-Geräte wie beispielsweise Arbeitsplatzrechner.

Obschon es sich bei der DGUV-V3 um eine reine Unfallverhütungsvorschrift handelt, können und sollten die bei der darauf beruhenden Prüfung gewonnenen Erkenntnisse bei den VDE-basierten Prüfungen berücksichtigt werden.

Protokollierung

Alle Prüfungen und deren Ergebnisse sind in geeigneter Form zu dokumentieren.

INF.3.M12 Vermeidung elektrischer Zündquellen

Der überwiegende Teil baulicher Brandschutzmaßnahmen zielt darauf ab, sich entwickelnde Brände einzugrenzen, sowie die Flucht von Personen und den Einsatz von Rettungskräften zu ermöglichen. Auf die Entstehung von Bränden haben diese Maßnahmen meist nur geringen Einfluss.

Hier muss der Mensch in seinem täglichen Arbeitsumfeld besondere Aufmerksamkeit und Vorsorge walten lassen. Neben den allseits bekannten und offensichtlichen Brandquellen wie Aschenbechern, der "Kippe im Papierkorb" oder weihnachtlichem Kerzenschmuck muss auch den weniger offensichtlichen elektrischen Zündquellen Beachtung geschenkt werden.

Elektrogeräte

Beim Kauf neuer privater Haushaltsgeräte werden die noch funktionierenden Altgeräte als "Spende" im Betrieb weiter genutzt. Dabei wird übersehen, dass gerade alte Elektrogeräte mit ihren altersbedingt viel wahrscheinlicheren Defekten eine besonders hohe Brandgefährdung darstellen.

Die Nutzung privater Elektrogeräte innerhalb eines Unternehmens oder einer Behörde ist daher klar zu regeln. Sie sollte nur als Ausnahme gestattet sein, wenn derartige Geräte vorher durch eine Elektrofachkraft geprüft und für sicher befunden wurden. Diese Prüfpflicht gilt selbstverständlich für alle von der Institution bereitgestellten Elektrogeräte. Genehmigte Geräte sollten speziell gekennzeichnet werden, so dass ungenehmigte Geräte einfach erkannt und aus dem Verkehr gezogen werden können.

Besonders Kühlschränke, die im Dauerbetrieb laufen, und Kaffeemaschinen, die oft stundenlang eingeschaltet bleiben, sollten nur in Räumen betrieben werden, die ausdrücklich und baulich dafür vorgesehen sind (Teeküchen etc.).

Steckdosenleisten

Egal wie viele Steckdosen vom Architekten vorgesehen wurden, es sind immer zu wenig oder sie sind am falschen Platz. Um dann fehlende Steckdosen bereitzustellen, werden oft Steckdosenleisten verwendet. Sind diese von unzureichender Qualität oder werden sie unsachgemäß eingesetzt, stellen solche Steckdosenleisten eine gefährliche Zündquelle dar.

Die Verwendung von Steckdosenleisten sollte so weit wie möglich vermieden werden. Fehlende Steckdosen sollten durch eine Elektrofachkraft in vorhandenen Kanalsystemen nachgerüstet oder fachgerecht auf Putz montiert werden.

Ist dies nicht möglich und somit die Verwendung von Steckdosenleisten unvermeidbar, ist zu beachten:

- Es dürfen ausschließlich hochwertige Steckdosenleiste verwendet werden, die von einer Elektrofachkraft geprüft und für sicher befunden wurden.
- Es sollten einzelne ausreichend große Steckdosenleiste benutzt werden statt mehrerer kleiner.
- Steckdosenleisten dürfen keinesfalls hintereinander gesteckt werden.
- Steckdosenleisten dürfen auf keinen Fall überlastet werden. In der Regel liegt die Grenze bei 3500 Watt. Hier ist unbedingt das Typenschild zu beachten.
- Steckdosenleisten dürfen sich weder im Fußbereich am Arbeitsplatz noch in Verkehrsflächen befinden.

Lüfter

Durch Staub blockierte Lüfter können zur Überhitzung der zu kühlenden IT-Geräte führen, aber auch selbst zu einem Brandherd werden.

Lüfter sind folglich in regelmäßigen Abständen auf freien Rundlauf und auf Staubablagerung hin zu untersuchen und zu reinigen. Dies sollte mindestens einmal im Jahr und bei erkennbarem Bedarf auch öfter erfolgen.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

INF.3.M13 Sekundär-Energieversorgung (A)

Die primäre Energieversorgung aus dem Netz eines Energieversorgungs-Unternehmens (EVU) sollte bei erhöhten Anforderungen an die Verfügbarkeit um Maßnahmen zur Notfall-Versorgung ergänzt werden, beispielsweise für Serverräume.

Die sekundäre Energieversorgung besteht üblicherweise aus einer zentralen USV für die abzusichernden Bereiche und einer Netzersatzanlage (NEA). Falls die örtlichen Gegebenheiten und das Anforderungsprofil an die Verfügbarkeit es zulassen, kann statt einer NEA auch eine zweite Einspeisung aus dem Netz eines zweiten Energieversorgungs-Unternehmens diese Auffang-Funktion erfüllen.

Während eine USV Schwankungen oder kurzfristige Unterbrechungen der Stromversorgung überbrückt, fängt eine Netzersatzanlage längerfristige Stromausfälle auf.

Weitere Ausführungen zum Thema Redundanz und den damit eng verbundenen Aspekten Modularität und Skalierbarkeit sind in INF.2 Rechenzentrum zu finden.

Bei einem länger andauernden Ausfall der primären Energieversorgung ist eine NEA für die Aufrechterhaltung des IT-Betriebs unverzichtbar. Ihr Schutzbedarf entspricht also dem der IT, die sie versorgt. Dabei ist besonders auf den Schutz vor Brand und Wasser sowie Zugriff Unbefugter zu achten.

Um die Schutzwirkung einer NEA und einer USV aufrechtzuerhalten, müssen sie regelmäßig gewartet werden. Dafür sind die vom Hersteller vorgesehenen Wartungsintervalle einzuhalten. Bei diesen Wartungen sollten auch Belastungs- und Funktionstests durchgeführt werden. Außerdem muss mindestens einmal in 2 Jahren ein Testlauf von USV und NEA unter Echtbedingungen (als "Black-Building-Test") durchgeführt werden.

INF.3.M14 A-B-Versorgung (A)

Bei einer redundanten Stromversorgung mittels einer sogenannten A-B-Versorgung wird deren Funktionsfähigkeit meist dadurch ohnehin permanent überwacht, dass Geräte mit zwei Netzteilen, die A-B-versorgt sind, den Ausfall einer der beiden Speisungen über Netzwerkprotokolle melden können. Sollte diese Möglichkeit nicht bestehen oder aus bestimmten Gründen nicht genutzt werden können, kann die Verfügbarkeit der A-B-Versorgung auch z. B. mittels Einrichtungen der Gebäudeleittechnik (GLT) überwacht werden.

Im Bereich der vorgelagerten Verteilung (von der Hauptverteilung bis einschließlich der letzten Verteilung vor den Verbrauchern) sollten die Leitungen räumlich und brandschutztechnisch getrennt voneinander geführt werden. Nur so wird sichergestellt, dass die durch die A-B-Versorgung herbeigeführte Redundanz optimal wirken kann.

Die letzten Verteilungen (A und B) vor den Verbrauchern sind bei Unmöglichkeit einer räumlich getrennten Anordnung mindestens so weit auseinander anzuordnen, dass es nicht möglich ist, dass eine Person gleichzeitig in beiden Verteilungen aktiv werden kann.

Im Endbereich der Verteilung (also zwischen der letzten Verteilung und den Verbrauchern) ist eine brandschutztechnisch getrennte Verlegung kaum realisierbar und kann folglich entfallen. Eine räumlich getrennte Verlegung sollte aber, soweit platzmäßig möglich, sehr wohl realisiert werden. Dadurch wird das Risiko, dass eine versehentlich Beschädigung der Versorgungsleitungen beide Wege, also den A- und den B-Weg, trifft, deutlich minimiert.

INF.3.M15 Materielle Sicherung der elektrotechnischen Verkabelung (A)

In Räumen mit Publikumsverkehr oder in unübersichtlichen Bereichen eines Gebäudes kann es sinnvoll sein, Leitungen und Verteiler gegen unbefugte Zugriffe zu sichern. Dies kann auf verschiedene Weise erreicht werden:

- Verlegung der Leitungen oder Kabelkanäle unter Putz,
- Verlegung der Leitungen in Stahlpanzerrohr,
- Verlegung der Leitungen in mechanisch festen und abschließbaren Kanälen,
- Verschluss von Verteilern und
- elektrische Überwachung von Verteilern und Kanälen.

In jedem Fall ist die Zahl der Stellen, an denen das verlegte Kabel zugänglich ist, auf ein Mindestmaß zu reduzieren und die Länge der vor unberechtigten Zugriff zu schützenden Verbindungen möglichst klein zu halten.

Besonders die Absicherung zentraler Trassen und Kabel der elektrischen Versorgung muss im gesamten Kabelweg an die Gefährdungslage angepasst werden. In Bereichen wie Tiefgaragen und auch in Fluren, die als Transportwege genutzt werden, muss ein angemessener Schutz gegen zufällige mechanische Beschädigung und gegebenenfalls auch gegen Sabotagehandlungen durch eine stabile Ummantelung der Trasse oder des Kabels getroffen werden.

Wenn Verteiler verschlossen werden, sind Regelungen nötig, die Zutrittsrechte zum Verteiler, Verteilung der Schlüssel und Zugriffsmodalitäten festlegen. Darin ist unter anderem vorzugeben, was vor Änderungen an Kabeln oder Verteilern und nach der Ausführung solcher Arbeiten zu tun ist. Es muss sichergestellt sein, dass Änderungen abgestimmt und genehmigt werden und dass die Dokumentation nachgeführt wird.

INF.3.M16 Nutzung von Schranksystemen (A)

Zur Verbesserung der Betriebssicherheit elektrotechnischen Anschlüssen und -verteilern sollten diese Geräte in Schranksystemen eingebaut oder aufgestellt werden (siehe auch INF.6 Schutzschrank).

INF.3.M17 Brandschott-Kataster (A)

Es sollte ein Brandschott-Kataster geführt werden, das mindestens folgende Anforderungen erfüllt:

- Im Kataster sind alle Schotts aufzunehmen, also reine Kabelschotts, Rohrleitungsschotts, Kombischotts etc.
- Jedes Brandschott im Gebäude bzw. in der Liegenschaft ist im Kataster individuell zu führen. (Die Aufnahme von Schotts in das Kataster kann für solche Schotts entfallen, deren Versagen nachweislich keinerlei nachteiligen Einfluss auf den IT-Betrieb des Gebäudes bzw. der Liegenschaft hat.)
- Jedes Brandschott wird im Kataster unter einer individuellen eindeutigen Kennzeichnung geführt. Diese Kennung ist im unmittelbaren Umfeld des betreffenden Schotts (soweit irgend möglich auf beiden Seiten) gut lesbar anzubringen.
- Im Kataster ist für jedes Schott individuell der Nachweis einer mindestens jährlichen Sichtkontrolle mit den sich dabei ergebenden Feststellungen zu führen.
- In das Kataster sind für Schotts, die zum Zeitpunkt der Erstellung des Katasters schon eingebaut sind, alle verfügbaren Informationen strukturiert aufzunehmen, also mindestens:
  - Einbauort
  - Hersteller des Schotts
  - Produktbezeichnung
- Die zum Zeitpunkt der Errichtung gültigen Allgemeinen bauaufsichtlichen Zulassungen (AbZ) oder die allgemeinen bauaufsichtlichen Prüfzeugnisse (AbP). Diese AbZ bzw. AbP sind in der Regel nur 5 Jahre gültig und werden danach entweder verlängert oder aufgehoben. Oft ist es sehr schwer, Hinweise auf abgelaufene AbZ oder AbP im Internet zu finden.
- Einbaudatum
- Einbaufirma und ein aktuelles Foto beider Seiten des eingebauten Schotts.

Bei Bestands-Schotts kann es in Einzelfällen bei unklarer Sachlage zwingend erforderlich sein, es durch ein neues zu ersetzen. Für ein solches Schott gelten dann auch die folgenden Vorgaben:

- Für alle nach der erstmaligen Erstellung des Katasters neu eingebauten oder veränderten Schotts sind über die oben genannten Informationen hinaus mindestens folgende weitere im Kataster aufzunehmen:
  - Lückenlose Fotodokumentation aller wesentlichen Einzelschritte des Ein- oder Umbaus,
  - Grund des Umbaus,
  - Nachweis, dass die beim Umbau verwendeten Materialien vom Hersteller des Schotts für den Umbau zugelassen sind.
  - Alle Eintragungen im Kataster sind unverzüglich vorzunehmen, spätestens 4 Wochen nach Beendigung der Arbeiten.

Nach einem Umbau ist das alte Zertifikat am Einbauort deutlich als ungültig zu kennzeichnen aber so, dass man noch alle relevanten technischen Informationen lesen kann, und durch ein neues, den Umbau berücksichtigende Zertifikat zu ergänzen.

3 Weiterführende Informationen

3.1 Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Elektrotechnische Verkabelung" finden sich unter anderem in folgenden Veröffentlichungen:

[BGVA3] DGUV Vorschrift 3

Elektrische Anlagen und Betriebsmittel, Unfallverhütungsvorschrift, Berufsgenossenschaft für Gesundheitsdienst und Wohlfahrtspflege (BGW), Mai 2014, https://www.bgw-online.de/SharedDocs/Downloads/DE/Medientypen/DGUV_vorschrift-regel/DGUV-Vorschrift3_Unfallverhuetungsvorschrift-elektr-Anlagen-Betriebsmittel_Download.pdf?__blob=publicationFile, zuletzt abgerufen am 05.10.2018

[DIN4102] DIN 4102 Brandverhalten von Baustoffen und Bauteilen

[IEC60364] DIN IEC60364- Einrichten von Niederspannungsanlagen

[IEC62305] IEC 62305 Merkblatt

Die Blitzschutz-Normen DIN EN 62305 / VE 01805-305:2006, VDE (ABB), Oktober 2006, https://www.vde.com/resource/blob/936756/5b65d838e75e83f750bd8fa23bb620b1/merkblatt-blitzschutznormen-13-download-data.pdf , zuletzt abgerufen am 05.09.2018

[VDE100] DIN VDE 0100: Errichten von Niederspannungsanlagen

[VDE105] DIN VDE 0105-100: Betrieb von elektrischen Anlagen

INF: Infrastruktur

Umsetzungshinweise zum Baustein INF.4 IT-Verkabelung

1 Beschreibung

1.1 Einleitung

Die IT-Verkabelung umfasst alle Kommunikationskabel und passiven Komponenten (Rangier- bzw. Spleißverteiler, Patchfelder), die in eigener Hoheit der Institution betrieben werden. Sie ist also die physikalische Grundlage der internen Kommunikationsnetze einer Institution. Die IT-Verkabelung reicht von Übergabepunkten aus einem Fremdnetz (z. B. ISDN-Anschluss eines TK-Anbieters, DSL-Anbindung eines Internet-Providers) bis zu den Anschlusspunkten der Netzteilnehmer.

Die IT-Verkabelung als Teil der technischen Infrastruktur von Gebäuden und Liegenschaften wird nach der etablierten Betrachtungs- und Vorgehensweise der strukturierten Verkabelung in Primär-, Sekundär- und Tertiärbereich aufgeteilt.

Mit Primärbereich wird der Bereich der Kabelführung, der Gebäude miteinander verbindet, bezeichnet. Der Primärbereich überbrückt große Entfernungen mit hohen Übertragungsraten zwischen wenigen Anschlusspunkten. Eine Primärverkabelung in eigener Hoheit haben also nur Instanzen, die größere Liegenschaften mit mehreren Gebäuden betreiben. Wenn nur ein Gebäude zu betrachten ist, stellt der Hauptverteiler im Gebäude logisch den Primärbereich dar.

Mit Sekundärbereich wird die Verkabelung zwischen dem Gebäudeverteiler und Verteilern der Etagen oder Gebäudebereichen bezeichnet. Diese Verkabelung ist in vielen größeren Gebäuden anzutreffen.

Die Tertiärverkabelung ist die Anbindung der Endgeräte an einen zentralen Verteilpunkt (z. B. in der Etage). Sie ist immer vorhanden.

Eine oft betriebene Mischform der strukturierten Verkabelung liegt dann vor, wenn die Anbindung der Endgeräte direkt von einem zentralen Punkt im Serverraum oder einem Raum für technische Infrastruktur (häufig als "Netzwerkraum" oder "TK-Raum" bezeichnet) ausgeführt wird. In diesem Fall besteht die Sekundärverkabelung gegebenenfalls nur aus den Verbindungskabeln zwischen den Switches. Die Tertiärverkabelung reicht vom zentralen Verteilpunkt im Gebäude zu den Anschlussdosen in den Räumen.

1.2 Lebenszyklus

Für eine sichere IT-Verkabelung sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung über die Umsetzung bis zum Betrieb und zur Notfallvorsorge. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt. Dabei ist zu berücksichtigen, dass die Einflussmöglichkeiten in Bezug auf die Absicherung der IT-Verkabelung beim Einzug in ein schon bestehendes Gebäude wesentlich geringer sind als bei der Errichtung eines Neubaus.

Planung und Konzeption

In der Planungsphase werden die Grundlagen für eine leistungsfähige, gut abgesicherte IT-Verkabelung gelegt. Ausgangspunkt ist eine Anforderungsanalyse, mit der der aktuelle Bedarf eingeschätzt wird und ein Ausblick auf kommende Entwicklungen samt Folgenabschätzung für die IT-Verkabelung in der Institution vorgenommen wird (siehe INF.4.M2 Planung der Kabelführung und INF.4.M4 Anforderungsanalyse für die IT-Verkabelung).

Auf Grundlage dieser Anforderungsplanung wird die Netzstruktur festgelegt und in das Gebäude eingepasst. Die mechanischen und elektrischen Eigenschaften der Verkabelung werden weitgehend durch die Auswahl der einzusetzenden Kabeltypen festgelegt (siehe INF.4.M1 Auswahl geeigneter Kabeltypen). Bei der Planung sollte nach Möglichkeit auch darauf geachtet werden, dass Leitungen und über das Gebäude verteilte Schaltschränke gegen Missbrauch in geeigneter Weise physisch gesichert werden (siehe INF.4.M13 Materielle Sicherung der IT-Verkabelung und INF.4.M15 Nutzung von Schranksystemen).

Umsetzung

Ein wesentliches Element des Brandschutzes ist die richtige Installation von Kabelkanälen (siehe INF.4.M3 Fachgerechte Installation), die durch eine fehlende Brandabschottung erhebliche Risiken verursachen können (siehe INF.4.M8 Brandabschottung von Trassen). Beim Einbau der Verkabelung ist auch auf eine ausführliche und korrekte Dokumentation zu achten, da es im Nachhinein ohne eine solche meist sehr schwierig oder sogar unmöglich ist, festzustellen, wo Kabel verlaufen und was sie verbinden (siehe INF.4.M9 Dokumentation und Kennzeichnung der Verkabelung und INF.4.M10 Neutrale Dokumentation in den Verteilern). Für einen störungsfreien Betrieb muss die IT-Verkabelung sachgerecht installiert werden (siehe INF.4.M3Fachgerechte Installation).

Vor Inbetriebnahme ist die Installation der IT-Verkabelung abzunehmen und die Qualität der zugehörigen Dokumentation zu prüfen (siehe INF.4.M5 Abnahme der IT-Verkabelung).

Betrieb

Um das Aufschalten ungenehmigter IT-Geräte zu verhindern, sollten jeweils nur die Verbindungen und Anschlussdosen aktiviert sein, die tatsächlich benötigt werden (siehe INF.4.M13 Materielle Sicherung der IT-Verkabelung). Zusätzlich sollte durch regelmäßige Kontrollen sichergestellt werden, dass diese Aktivierung auch den tatsächlichen Erfordernissen entspricht (siehe INF.4.M11 Kontrolle bestehender Verbindungen). Zudem ist sicherzustellen, dass die Dokumentation aktuell gehalten wird (siehe INF.4.M6 Laufende Fortschreibung und Revision der Netzdokumentation).

Aussonderung

Wenn Komponenten der IT-Verkabelung nicht mehr benötigt werden, müssen sie entfernt werden (siehe INF.4.M7 Entfernen und Deaktivieren nicht mehr benötigter Leitungen).

Notfallvorsorge

Sofern erhöhte Anforderungen an die Verfügbarkeit gestellt werden, sollte die Verkabelung, gegebenenfalls einschließlich der externen Anschlüsse, so redundant ausgelegt werden, dass ein Schaden an einer einzigen Stelle nicht zu einem Totalausfall aller Teilnehmeranschlüsse führen kann. Dazu sind gegebenenfalls Redundanzen der Verbindung zwischen Gebäuden und innerhalb eines Gebäudes zu schaffen (siehe INF.4.M12 Redundanzen für die Verkabelung).

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "IT-Verkabelung" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

INF.4.M1 Auswahl geeigneter Kabeltypen [Leiter Haustechnik]

Bei der Auswahl von Kabeln sind neben den übertragungstechnischen Notwendigkeiten auch die Umgebungsbedingungen bei der Verlegung sowie im Betrieb zu berücksichtigen. Um diesen unterschiedlichen Anforderungen gerecht zu werden, bieten die Kabelhersteller unterschiedliche Arten von Kabeln am Markt an oder entwickeln entsprechende Lösungen.

In Bezug auf den Kabelmantel für Verlegung im Innen- oder Außenbereich müssen folgende Kriterien berücksichtigt werden:

- Temperatur,
- Umgebendes Medium (Wasser, Abwasser, Säure, Gas, Licht),
- Nagetierschutz, Hieb- und Spatenstichfestigkeit, Steinschlagfestigkeit, Wasserdruckfestigkeit,
- Funktionserhalt in feuergefährdeten Bereichen,
- Spezielle Zugkräfte durch z. B. Freileitungsverwendung.

Außerdem sind die vorgesehenen Trassensysteme zu beachten, wie Kabelpritschen, Kabelleiter, Kabelkanäle, Kabelzugrohre, Kabelformsteine, Steigebereiche und Freileitungsbau.

Der weitere Kabelaufbau muss folgende Faktoren berücksichtigen:

- Zugkräfte durch maschinelle Verlegung, z. B. Kabelzugwinde, Einblassystem oder Handverlegung,
- Biegeradius und Querdruckstabilität, entsprechend Verlegeart und Ruhezustand im Betrieb,
- Feucht- oder Nassbereiche durch Längswasserschutz,
- spezielle Zugkräfte im verlegten Zustand, die durch große Spann- oder Abfangweiten bei Freileitungen oder extremen Steigungen entstehen,
- starke elektrische und induktive Störfelder durch Kabelschirmung.

Die richtige und den Vorschriften gemäße Auswahl von Elektrokabeln und die Beachtung der einschlägigen Normen (DIN VDE 0100 "Bestimmungen für das Errichten von Starkstromanlagen mit Nennspannungen bis 1000 V", DIN 4102 "Brandverhalten von Baustoffen und Bauteilen") und Vorschriften sowie der anerkannten Regeln der Technik stellt die grundlegende Notfallvorsorge der elektrotechnischen Installation dar.

Individuelle Anforderungen für die Auswahl von Kabeln dürfen gerade bei Betriebsumgebungen, in denen Umwelteinflüsse oder besondere bauliche Gegebenheiten zu beachten sind, nicht ausschließlich durch die IT selbst definiert werden. Insbesondere Mitarbeiter der Haustechnik, die mit Betriebsabläufen und sonstigen besonderen Bedingungen vertraut sind, müssen zur geplanten Kabelführung, bei der Feststellung der relevanten Einflüsse und damit der besonderen Anforderung an die Ausführung von Kabeln beteiligt werden.

Die Auswahl des Kabels aus kommunikationstechnischer Sicht wird bestimmt durch die erforderliche Übertragungsrate (Diese wird auch häufig Bandbreite genannt, was allerdings nicht ganz korrekt ist.) und die Entfernung zwischen den Übertragungseinrichtungen. Zusätzlich zu beachten sind die baulichen Gegebenheiten, d. h. die Trassen und die Umgebungsbedingungen, unter welchen die Kabel verlegt und betrieben werden. Da sich auch diese auf den Kabelaufbau auswirken, sind sie bei der Auswahl ebenso zu berücksichtigen. Vor- und Nachteile werden nachfolgend unter Sicherheitsgesichtspunkten beschrieben.

Die heute eingesetzten Übertragungssysteme verwenden für die kabelgebundene Kommunikation elektrische oder optische Schnittstellen. Entsprechend müssen die Kabel als Übertragungsmedium metallene Leiter für die elektrische Übertragung bzw. Kunststoff oder Glas (Lichtwellenleiter, LWL) für die optische Übertragung zur Verfügung stellen.

Im Folgenden werden Kupfer- und Lichtwellenleiterkabel näher betrachtet:

Zum Beispiel:

- das ungeschirmte U/UTP,
- das ungeschirmte mit einem Gesamtschirm für alle Aderpaare (F/UTP oder SF/UTP),
- das geschirmte, bei dem lediglich die einzelnen Aderpaare abgeschirmt sind (U/FTP) - früher auch als Paare in Metallfolie (PiMf) bezeichnet - und
- vorgenannter Aufbau mit einer zusätzlichen Gesamtabschirmung (F/FTP, S/FTP und SF/FTP).

Die Normen ordnen Grenzwerte für die Übertragungseigenschaften von Kabeln und Anschlusskomponenten Kategorien und Klassen zu. Die Kategorien beschreiben die Anforderungen und Grenzwerte an die einzelnen Elemente der Verkabelungsinfrastruktur, die Klassen regeln diese für das installierte Gesamtsystem.

Die Übertragungseigenschaften für die einzelnen Komponenten sind derzeit in die Kategorien 1 bis 7 eingeteilt. Hierbei gilt, je höher die Kategorie, desto höher ist auch die mögliche Übertragungsbandbreite.

Hohe Übertragungsqualitäten lassen sich zuverlässig nur erzielen, wenn eine in sich harmonische Kombination aus Kabel und Anschlusskomponenten (Buchsen und Stecker) gewählt und fachmännisch installiert wurde. Die Geräte "erkennen" keine verlegte Länge, sondern reagieren auf elektrische Signale. Daher sind die elektrischen Grenzwertvorgaben für die Strecken die führende Größe. Gemäß ISO/IEC 11801 beträgt die Maximallänge bei Kupferkabeln 90 m (inklusive Patch- und Anschlusskabel 100 m). Diese Maximallänge kann jedoch überschritten werden, wenn die geforderten elektrischen Übertragungsparameter eingehalten werden.

Das TP-Kabel ist durch die Verkabelungsnormen Standard bei der Verkabelung im sogenannten Access-Bereich auf der Etage. Dieser Kabeltyp hat folgende Vorteile:

- TP-Kabel, insbesondere deren Konfektion, sind bei geringerem Bandbreitenbedarf im Vergleich zu LWL relativ billig.
- TP-Kabel lassen sich relativ einfach verlegen und konfektionieren.
- TP-Kabel können als Universalverkabelung angesehen werden, da andere Dienste ohne größeren technischen Aufwand hierüber genutzt werden können (z. B. Telefonie).
- Die Installationen können messtechnisch leicht überprüft werden.
- TP-Kabel ermöglichen die Stromversorgung von Geräten, die nach den Vorgaben der Spezifikation "Power over Ethernet" (PoE) versorgt werden.

Dem stehen folgende Nachteile gegenüber:

- Durch die bei der Datenübertragung in den Kabeln fließenden Wechselströme und die im Kabel immer vorhandenen geringen Unsymmetrien in der Verseilung der Adern werden elektromagnetische Felder erzeugt, welche in der Umgebung wahrgenommen werden (Abhörgefahr) und Systeme stören können. Aber auch elektromagnetische Felder der Umgebung können wiederum die Übertragung im Kabel stören.Durch die Verwendung von Schirmen im Kabelaufbau werden diese Effekte minimiert (vergleiche U/UTP bis SF/FTP). Die Angaben zum Mindestabstand zwischen unterschiedlichen Kabeln, Leitungen und Systemen sowie zur Erdung von Schirmen sind zu beachten.
- Die vorgenannten Effekte wirken auch innerhalb des Kabels. Ungeschirmte Installationskabel (U/UTP) bieten vor dem sogenannten Übersprechen zwischen einzelnen Paaren den geringsten Schutz. Hier wirkt lediglich die Verseilung der einzelnen Adern.

Lichtwellenleiter (LWL)

Bei der Übertragung von Signalen in Lichtwellenleitern wird Licht vom sichtbaren bis stark infraroten Bereich verwendet. Zur Erzeugung dieses Lichts werden Dioden oder Laser eingesetzt. Diese wandeln das elektrische Signal in Lichtmoden unterschiedlicher Richtungen bzw. unterschiedlich starker Bündelung.

Der Lichtwellenleiter, auch Faser genannt, besteht aus dem zur Übertragung verwendeten Kern- und einem umgebenden Mantelmaterial. Die Materialien unterscheiden sich in der sogenannten Brechzahl.

Die Verkabelungsstandards der IEEE 802.3 Reihe definieren für Multimode-LWL die Kategorien OM-1, OM-2, OM-3 und OM-4. Gegenstand dieser Spezifikationen sind Lichtwellenleiter mit Gradientenprofil der Brechzahl und einem Kern/Mantel-Nenndurchmesser von 50/125 oder 62,5/125 Mikrometern. Der Kern/Mantel-Nenndurchmesser von Singlemode-LWL beträgt 9/125 Mikrometer.

Während sich in Multimodefasern mehrere Lichtmoden eines Signals einkoppeln, koppelt sich in Singlemodefasern aufgrund des geringen Kerndurchmessers nur eine Lichtmode ein. Dadurch unterscheiden sich die Fasertypen in den möglichen Bandbreiten und den maximalen Längen, die ohne zusätzliche Verstärker erreicht werden können. Die Fasertypen können bei der Verbindung von Systemen in einigen Fällen nicht gemischt werden.

Eingesetzt werden Lichtwellenleiter unter anderem in folgenden Bereichen:

- bei der Überbrückung großer Entfernungen in Weitverkehrsnetzen (Wide Area Network, WAN),
- in Stadtnetzen (Metropolitan Area Network, MAN),
- in Unternehmensnetzen (Local Area Network, LAN) für die Verbindungen zwischen den Gebäuden und in die Etagen,
- in Bereichen mit hohen elektromagnetischen Störstrahlungen sowie
- in Speichernetzen (Storage Area Network, SAN) in Rechenzentren zur Verbindung der Systeme zur Übertragung höchster Datenraten.

Entscheidend für die Qualität der Verbindungen ist auch die Auswahl der Steckverbinder für die Glasfaserinfrastruktur.

Die Verwendung von Lichtwellenleitern bietet folgende Vorteile:

- LWL erlauben hohe Bandbreiten in Verbindung mit großen überbrückbaren Entfernungen im Vergleich zu Kupferkabeln.
- LWL sind unempfindlich gegenüber elektromagnetischen Feldern.
- Es entstehen keinerlei Übersprecheffekte wie bei elektrischen Leitern.
- LWL bieten eine potentialfreie Verbindung zwischen den Endstellen der Verkabelung.
- Ein Abhören ist nur mit hohem technischen Aufwand möglich.
- Kabel mit hohen Faserzahlen können kompakter gebaut werden als vergleichbare Kupferkabel bei deutlich geringerem Gewicht.
- Die Brandlast ist bei LWL im Vergleich zu Kupferkabeln geringer. Die Gründe hierfür sind die im Vergleich geringere erforderliche Menge an Material, der Materialmix im Kabelaufbau und die möglichen hohen Faserzahlen ohne die Bauform massiv zu vergrößern.

Der Einsatz von Lichtwellenleitern ist jedoch mit folgenden Nachteilen verbunden:

- Der Installationspreis für LWL liegt vor allem durch die notwendigen Spleißarbeiten höher als bei Kupferkabeln.
- Die Koppel-Komponenten zum Betrieb von LWL, insbesondere für Singlemode-LWL, sind teurer als solche für Kupferkabel.
- Die LAN-Anbindung über TP-Kabel wird von gängigen Arbeitsplatz-Computern in der Grundausstattung meist besser unterstützt als über LWL. Arbeitsplatz-Clients werden derzeit meist über Kupferkabel an das LAN angeschlossen.

Zu beachten ist, dass hier die jeweilige maximale Länge genannt ist. Diese setzt sich häufig aus dem eigentlichen Installationskabel und den Anschlusskabeln (Patchkabeln) zusammen. Für 1000Base-T sollte also z. B. die Länge des Installationskabels 90 m nicht überschreiten, um genügend Längenspielraum für Patchkabel zu haben.

Zusammenfassung

Im WAN und MAN sind LWL-Verkabelungen mit Singlemode-Fasern Standard. In der LAN-Verkabelung sind diese Fasern heute zwischen den Gebäuden und bei weiter entfernten Etagenverteilern aufgrund der Längeneinschränkungen von 10 Gigabit Ethernet unbedingt zu empfehlen.

Der Einsatz von LWL bis zum Arbeitsplatz und damit der Wegfall der Kupferverkabelung auf der Etage kann nur in einer Gesamtbetrachtung bewertet werden.

Für den Einsatz von LWL sprechen:

- die günstigere Brandlastsituation,
- die bessere Abhörsicherheit von LWL,
- EMV-Neutralität,
- mögliche Einsparungen im Trassenbau,
- Flächeneinsparungen durch die geringere Zahl erforderlicher Verteilerräume und damit Einsparungen in der Elektroverkabelung für die Verteilerräume,
- Vereinfachungen im USV- und Erdungskonzept.

Gegen LWL sprechen andererseits:

- die höheren Kosten für Schnittstellenkarten in den Endgeräten und in den Netzkomponenten
- die meist weiter bestehende Notwendigkeit einer Telefonverkabelung über Kupferkabel,
- mögliche Einschränkungen für die Umsetzung von Power-over-Ethernet für IP-Telefonie oder auch für den Anschluss von Access-Points im WLAN.

Für Neuinstallationen wie auch bei Modernisierungen ist es daher zu empfehlen, mit einem Fachplaner die Anforderungen aus technischer, sicherheitstechnischer und wirtschaftlicher Sicht zu erarbeiten und auszuwerten.

Twisted-Pair-Kabel

Bei Kupferkabeln für die IT wird ein symmetrischer Kabelaufbau verwendet. Bei diesem Kabelaufbau werden jeweils zwei Adern miteinander zu einem Paar verdrallt und vier dieser Paare zu einem Kabel (Twisted-Pair-Kabel, TP) miteinander verseilt. Der Durchmesser der Adern, deren Isoliermaterial inklusive der Farbstoffe, die Art der Verseilung und Abschirmung dieser Paare unterscheidet die Kabel hinsichtlich ihrer möglichen Bandbreite und ihrer Störunempfindlichkeit. Für eine einheitliche Bezeichnung der Kabeltypen schlägt die ISO/IEC 11801 "Informationstechnik - Anwendungsneutrale Standortverkabelung" in der 2. Ausgabe eine Vereinheitlichung der Typenbezeichnungen vor, welche die Konstruktionselemente von außen nach innen gelesen eindeutig bestimmt. Diese ist nach dem Schema XX/YTP aufgebaut. XX gibt hier den Gesamtschirm des Kabels an. Mögliche Typen wären U (ungeschirmt), F (Folienschirm) und SF (Schirm aus Geflecht und Folie). Y definiert den Einzelschirm mit den Möglichkeiten U und F. TP steht in jedem Fall für Twisted Pair Kabel.

INF.4.M2 Planung der Kabelführung [Leiter Haustechnik]

Kabeltrassen (z. B. Fußbodenkanäle, Fensterbank-Kanäle, Pritschen, Rohrtrassen im Außenbereich) sind ausreichend zu dimensionieren. Es muss einerseits genügend Platz vorhanden sein, um eventuell notwendige Erweiterungen des Netzes vornehmen zu können. Andererseits sind zur Verhinderung des Übersprechens (gegenseitige Beeinflussung von Kabeln) eventuell Mindestabstände zwischen den Kabeln einzuhalten. Insbesondere ist bei der Nutzung von gemeinsamen Trassen für Energie- und IT-Verkabelung sicherzustellen, dass die Trassen durch einen Mittelsteg getrennt sind. Schon durch eine einfache getrennte Führung von Stromkabeln und IT-Kabeln lassen sich Störungen der IT meist vermeiden.

Ist es nicht möglich, Trassen mit ausreichenden Reserven zu errichten, sollte zumindest darauf geachtet werden, dass im Bereich der Trassenführung genügend Platz ist, um Erweiterungen unterzubringen. Werden Wand- und Deckendurchbrüche in hinreichender Größe ausgelegt, kann auf spätere lärm-, schmutz- und kostenintensive Arbeiten verzichtet werden. Bei Verwendung von nachinstallationsfähigen Brandschotten können Durchbrüche so gerüstet werden, dass der Schutz vor Feuer und Verrauchung stets gewährleistet ist, zugleich die Nachführung von Kabeln aber jederzeit problemlos möglich bleibt.

Zu beachten ist, dass Durchbrüche durch Wände mit einer Feuerwiderstandsklasse nur zu 60 % belegt werden dürfen, um eine wirksame Schottung dieser Öffnungen erreichen zu können. Gegebenenfalls sollten für spätere Erweiterungen bei der Errichtung Durchbrüche vorgesehen und diese vorerst mittels Weichschott oder Brandschutzkissen verschlossen werden.

Wichtig ist, dass die Trassendimensionierung immer im Zusammenhang mit der Auswahl der Kabeltypen geplant werden muss. Beispielsweise kann durch Verwendung einiger vieladriger Kabel gegenüber vielen kleinen Kabeln Platz eingespart werden. Durch den Einsatz von geschirmten Kabeln oder Lichtwellenleitern kann Übersprechen verhindert werden. So kann auch auf Trassenwegen mit wenig Platz ein störungsfreier Betrieb gewährleistet werden.

Bei der Planung von Kabeltrassen ist darauf zu achten, dass erkennbare Gefahrenquellen umgangen werden. Grundsätzlich sollten Trassen nur in den Bereichen verlegt werden, die ausschließlich innerhalb der Räumlichkeiten einer Institution zugänglich sind. Ein übersichtlicher Aufbau der Trassen erleichtert die Kontrolle. Trassen und einzelne Kabel sollten immer so verlegt werden, dass sie vor direkten Beschädigungen durch Personen, Fahrzeuge und Maschinen geschützt sind.

Der Standort von Geräten sollte so gewählt werden, dass die daran angeschlossenen Kabel nicht im Lauf- oder Fahrbereich liegen. Ist dies nicht zu vermeiden, sind die Kabel den zu erwartenden Belastungen entsprechend durch geeignete Kanalsysteme zu schützen.

Grundsätzlich ist bei Geräteanschlussleitungen auf eine ausreichende Zugentlastung der Kabel in den Steckern zu achten. Bisweilen kann es sinnvoll sein, auf die vorgesehene Verschraubung von Steckern zu verzichten. Bei überhöhter Zugbelastung werden dann nur Steckverbindungen auseinander gerissen und nicht die Stecker-Kabel- oder Stecker-Geräte-Verlötung.

Tiefgaragen stellen ein großes Problem für eine schadensmindernde Kabelführung dar. Durch die Sicherheitsschaltungen und die langen Offenzeiten von Einfahrtstoren ist der Zutritt von Fremdpersonen zu Tiefgaragen nie auszuschließen. Durch die in der Regel geringen Deckenhöhen ist es mit einfachen Mitteln möglich, sich Zugriff zu dort verlaufenden Trassen zu verschaffen. Durch Trassen im Fahrbereich kann die zulässige Fahrzeughöhe unterschritten werden. Beschädigungen oder Zerstörungen der Trassen und Kabel durch zu hohe Fahrzeuge sind dann nicht auszuschließen.

Bei gemeinsam mit Dritten genutzten Gebäuden ist darauf zu achten, dass Kabel nicht in Fußboden-, Decken- oder Wandkanälen durch deren Bereiche führen. Alle Kanalsysteme sind gegenüber den fremdgenutzten Bereichen mechanisch fest zu verschließen. Besser ist es, sie an den Bereichsgrenzen enden zu lassen.

Durch Bereiche mit hoher Brandgefahr sollten möglichst keine Kabel verlegt werden. Ist dies nicht möglich und ist der Funktionserhalt aller auf der Trasse liegenden Kabel erforderlich, ist der entsprechende Trassenbereich mit Brandabschottung zu versehen. Ist der Funktionserhalt nur für einzelne Kabel erforderlich, sollte dafür ein entsprechendes Kabel und die dazu gehörige Befestigung gewählt werden. Ein Funktionserhalt-Kabel kann nie allein die geforderte Funktion erfüllen. Die Kabelanlage ist als Ganzes zu betrachten, dazu gehört auch die Befestigung, wie Trassen, Schellen oder Rohre. Ebenso wichtig ist, dass die Kabelanlage nicht durch darüber befindliche Teile ohne Funktionserhalt zerstört werden kann, wenn diese im Brandfall herabfallen.

In Produktionsbetrieben ist mit hohen induktiven Lasten und daraus resultierenden Störfeldern zu rechnen. Auch diese sind bei der Trassen- und Kabelverlegung zu berücksichtigen. Für den Schutz der Kabel gilt sinngemäß das gleiche wie bei der Brandabschottung.

Bei Erdtrassen ist ca. 10 cm über der Trasse ein Warnband zu verlegen. Bei einzelnen Kabeln (ohne Rohr) ist der Einbau von Kabelabdeckungen sinnvoll.

Leitungen müssen so verlegt sein, dass ein Sturm sie nicht bewegen kann. Beispielsweise sollte dafür Sorge getragen werden, dass Leitungen auf freien Dachflächen mindestens alle 5 m angemessen befestigt sind. Hierbei sollte berücksichtigt werden, dass bei einem Sturm starke Kräfte auf die Kabel oder Kabelstränge wirken können. Außerdem müssen Leitungen geschützt gegen mechanische Beschädigungen verlegt werden, da Gegenstände darauf fallen könnten. Leitungen auf Dachflächen oder in Bereichen, die mit Lamellenwänden verkleidet sind, sollten daher immer in Schutzrohren verlegt sein.

INF.4.M3 Fachgerechte Installation [Leiter Haustechnik]

Die Installationsarbeiten der IT-Verkabelung erfordern besondere Fachkunde und Sorgfalt. Sofern Hersteller von Kabeln und passiven Komponenten Gewährleistungen anbieten, die über gesetzliche Mindestgrenzen hinaus gehen, erfolgt dies oft nur unter der Voraussetzung, dass ein Unternehmen mit bestätigter Qualifikation die Installation vornimmt.

Die entscheidenden Kriterien für eine fachgerechte Ausführung der IT-Verkabelung sollten vom Auftraggeber in allen Phasen überprüft werden.

Zunächst ist bei Anlieferung des Materials zu prüfen, ob die richtigen Kabel und Anschlusskomponenten geliefert wurden. Zueinander passende Kategorien von Kabeln und Anschlusskomponenten (z. B. Schirmung) sind dabei der erste Prüfschritt.

Wenn die gelieferten Kabel und zugehöriges Material nicht unmittelbar eingebaut werden, so ist eine angemessene Lagerung sicherzustellen. Der Lagerort muss trocken und vor starken klimatischen Einflüssen geschützt sein.

Es wird empfohlen, das eingelagerte Material in der Originalverpackung zu belassen, bis es installiert wird.

Bei der Verlegung von IT-Kabeln sollte besondere Sorgfalt darauf gelegt werden, dass die Montage keine Beschädigungen hervorruft und dass die Kabelwege so gewählt sind, dass Beschädigungen der verlegten Kabel durch die normale Nutzung des Gebäudes ausgeschlossen sind.

Zudem ist generell darauf zu achten, dass IT-Kabel getrennt von der elektrotechnischen Verkabelung geführt werden. Schon Trennstege auf gemeinsam genutzten Trassen helfen meist, Beeinflussungen des IT-Kabels durch Stromkabel zu verhindern.

Bei der Verlegung müssen schützende Maßnahmen und Belastungsgrenzen beachtet werden:

- Vor der Verlegung müssen Mauerdurchbrüche und vergleichbare Durchgänge entgratet und gerundet werden, um beim Einziehen und Befestigen eine mechanische Beschädigung der Kabelummantelung zu vermeiden.
- Der Mindest-Biegeradius für Verlegung und Betrieb darf nicht unterschritten werden. Falls dieser nicht auf dem Kabel vermerkt ist, gilt nach EN 50173, dass der geringst zulässige Biegeradius nicht kleiner als der 8-fache Außendurchmesser des Kabels sein darf. Entsprechend ist sicherzustellen, dass Biegungen in Kabelkanälen und Kabeltrassen den zulässigen Biegeradien entsprechen.
- Gegebenenfalls gibt der Hersteller in Datenblätter zu den Kabeln typspezifisch zwei Biegeradien an: der angegebene Biegeradius mit dem größeren Wert gilt als maximale Biegebelastung für das Einziehen der Kabel. Der kleinere Wert gilt für das fertig verlegte Kabel.
- Ebenfalls ist dem Datenblatt die maximale Zugbelastung des Kabeltyps zu entnehmen.
- Beim Kabeleinzug dürfen nur geeignete Schmiermittel als Einzugshilfe verwendet werden. Generell sind öl- und fettfreie Schmiermittel (z. B. Talkum) einzusetzen.
- Bei der Befestigung der Kabel auf Kabeltrassen mit Kabelbindern oder Kabelschellen dürfen die Kabel keinesfalls gequetscht werden.

Kabel sollten unter Putz, in Kabelkanälen oder auf Kabeltrassen verlegt werden. Die offene Verlegung von Kabeln ist durchaus zulässig, es ist aber sicherzustellen, dass keine Beschädigung des Kabels etwa durch Überfahren von Kabeln mit Büromöbeln oder Transportgeräten auftreten kann.

Unter dem Begriff "Anwendungsneutrale Kommunikationskabelanlagen" wurde 1995 erstmalig eine Norm veröffentlicht, welche Topologie und Klassifizierung von Übertragungsstrecken mit definierten Eigenschaften sowie eine einheitliche Schnittstelle zum Anschluss der Endgeräte beschreibt. Diese Vorgaben gelten nicht nur für den Einsatz in Bürogebäuden, sondern lassen sich auch auf andere Anwendungsgebiete übertragen.

Unter der Verantwortung des Europäischen Komitees für Elektrotechnische Normung (CENELEC) werden die Normen überwacht, mit den Internationalen Gremien (ISO/IEC) abgestimmt und bei Bedarf weiterentwickelt und verfeinert.

Die Normen unterstützen die Anwender in den Phasen der Gebäudeplanung, des Verkabelungsentwurfs, der Planung, der Realisierung und des Betriebs von Kommunikationskabelanlagen.

Neben der EN 50173-1 - Anwendungsneutrale Kommunikationskabelanlagen, Allgemeine Anforderungen sowie der Teile 2 Bürogebäude, 3 Industriell genutzte Gebäude, 4 Wohneinheiten und 5 Rechenzentren gibt es weitere Normen, die in der Planung und Ausführung der IT-Verkabelung Anwendung finden.

Übertragen auf den Lebenszyklus bei der IT-Verkabelung lassen sich Normen wie folgt zuordnen:

Gebäudeplanung

- EN 50310 - Anwendung von Maßnahmen für Erdung und Potentialausgleich in Gebäuden mit Einrichtungen der Informationstechnik
  5.2: Gemeinsame Potentialausgleichsanlage (CBN) in einem Gebäude
  6.3: AC-Verteilung und Anschluss des Schutzleiters (TN-S)

Verkabelungsentwurf

- EN 50173-1 - Anwendungsneutrale Kommunikationskabelanlagen, Allgemeine Anforderungen und Bürobereiche
  4: Topologie
  5: Leistungsvermögen der Übertragungsstrecken
  7: Anforderungen an Kabel
  8: Anforderungen an Verbindungstechnik
  9: Anforderungen an Schnüre
  A.1: Grenzwerte für Strecken

Planung

- EN 50174-1 - Installation von Kommunikationsverkabelung, Spezifikation und Qualitätssicherung
  4: Betrachtungen zu Festlegungen
  5: Qualitätssicherung
  7: Verwaltung der Verkabelung
- EN 50174-2 - Installation von Kommunikationsverkabelung, Installationsplanung und -praktiken in Gebäuden
  4: Sicherheitsanforderungen
  5: Allgemeine Festlegungen für die Verlegung von metallener Verkabelung und Lichtwellenleiterverkabelung
  6: Zusätzliche Festlegungen für die Verlegung metallener Verkabelung
  7: Zusätzliche Festlegungen für die Verlegung von Lichtwellenleiterverkabelung
- EN 50174-3 - Installation von Kommunikationsverkabelung, Installationsplanung und -praktiken im Freien
- EN 50310 - Anwendung von Maßnahmen für Erdung und Potentialausgleich in Gebäuden mit Einrichtungen der Informationstechnik
  5.2: Gemeinsame Potentialausgleichsanlage (CBN) in einem Gebäude
  6.3: AC-Verteilung und Anschluss des Schutzleiters (TN-S)

Realisierung

- EN 50174-1 - Installation von Kommunikationsverkabelung, Spezifikation und Qualitätssicherung
  6: Dokumentation
  7: Verwaltung der Verkabelung
- EN 50174-2 - Installation von Kommunikationsverkabelung, Installationsplanung und -praktiken in Gebäuden
  4: Sicherheitsanforderungen
  5: Allgemeine Festlegungen für die Verlegung von metallener Verkabelung und Lichtwellenleiterverkabelung
  6: Zusätzliche Festlegungen für die Verlegung metallener Verkabelung
  7: Zusätzliche Festlegungen für die Verlegung von Lichtwellenleiterverkabelung
- EN 50174-3 - Installation von Kommunikationsverkabelung, Installationsplanung und -praktiken im Freien
- EN 50310 - Anwendung von Maßnahmen für Erdung und Potentialausgleich in Gebäuden mit Einrichtungen der Informationstechnik
  5.2: Gemeinsame Potentialausgleichsanlage (CBN) in einem Gebäude
  6.3: AC-Verteilung und Anschluss des Schutzleiters (TN-S)
- EN 50346 - Installation von Verkabelung, Prüfen installierter Verkabelung
  4: Allgemeine Anforderungen
  5: Prüfparameter für symmetrische Verkabelung
  6: Prüfparameter für Lichtwellenleiterverkabelung

Betrieb

- EN 50174-1 - Installation von Kommunikationsverkabelung, Spezifikation und Qualitätssicherung
  5: Qualitätssicherung
  7: Verwaltung der Verkabelung
  8: Instandsetzung und Instandhaltung

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "IT-Verkabelung".

INF.4.M4 Anforderungsanalyse für die IT-Verkabelung

Bei der Analyse der Anforderungen, die Einfluss auf eine zukunftssichere, bedarfsgerechte und wirtschaftliche Ausführung der IT-Verkabelung haben, müssen verschiedene Fragestellungen bearbeitet werden.

Die meistens im Vordergrund stehende Frage ist die nach dem erforderlichen Daten-Durchsatz. In ihr wird zunächst die kurzfristig geplante Nutzung durch die Anwender in der Institution und darauf aufbauend die längerfristige Entwicklung der IT-Nutzung abgeschätzt.

Zwei Entwicklungen sind dabei zu berücksichtigen:

Zum einen wird Bandbreite stetig billiger. Die Folge ist, dass Dienste, die von Dritten angeboten und von diesen bezogen werden, immer höhere Anforderungen an die Kapazität der IT-Verkabelung stellen. Nach den IT-typischen Diensten wie E-Mail und WWW werden nun auch Sprach- und Bildübertragung bis hin zum digitalen Fernsehen zum Inhalt von IT-Netzdiensten. Der damit steigende Bedarf an Bandbreite muss bei der Auswahl der Qualität der IT-Verkabelung berücksichtigt werden.

Zum zweiten wird das IT-Netz zum Träger für immer weitere Anwendungen. Alle Anwendungen, die die Protokolle und Standards der IT-Welt nutzen können, werden sie voraussichtlich auch einsetzen. Das bedeutet, dass ein IT-Netz und damit die IT-Verkabelung zukünftig nicht mehr nur als Träger der Kommunikation zwischen Rechnern dient. Auch die Telefonie und Anwendungen, die bislang auf eigene, anwendungsspezifische Netztechnik angewiesen sind, werden zur Nutzung einheitlicher IT-Technik weiterentwickelt. Diese absehbaren Entwicklungen haben zur Folge, dass die Anzahl der Anschlüsse entsprechend zu planen ist und dass kein Teil eines Gebäudes mehr bei der Planung einer IT-Verkabelung ausgespart werden kann. Zudem ist die interne Verkabelung eines Gebäudes flexibel und erweiterbar auszulegen, weil eine Nutzungsänderung von Räumen oder Gebäudeteilen zugleich auch eine Änderung der Anforderungen an den Netzanschluss darstellen wird.

Trotz Vereinheitlichung der Technik ist es in einigen Fällen erforderlich, unterschiedliche oder separate Kabel für bestimmte Anwendungen einzuplanen. Gerade in besonders sicherheitsbedürftigen Anwendungsbereichen, wie Alarm gebender Technik oder bei der Steuerung von Maschinen und Anlagen, wird es angemessen oder sogar nötig sein, eigene Kabel und Vermittlungstechnik für solche Anwendungen zu verwenden. Besitzen die Anwendungsbereiche einen unterschiedlichen Schutzbedarf und können diese nicht auf einem anderen Weg geschützt werden (z. B. mit VPNs), sollte generell eine Trennung erfolgen.

Verfügbarkeit

Das Schutzziel Verfügbarkeit wird zunächst durch eine sorgfältige Planung und Ausführung der Kabeltrassen verfolgt. Wenn die Anforderungen der Nutzer so weit gehen, dass auch bei umfassenderen Vorfällen die Anbindung und die Netzinfrastruktur des Gebäudes nutzbar bleiben muss, so muss dies durch eine durchdachte redundante Trassenführung angestrebt werden.

Integrität

Um die Integrität der transportierten Daten sicherzustellen, ist die Abschirmung gegen äußere Einflüsse das oberste Gebot. Das bedeutet vor allem, dass die IT-Verkabelung getrennt von der elektrotechnischen Verkabelung zu führen ist. Zudem ist zu bestimmen, welche Kabeltypen für die Einsatzanforderungen angemessen sind.

Vertraulichkeit

Wenn Vertraulichkeit der transportierten Daten, also Abhörsicherheit des Kabels, ein wesentlicher Aspekt ist, sind Lichtwellenleiter (LWL) die erste Wahl. Sie erfordern weitaus mehr technischen Aufwand für den potentiellen Lauscher an der Leitung als alle Kupfer-basierten Lösungen.

Wichtiger noch ist der Schutz von Verteilern und Anschlussdosen, um zu verhindern, dass normale IT-Geräte für Abhörversuche an das lokale Netz angeschlossen werden können. Das gilt natürlich auch für eine LWL-Verkabelung.

In vielen Fällen kann die Vertraulichkeit und Integrität der transportierten Daten alternativ oder ergänzend mit Hilfe von kryptographischen Verfahren geschützt werden, sofern die angeschlossenen Endgeräte und die genutzten Übertragungsprotokolle dies unterstützen. Zum Schutz der Verfügbarkeit tragen kryptographische Verfahren hingegen nur in Spezialfällen bei.

Weitere Anforderungen

Es ist zu beachten, dass auch die Energieversorgung von aktiven Komponenten, wie IP-Telefone oder WLAN-Access Points, durch die IT-Verkabelung stattfinden kann oder soll. Wo der Anschluss solcher Geräte zu planen ist, wird Kupferverkabelung obligatorisch, weil die Stromversorgung nur über Kupferkabel möglich ist.

INF.4.M5 Abnahme der IT-Verkabelung [Leiter Haustechnik]

Bei der Analyse der Anforderungen, die Einfluss auf eine zukunftssichere, bedarfsgerechte und wirtschaftliche Ausführung der IT-Verkabelung haben, müssen verschiedene Fragestellungen bearbeitet werden.

Die meistens im Vordergrund stehende Frage ist die nach dem erforderlichen Daten-Durchsatz. In ihr wird zunächst die kurzfristig geplante Nutzung durch die Anwender in der Institution und darauf aufbauend die längerfristige Entwicklung der IT-Nutzung abgeschätzt.

Zwei Entwicklungen sind dabei zu berücksichtigen:

Zum einen wird Bandbreite stetig billiger. Die Folge ist, dass Dienste, die von Dritten angeboten und von diesen bezogen werden, immer höhere Anforderungen an die Kapazität der IT-Verkabelung stellen. Nach den IT-typischen Diensten wie E-Mail und WWW werden nun auch Sprach- und Bildübertragung bis hin zum digitalen Fernsehen zum Inhalt von IT-Netzdiensten. Der damit steigende Bedarf an Bandbreite muss bei der Auswahl der Qualität der IT-Verkabelung berücksichtigt werden.

Zum zweiten wird das IT-Netz zum Träger für immer weitere Anwendungen. Alle Anwendungen, die die Protokolle und Standards der IT-Welt nutzen können, werden sie voraussichtlich auch einsetzen. Das bedeutet, dass ein IT-Netz und damit die IT-Verkabelung zukünftig nicht mehr nur als Träger der Kommunikation zwischen Rechnern dient. Auch die Telefonie und Anwendungen, die bislang auf eigene, anwendungsspezifische Netztechnik angewiesen sind, werden zur Nutzung einheitlicher IT-Technik weiterentwickelt. Diese absehbaren Entwicklungen haben zur Folge, dass die Anzahl der Anschlüsse entsprechend zu planen ist und dass kein Teil eines Gebäudes mehr bei der Planung einer IT-Verkabelung ausgespart werden kann. Zudem ist die interne Verkabelung eines Gebäudes flexibel und erweiterbar auszulegen, weil eine Nutzungsänderung von Räumen oder Gebäudeteilen zugleich auch eine Änderung der Anforderungen an den Netzanschluss darstellen wird.

Trotz Vereinheitlichung der Technik ist es in einigen Fällen erforderlich, unterschiedliche oder separate Kabel für bestimmte Anwendungen einzuplanen. Gerade in besonders sicherheitsbedürftigen Anwendungsbereichen, wie Alarm gebender Technik oder bei der Steuerung von Maschinen und Anlagen, wird es angemessen oder sogar nötig sein, eigene Kabel und Vermittlungstechnik für solche Anwendungen zu verwenden. Besitzen die Anwendungsbereiche einen unterschiedlichen Schutzbedarf und können diese nicht auf einem anderen Weg geschützt werden (z. B. mit VPNs), sollte generell eine Trennung erfolgen.

Verfügbarkeit

Das Schutzziel Verfügbarkeit wird zunächst durch eine sorgfältig Planung und Ausführung der Kabeltrassen verfolgt. Wenn die Anforderungen der Nutzer so weit gehen, dass auch bei umfassenderen Vorfällen die Anbindung und die Netzinfrastruktur des Gebäudes nutzbar bleiben muss, so muss dies durch eine durchdachte redundante Trassenführung angestrebt werden.

Integrität

Um die Integrität der transportierten Daten sicherzustellen, ist die Abschirmung gegen äußere Einflüsse das oberste Gebot. Das bedeutet vor allem, dass die IT-Verkabelung getrennt von der elektrotechnischen Verkabelung zu führen ist. Zudem ist zu bestimmen, welche Kabeltypen für die Einsatzanforderungen angemessen sind.

Vertraulichkeit

Wenn Vertraulichkeit der transportierten Daten, also Abhörsicherheit des Kabels, ein wesentlicher Aspekt ist, sind Lichtwellenleiter (LWL) die erste Wahl. Sie erfordern weitaus mehr technischen Aufwand für den potentiellen Lauscher an der Leitung als alle Kupfer-basierten Lösungen.

Wichtiger noch ist der Schutz von Verteilern und Anschlussdosen, um zu verhindern, dass normale IT-Geräte für Abhörversuche an das lokale Netz angeschlossen werden können. Das gilt natürlich auch für eine LWL-Verkabelung.

In vielen Fällen kann die Vertraulichkeit und Integrität der transportierten Daten alternativ oder ergänzend mit Hilfe von kryptographischen Verfahren geschützt werden, sofern die angeschlossenen Endgeräte und die genutzten Übertragungsprotokolle dies unterstützen. Zum Schutz der Verfügbarkeit tragen kryptographische Verfahren hingegen nur in Spezialfällen bei.

Weitere Anforderungen

Es ist zu beachten, dass auch die Energieversorgung von aktiven Komponenten, wie IP-Telefone oder WLAN-Access Points, durch die IT-Verkabelung stattfinden kann oder soll. Wo der Anschluss solcher Geräte zu planen ist, wird Kupferverkabelung obligatorisch, weil die Stromversorgung nur über Kupferkabel möglich ist.

INF.4.M6 Laufende Fortschreibung und Revision der Netzdokumentation

Die IT-Verkabelung sollte nach Abschluss der Installation einem Abnahmeprozess unterzogen werden, der auch die Aspekte der Informationssicherheit umfasst.

Eine Abnahme darf erst dann erfolgen, wenn alle durchzuführenden Aufgaben abgeschlossen sind, der Ausführende die Maßnahme zur Abnahme gemeldet hat und sich bei den Kontrollen durch den Auftraggeber keine inakzeptablen Mängel gezeigt haben. Der Abnahmetermin sollte zeitlich so gewählt werden, dass die Kontrollen zur Abnahme in ausreichender Zeit vorbereitet werden können.

Der Abschluss aller durchzuführenden Aufgaben wird im Allgemeinen durch das Aufmaß dieser Leistungen bestätigt. Neben der korrekten Abrechnung und dem tatsächlichen Umfang der Leistungen sind bei der Abnahme die Aspekte der Informationssicherheit zu kontrollieren.

Als vorbereitende Kontrollen sind nachfolgende Punkte sinnvoll:

- Alle zur Installation gehörenden Dokumentationen sind auf Vollständigkeit und Plausibilität zu überprüfen.
- Vor allem die Messprotokolle sind auf ihre Werte zu überprüfen. Es ist zu empfehlen, besonders auffällige Messergebnisse für eine Nachmessung im Rahmen der Abnahme auszuwählen.

Die Durchführung der Abnahme umfasst folgende Kontrollen und Tätigkeiten:

- Eintragungen in Grundriss-, Lage- und Schrankansichtspläne werden während der Abnahme auf Richtigkeit überprüft.
- Die Lieferung wird auf die richtige Anzahl und die geforderte Qualität kontrolliert.
- Die fachliche Ausführung der Leistungen wird überprüft. Es empfiehlt sich, durch Stichproben z. B. die Installation von Datendosen genau zu kontrollieren, die Einhaltung von Biegeradien und die Verlegung in Trassen zu überprüfen.
- Auffällige Messergebnisse, die bei der Vorbereitung der Abnahme identifiziert wurden, werden nachgemessen.
- Die abgenommenen Anlagenteile, die Mängel und die erforderlichen Nach- und Restarbeiten werden protokolliert.
- Für die Behebung von Mängeln sowie für die Erledigung von Nach- und Restarbeiten werden feste Termine vereinbart, die auch zwingend eingehalten werden müssen.
- Die Garantie und Gewährleistungsfristen werden festgehalten.

Es empfiehlt sich, das Abnahmeprotokoll als Checkliste vorzubereiten. Die Checkliste sollte auch Punkte zu allgemeinen Anforderungen an die Betriebsräume enthalten, welche über den Rahmen der Maßnahme hinausgehen, um den allgemeinen Zustand und die Qualität der Anlagen festzuhalten. Dadurch wird der Betrieb der Anlagen umsichtig unterstützt und Ausfällen vorgebeugt.

Diese Punkte sind nicht relevant für die Abnahme der IT-Verkabelung und werden im Nachgang an die zuständige Stelle weitergeleitet.

Es empfiehlt sich, die Checklisten für die Abnahme so zu gestalten, dass diese bereits die Installation- und Inbetriebnahme dokumentieren sowie die Maßnahmen zur Vorbereitung der Abnahme protokollieren. Die Checklisten sollten sich auf das notwendige Maß beschränken. Daher ist es sinnvoll, die enthaltenen Punkte zu hinterfragen, wo nötig zu ergänzen und um unwesentliche Punkte zu bereinigen.

Das Abnahmeprotokoll ist von den Teilnehmern und Verantwortlichen rechtsverbindlich zu unterzeichnen.

Nach der Abnahme müssen die Mängelbehebung sowie die Nach- und Restarbeiten kontrolliert werden. Soweit dies vertraglich und rechtlich zulässig ist, sollten erst danach die Rechnungen freigegeben werden. Die zusätzlich festgestellten Anmerkungen sind an die betroffenen Fachabteilungen weiterzuleiten.

INF.4.M7 Entfernen und Deaktivieren nicht mehr benötigter IT-Verkabelung [Leiter Haustechnik]

Netze sind einer laufenden Veränderung durch Nachverkabelungen, Umbau und Erweiterungsmaßnahmen bis hin zu Updates und Upgrades von aktiven Netzkomponenten unterworfen. Entsprechend muss die Dokumentation der IT-Verkabelung als ein elementarer Bestandteil einer jeden Veränderung im Netz betrachtet und behandelt werden. Erst nach Abschluss der Dokumentation gilt die Änderungsmaßnahme auch als vollständig erledigt.

Neben der allgemeinen Betriebssicherheit und Nachvollziehbarkeit dient eine konsistente Dokumentation der IT-Verkabelung auch folgenden Zielen:

- Kurze Umschaltzeiten bei Netzerweiterungen,
- Einfache Fehlereingrenzung und -suche,
- Kurze Wiederherstellungszeiten im Fehlerfall,
- Wirtschaftlichkeit von Wartungsverträgen.

Wichtig ist, dass alle von der Änderung betroffenen Dokumentationsbereiche leicht erfasst und angepasst werden können. Eine Dokumentationsrichtlinie vereinfacht den Umgang mit der Dokumentation. Sie sollte die Abläufe, die Dokumentationsbereiche und die Vorgaben beschreiben, beispielsweise auch Namens- und Nummerierungsschemata.

Außerdem sollte geprüft werden, ob der Einsatz eines Dokumentenmanagements für die Netzdokumentation zweckmäßig ist. Ein Dokumentenmanagement kann unter anderem folgende Aspekte bei der Dokumentation erleichtern:

- Dokumentation von Änderungen bereits während der Planungsphase,
- Information aller beteiligten Personen über die Planungen,
- Integration von Freigabeprozessen,
- Archivierung von Altdokumentation.

Verschiedene Software-Werkzeuge können darüber hinaus die Dokumentation der Kabel und der Netzkomponenten inklusive deren Verschaltung unterstützen. Manche dieser Werkzeuge ermöglichen die Kopplung und Integration mit Netzmanagementsystemen. Auch die aktive Überwachung von Patchungen in der passiven Infrastruktur wird unterstützt.

INF.4.M8 Brandabschottung von Trassen [Leiter Haustechnik]

Elektroleitungen und IT-Verkabelung werden typischerweise in Installationstrassen konzentriert. Es ist oft festzustellen, dass Trassen entlang von Flucht- und Rettungswegen, durch Tiefgaragen, Lager, Werkstätten oder als Transittrassen durch fremde Nutzungsbereiche führen.

Bei Gebäuden mit mehreren Brandabschnitten unterliegt die Ausführung von Elektroleitungen und der IT-Verkabelung brandschutztechnischen Auflagen. Dies betrifft insbesondere Leitungen, die Brandabschnitte, Wände oder Decken durchqueren oder die in Verkehrswegen verlegt wurden. Speziell wenn die Trassen für Brandmelde-, Alarmierungs-, Löschtechnik oder Sicherheitsbeleuchtung genutzt werden, sind zusätzliche Forderungen nach Funktionserhalt von Elektroleitungen im Brandfall einzuhalten. Daher sollte bei der Planung der Trassen in jedem Fall der Brandschutzbeauftragte hinzugezogen werden. Trassen müssen sowohl Brandschutz als auch Schutz gegen Sabotage bieten. Beides lässt sich durch eine fachgerechte Schottung der Trassen erreichen.

Wenn Elektrokabel in erheblicher Packungsdichte im brandschutztechnisch abgetrennten Kabelkanal geführt sind, können größere Temperaturerhöhungen entstehen. Dies kann ein Ansteigen des elektrischen Leitungswiderstandes mit zusätzlicher Erwärmung nach sich ziehen. Abhilfe lässt sich entweder durch eine Leitungsreduktion oder durch eine ausreichende Be- und Entlüftung erreichen. Daher sind die Vorgaben in DIN VDE 0100-520 "Errichten von Niederspannungsanlagen - Teil 5: Auswahl und Errichtung elektrischer Betriebsmittel - Kapitel 52: Kabel- und Leitungsanlagen" als deutsche Fassung der IEC 60364-5-52 in Abhängigkeit der Verlegeart zu beachten. Dies liegt im Verantwortungsbereich des Elektrofachplaners.

Die marktüblichen Be- und Entlüftungsmethoden bzw. -techniken z. B. durch Lüftungsbausteine haben den Nachteil, dass sie keinen ausreichenden Schutz vor Sabotagehandlungen bieten. Das bedeutet, dass Leitungen mit hohem oder sehr hohem Schutzbedarf, die durch ungeschützte Bereiche führen, wie z. B. eine Tiefgarage, in dieser Ausführung kaum gegen deliktische Handlungen geschützt sind. Hier sind individuelle Planungsmaßnahmen gefordert. Das kann die ausreichende Dimensionierung des Kanals sein, die eine Belüftung des Kanals im gefährdeten Bereich unnötig macht, oder ein spezielles Belüftungskonzept, das auf die spezifischen Sicherungsanforderungen ausgerichtet ist.

Durchbrüche sind nach Verlegung der Leitungen entsprechend der Feuerwiderstandsklasse der Wand bzw. Decke zu schotten. Um die Nachinstallation zu erleichtern, können geeignete Materialien wie Weichschotts oder Brandschutzkissen bei Maßnahmen mit temporärem Charakter verwendet werden. Entsprechende Normen und Richtlinien, wie die DIN 4102 "Brandverhalten von Baustoffen und Bauteilen", sind zu beachten. Kabeltrassen dehnen sich bei Erwärmung z. B. durch Brandeinwirkung aus und können ein Weich- oder Kissenschott zerstören, wenn sie durch Wände geführt werden.

Daher sollten Trassen nicht durch das Schott hindurch geführt werden, sondern beidseitig mindestens 10 cm vor der Wand enden. Diese Praxis erleichtert auch das Ausfächern der Kabel und Leitungen, die nicht als Bündel, sondern einzeln durch das Schott geführt werden müssen.

Häufig werden in einer Trasse unterschiedliche Kabel, z. B. für Telefon, LAN und Haustechnik, geführt. Falls Änderungen der Verkabelung anstehen, sollte bereits in der Planungsphase geklärt werden, ob in absehbarer Zeit auch andere Kabelsysteme ausgewechselt werden sollen. Eine entsprechende Zusammenlegung von Projekten minimiert Ausfallzeiten und erspart zusätzliche Kosten für eine mehrmalige Brandschottung.

Ist die geplante Trassenführung gemäß den brandschutztechnischen Auflagen nicht möglich, so ist eine alternative Trassenführung zu prüfen. Darüber hinaus sollten nach Abschluss der Installationsarbeiten die Brandabschottung in regelmäßigen Abständen, beispielsweise jährlich, kontrolliert werden.

INF.4.M9 Dokumentation und Kennzeichnung der IT-Verkabelung

Für die Wartung, Fehlersuche, Instandsetzung und für eine erfolgreiche Überprüfung der Verkabelung ist eine gute Dokumentation und eine eindeutige Kennzeichnung aller zugehörigen Komponenten erforderlich. Die Güte dieser Revisionsdokumentation ist abhängig von der Vollständigkeit, der Aktualität und der Lesbarkeit der Unterlagen. In jedem Fall ist ein Verantwortlicher für die Dokumentation der Verkabelung zu benennen.

Da es mit zunehmender Größe eines Netzes nicht möglich ist, alle Informationen in einem Plan unterzubringen, ist eine Aufteilung der Informationen sinnvoll. Tatsächliche Lageinformationen sind immer in maßstäbliche Pläne einzuzeichnen. Andere Informationen können in Tabellenform oder Schemapläne geführt werden. Wichtig dabei ist eine eindeutige Zuordnung aller Angaben untereinander. Die Dokumentation sollte somit aus beschreibenden Unterlagen, Listen und Plänen bestehen.

Die beschreibenden Unterlagen, wie z. B. eine Dokumentationsrichtline, enthalten die Informationen über die Abläufe zur Dokumentation, Bezeichnungs- und Kennzeichnungsregelungen. In dieser sollte beispielsweise in allgemeiner Form beschrieben werden, welche Listen und Pläne zu erstellen sind und wie diese auch revisionssicher zu führen sind.

In die Listen- und Bestandspläne sind alle das Netz betreffenden Sachverhalte aufzunehmen. Die Listen sollten unter anderem folgende Informationen enthalten:

- Liefer- und Komponenteninformationen,
- Genaue Kabeltypen (bei Lichtwellenleiterkabel auch Faserqualität),
- Nutzungsorientierte Kabelkennzeichnung,
- Standorte von Zentralen und Verteilern mit genauen Bezeichnungen und Zugangsregelungen mit Ansprechpartnern zu den Gebäuden und Räumlichkeiten,
- Belegungspläne aller Rangierungen und Verteiler,
- Nutzung aller Leitungen, Nennung der daran angeschlossenen Netzteilnehmer,
- Technische Daten von Anschlusspunkten,
- Gefahrenpunkte,
- Vorhandene und zu prüfende Schutzmaßnahmen.

Die Bestandspläne bestehen typischerweise aus:

- Standortübersichten und bemaßten Lageplänen mit der genauen Führung der Trassen und der Primärverkabelung,
- Gebäudeschnitten als Schemapläne und bemaßten Etagengrundrissplänen mit der genauen Lage und Führung der Verteilerräume, Trassen und Kabel sowie den IT-Anschlüssen pro Raum in z. B. Brüstungskanälen und/oder Bodenauslässen,
- Technikraumplänen mit Raumlayout, Doppelbodenraster und Schrankpositionierung, Stromverteilung und Potentialausgleichsschiene sowie einer vorhandenen Klimatisierung,
- Schrankansichtsplänen zur lagerichtigen Beschreibung der eingebauten passiven und aktiven Komponenten inklusive der Steckdosenleisten,
- Physikalischen und logischen Verbindungsplänen des Netzes.

Es muss möglich sein, sich anhand dieser Dokumentation einfach und schnell ein genaues Bild über die Verkabelung zu machen.

Um die Aktualität der Dokumentation zu gewährleisten, ist sicherzustellen, dass alle Arbeiten am Netz rechtzeitig und vollständig demjenigen bekannt werden, der die Dokumentation führt. Es ist z. B. denkbar, die Ausgabe von Material, die Vergabe von Fremdaufträgen oder die Freigabe gesicherter Bereiche von der Mitzeichnung dieser Funktion abhängig zu machen.

Da diese Dokumentation schutzwürdige Informationen beinhaltet, ist sie sicher aufzubewahren und der Zugriff zu regeln. Weiterhin sind die Kabel selbst zu kennzeichnen, um die Informationen aus den Bestandsplänen zuordnen zu können. Die Beschriftung der Kabel muss an beiden Enden erfolgen. Im Bedarfsfall kann die Beschriftung auch sich mehrfach wiederholend am Kabel angebracht werden, um es auch bei der Nachverfolgung in der Trasse eindeutig zu identifizieren. Es sind Kennzeichnungsfelder oder Beschriftungsbänder einzusetzen, die manuell oder maschinell dauerhaft lesbar beschriftet werden. Eine Beschriftung mit Folienstift ist häufig nicht ausreichend.

Die Kabel und Leitungen sollten immer so beschriftet oder gekennzeichnet werden, dass daraus lediglich eine Referenzierung in die Dokumentation erfolgen kann. Eine Kennzeichnung, die einen direkten Rückschluss auf die Bedeutung des Kabels oder der Leitung zulässt, ist unbedingt zu vermeiden, soweit dies nicht auf Grund von anderen Regelungen erforderlich ist.

Sinnvollerweise wird bereits bei der Planung von Verkabelungsmaßnahmen in einem solchen Tool mit der Dokumentation begonnen und diese nach der Realisierung vom Planungsstatus in den Produktivstatus übernommen. Auf diesem Wege ist es leichter, die Nutzer der Dokumentation über bevorstehende Änderungen zu informieren und die Dokumentation aktuell zu halten.

Wenn eine Erneuerung oder Modernisierung der IT-Verkabelung geplant wird, ist zwischen Auftraggeber und den Auftragnehmern (Netzplaner, Lieferanten und Errichtern) zu vereinbaren, wie die Dokumentation der IT-Verkabelung auszuführen ist. Der Auftraggeber muss sicherstellen, dass er bei Inbetriebnahme eine interne und eine externe Dokumentation der Verkabelung besitzt.

Die interne Dokumention umfasst alle Aufzeichnungen, die die Errichtung und den Betrieb der IT-Verkabelung betreffen. Für die interne Dokumentation gilt, dass sie so umfangreich angefertigt und gepflegt werden sollte, dass der Betrieb und die zukünftige Weiterentwicklung bestmöglich unterstützt werden.

Die externe Dokumentation ist die Beschriftung von Anschlüssen zur Unterstützung des Betriebs. Im Sinne des Schutzes vor Sabotage und anderem böswilligen Eingriff gilt, dass die extern sichtbare Dokumentation der Verkabelung (z. B. die Beschriftung der Netzdosen und Kabelenden) so sparsam wie möglich ausfallen sollte. Hier gilt es, einem potentiellen Angreifer so wenig Hinweise wie möglich zu geben, jedoch gleichzeitig dem IT-Personal die notwendigen Kennzeichnungen bereitzustellen, die für ordnungsgemäße und nachvollziehbare Patch- und Vernetzungsarbeiten erforderlich sind.

Bei mittleren und großen Vorhaben zur Verkabelung ist der Einsatz von geeigneter Software zur Dokumentation zwingend. Bereits in der Planungsphase müssen deshalb Vorgaben über Dateiformate und damit über Programm und Version der einzusetzenden Software gemacht werden. So wird sichergestellt, dass der Auftragnehmer seine Dokumentation in einer Form liefern kann, die der Auftraggeber unmittelbar weiter nutzen kann. Ebenso sollten Vorgaben zur Namenskonvention für die Dateien selbst und auch für Elemente und Strukturen, die in den Dateien beschrieben sind, gemacht werden. Die Version einer Datei sollte möglichst schon am Dateinamen erkennbar sein, beispielsweise dadurch dass jeder Dateiname mit einer Datumsangabe der Form JJJJMMTT beginnt.

Auch für die Namenskonventionen und Kennzeichnungen in den Dokumenten sind klare Vorgaben zu machen. Beispielsweise ist zu vereinbaren, wie unterschiedliche Klassen von verlegten Kupferkabeln in Zeichnungen auszuzeichnen sind (Beispiel: L123-cu6a = Leitung 123, Kupfer, CAT 6a).

Ein Problem ergibt sich oft bei Raumnummern: der Architekt vergibt diese üblicherweise in der Planungsphase. Diese Raumnummern werden auch bei der Planung und Ausführung der IT-Verkabelung verwendet. Wenn der Nutzer nach Übernahme des Gebäudes eine andere Systematik für die Kennzeichnung und Beschriftung von Räumen einführt, kann dies zu Unklarheiten, zu Beeinträchtigungen des Betriebes oder zu anderen Sicherheitsproblemen führen.

Beispielsweise kann es passieren, dass durch Inkonsistenzen bei der Raumnummerierung Kabelverbindungen zu falschen Räumen und somit zwischen den falschen IT-Systemen hergestellt werden.

Erster Schritt der Dokumentation der IT-Verkabelung ist die Planungs- und Errichtungsdokumentation. Zu dokumentieren ist zunächst die geplante Topografie des Netzes. Dabei wird in die Gebäude- und Raumplanung zunächst der geplante Verlauf der Wege von Kabeln und Trassen und die Lage der Anschlussdosen eingezeichnet. Vom Errichter sind dann Dokumente zur Ausführung der Verkabelungsarbeiten zu erbringen.

Die Dokumentation der IT-Verkabelung besteht aus:

- Trassenverlauf und -nutzung im Gebäudeabschnitt,
- Trassenverlauf, Leitungsführung und Lage der Anschlussdosen pro Etage,
- Raumpläne für alle Technikräume der IT-Verkabelung mit Schrankaufstellung und eventuell Einspeisungspunkten von Fremdnetzen,
- Schrankansichtspläne mit Schrankeinbauten und Patchplänen,
- Konformitätsnachweise über die auftragsgerechte Ausführung,
- Lieferinformationen, Messprotokolle und Abnahmeprüfungen.

Diese Dokumentation ist Grundlage und wesentlicher Teil der Abnahme des Gewerkes durch den Bauherrn.

Für den späteren Netzbetrieb ist es zweckmäßig, getrennte Dokumente für die Ist-Beschreibung des Netzes und zur Fortschreibung anzufertigen. Die enge Anbindung an die Bauplanung und an typische Programme und Datenformate der Bauplanung (CAD) sind eher in der Errichtungsphase zweckmäßig.

Im laufenden Betrieb ist es oft zweckmäßiger, logische und IT-spezifische Strukturen des IT-Netzes in der Dokumentation zu betonen und bauliche Aspekte unterzuordnen. Zu diesem Zweck sind "IT-nahe" Software-Werkzeuge angemessener. Die Mitarbeiter sind mit der Bedienung solcher Programme meist besser vertraut, als im Umgang mit CAD-Software.

INF.4.M10 Neutrale Dokumentation in den Verteilern

In jedem Verteiler sollte sich eine Dokumentation befinden, die den derzeitigen Stand von Rangierungen und Leitungsbelegungen wiedergibt. Diese Dokumentation ist möglichst neutral zu halten. Nur bestehende und genutzte Verbindungen sind darin aufzuführen. Es sollten, soweit nicht ausdrücklich vorgeschrieben (z. B. für Brandmeldeleitungen), keine Hinweise auf die Nutzungsart der Leitungen gegeben werden. Leitungs-, Verteiler-, und Raumnummern reichen in vielen Fällen aus. Alle weitergehenden Informationen sind in einer Revisions-Dokumentation aufzuführen.

INF.4.M11 Kontrolle bestehender Verbindungen

Alle Verteiler und Zugdosen der Verkabelung sind regelmäßig einer (zumindest stichprobenartigen) Sichtprüfung zu unterziehen. Dabei ist auf folgende Punkte zu achten:

- Spuren von gewaltsamen Öffnungsversuchen an verschlossenen Verteilern,
- Aktualität der im Verteiler befindlichen Dokumentation,
- Übereinstimmung der tatsächlichen Beschaltungen und Rangierungen mit der Dokumentation,
- Unversehrtheit der Kurzschlüsse und Erdungen nicht benötigter Leitungen und
- unzulässige Einbauten oder Veränderungen.

Neben der reinen Sichtkontrolle kann zusätzlich eine funktionale Kontrolle durchgeführt werden. Dabei werden bestehende Verbindungen auf ihre Notwendigkeit und die Einhaltung technischer Werte hin geprüft. Bei Verbindungen, die nicht in zutrittsgeschützten Bereichen verlaufen, ist in zwei Fällen diese Prüfung anzuraten:

- Bei Verbindungen, die sehr selten genutzt und bei denen Manipulationen nicht sofort erkannt werden.
- Bei Verbindungen, auf denen häufig besonders schützenswerte Informationen übertragen werden.

Alle Unregelmäßigkeiten, die bei Sichtkontrollen oder funktionalen Kontrollen festgestellt werden, müssen unverzüglich dokumentiert und den zuständigen Organisationseinheiten gemeldet werden, damit zeitnah die notwendigen weiteren Schritte eingeleitet werden können. Wichtig ist außerdem, dass die festgestellten Unregelmäßigkeiten nicht nur beseitigt, sondern dass auch deren Ursachen ermittelt werden.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

INF.4.M12 Redundanzen für die Verkabelung (A)

Oft sind in größeren Liegenschaften mehrere Gebäude an ein Rechenzentrum, das sich in einem dieser Gebäude befindet, sternförmig angebunden. Es ist zu prüfen, ob zumindest für wichtige Gebäude eine redundante, über unabhängige Trassen geführte primäre IT-Verkabelung geschaffen werden soll.

Ebenso ist zu prüfen, ob die Anschlüsse an IT- oder TK-Provider redundant ausgelegt werden sollen. Um hier eine echte Redundanz zu schaffen, muss mit dem Provider geklärt werden, ob wirklich an unterschiedlichen Orten (Ortsvermittlungsstellen) der Anschluss an ein Carrier-Netz geschaffen wird.

Ob eine redundante Primärverkabelung beziehungsweise eine redundante Anbindung an Provider erforderlich ist, ergibt sich aus den Verfügbarkeitsanforderungen der Institution.

Parallelbetrieb

Innerhalb der Gebäude ist durch den Einsatz geeigneter aktiver Netzkomponenten sicherzustellen, dass die redundanten Leitungen im Betrieb automatisch parallel genutzt werden. So wird gleichzeitig Redundanz geschaffen und die Kapazität erhöht. Dabei ist jedoch zu beachten, dass sich beim Ausfall einer der Leitungen die Übertragungskapazität reduziert. Diese reduzierte Kapazität muss im Notfallvorsorge-Konzept berücksichtigt werden.

Umschaltung

Wenn die eingesetzte Technik oder die über die Verkabelung realisierten Dienste keinen Parallelbetrieb der redundanten Leitungen erlauben, muss bei Störungen der genutzten Leitung auf die jeweilige Ersatzleitung umgeschaltet werden. Diese Umschaltung kann automatisch oder manuell erfolgen.

Wenn kein Parallelbetrieb möglich ist, sollte in sinnvollen Zeitabständen auf die Ersatzleitungen umgeschaltet werden, auch wenn keine tatsächliche Störung vorliegt. Dies dient dazu, die Ersatzleitungen auf Funktionsfähigkeit zu überprüfen. Die Prüfintervalle sollten aus den Verfügbarkeitsanforderungen abgeleitet werden.

Überwachung

Redundanzen bei den Kommunikationsverbindungen können in der Regel nur dann das Verfügbarkeitsniveau wirksam steigern, wenn die Funktionsfähigkeit der Verbindungen überwacht wird. Die Überwachung dient dazu, Störungen, Engpässe und sonstige Unregelmäßigkeiten frühzeitig zu erkennen, damit Probleme zeitnah behoben oder sogar vermieden werden können. Ohne Überwachung besteht unter anderem die erhöhte Gefahr, dass Ausfälle von Leitungen nicht erkannt werden und in diesem Fall nur eine scheinbare, aber keine tatsächliche Redundanz besteht.

Bei hohen oder sehr hohen Verfügbarkeitsanforderungen sollte überlegt werden, in den relevanten Gebäuden die Sekundär- und Tertiärverkabelung redundant auszulegen.

Dazu wird die Sekundärverkabelung, also die Verbindung der Etagen, über mindestens zwei Steigeschächte geführt, die sich in verschiedenen Brandabschnitten des Gebäudes befinden sollten. Beispielsweise könnte die Sekundärverkabelung an den gegenüberliegenden Gebäudeseiten (z. B. Nord und Süd oder Ost und West) geführt werden.

Alle Räume, in denen Teilnehmer zu versorgen sind, werden jeweils an beide Sekundärverkabelungen angeschlossen. Die Hälfte der Anschlüsse in einem Raum wird dann mit einem Verteiler auf der einen Gebäudeseite verbunden, die andere Hälfte der Anschlüsse wird an einen Verteiler auf der anderen Seite des Gebäudes angeschlossen.

Damit ist es auch bei einem gravierenden Schaden möglich, den Betrieb auf den Etagen mindestens behelfsmäßig aufrecht zu erhalten, sofern der Schaden nicht beide Gebäudehälften betrifft.

INF.4.M13 Materielle Sicherung der IT-Verkabelung (IA)

In Räumen mit Publikumsverkehr oder in unübersichtlichen Bereichen eines Gebäudes kann es sinnvoll sein, Leitungen und Verteiler zusätzlich gegen unbefugte Zugriffe zu sichern. Dies kann auf verschiedene Weise erreicht werden:

- Verlegung der Leitungen oder Kabelkanäle unter Putz,
- Verlegung der Leitungen in Stahlpanzerrohr,
- Verlegung der Leitungen in mechanisch festen und abschließbaren Kanälen,
- Verschluss von Verteilern und
- elektrische Überwachung von Verteilern und Kanälen.

In jedem Fall ist die Zahl der Stellen, an denen das verlegte Kabel zugänglich ist, auf ein Mindestmaß zu reduzieren und die Länge der vor unberechtigten Zugriff zu schützenden Verbindungen möglichst klein zu halten.

Besonders die Absicherung zentraler Trassen und Kabel der elektrischen Versorgung und der IT-Verkabelung muss im gesamten Kabelweg an die Gefährdungslage angepasst werden. In Bereichen wie Tiefgaragen und auch in Fluren, die als Transportwege genutzt werden, muss ein angemessener Schutz gegen zufällige mechanische Beschädigung und gegebenenfalls auch gegen Sabotagehandlungen durch eine stabile Ummantelung der Trasse oder des Kabels getroffen werden.

Wenn Verteiler verschlossen werden, sind Regelungen nötig, die Zutrittsrechte zum Verteiler, Verteilung der Schlüssel und Zugriffsmodalitäten festlegen. Darin ist unter anderem vorzugeben, was vor Änderungen an Kabeln oder Verteilern und nach der Ausführung solcher Arbeiten zu tun ist. Es muss sichergestellt sein, dass Änderungen abgestimmt und genehmigt werden und dass die Dokumentation nachgeführt wird.

INF.4.M14 Verhinderung von Ausgleichsströmen auf Schirmungen (A)

In den Normen für die IT-Infrastruktur (DIN EN 50173, DIN EN 50174-2 "Installation von Kommunikationsverkabelung") sind sowohl geschirmte als auch ungeschirmte Datenverkabelungen sowie die Anforderungen an die Erdung und Schirmung dieser Anlagen beschrieben. Bei der Verwendung von geschirmten Datenleitungen wird in den Normen zwischen technisch genutzten Räumen (z. B. Serverräumen und Rechenzentren) und Räumen mit einer allgemeinen IT-Nutzung unterschieden. Für die technisch genutzten Räume ist das beidseitige Auflegen der Schirmung und eine enge Vermaschung der Systeme und Komponenten vorgegeben. Für die allgemeine Nutzung der IT-Infrastruktur, wie die Etagenverkabelung in Gebäuden, wird in den Normen das einseitige Auflegen der Schirmung vorgegeben. Das beidseitige Auflegen ist optional.

Ist der Netzbetrieb durch Ausgleichsströme bei Verwendung geschirmter Leitungen gestört, sollte zunächst die Ursache analysiert werden. Durch die immer höher frequent werdenden Übertragungsverfahren der IT werden die Anlagen empfindlicher gegen hochfrequente Störungen. Zudem werden sie unter Umständen auch selbst zu hochfrequenten Störern für umgebende Anlagen und Systeme. Wenn Betriebsstörungen festgestellt werden, muss abhängig von den Bedingungen vor Ort der richtige Lösungsweg erarbeitet werden. Da hierfür viel Fachwissen erforderlich ist, ist es im Allgemeinen empfehlenswert, eine Fachfirma zur Begutachtung, Analyse und Erarbeitung einer Lösung zu beauftragen.

Um beispielsweise Ausgleichsströme auf den Schirmungen von Datenleitungen in Gebäuden zu verhindern, gibt es verschiedene Möglichkeiten:

Ausgleichsströme können im TN-C-System vermieden werden, indem nur solche IT-Geräte über geschirmte Datenleitungen miteinander verbunden werden, die an einer gemeinsamen Elektro-Verteilung angeschlossen sind. Bei jeder Erweiterung des Datennetzes ist diese Bedingung zu prüfen und sicherzustellen.

Als Maßnahme gegen Ausgleichsströme im TN-C- bzw. TN-CS-System wird häufig das ausschließlich einseitige Auflegen der Schirmung von Datenleitungen vorgeschlagen. Hinsichtlich der Ausgleichsströme ist dieses Vorgehen auch tatsächlich wirksam. Aus anderen Gründen sollte dieses Mittel aber als absolute Ausnahme äußerst restriktiv angewandt werden:

- Geschirmte Leitungen, deren Schirmung nur einseitig aufgelegt ist, werden deutlich stärker durch Störstrahlungen von außen beeinflusst. Gleichzeitig strahlen sie selbst stärker ab als ungeschirmte symmetrische Leitungen. Es muss also bei einseitiger Schirmauflegung mit mehr Störungen der Datenübertragung (z. B. der Verfügbarkeit bzw. Integrität) gerechnet werden, als bei allen anderen Kabeln.Die stärkere Aussendung auswertbarer Abstrahlung derartiger Leitungen kommt als Risiko bei der Betrachtung der Vertraulichkeit von Informationen hinzu.
- Selbst wenn alle technischen Nachteile der einseitigen Schirmauflegung hingenommen werden, bleibt das Problem der durchgängigen Umsetzung. Es bedarf konsequenter Kontrolle bei allen Arbeiten am Datennetz, um sicher zu stellen, dass einseitig aufgelegte Schirmungen nicht doch irgendwann beidseitig aufgelegt werden. Solche Fehlauflegungen sind nachträglich nur mit sehr großem Aufwand zu finden.

Die aus Sicherheitssicht optimale Möglichkeit besteht darin, das Stromverteilnetz im gesamten Gebäude komplett als TN-S-System auszulegen. Dabei wird der PE- und der N-Leiter ab der Potentialausgleichsschiene (PAS) getrennt geführt. Einzelmaßnahmen an IT-Geräten sind dann in der Regel nicht mehr erforderlich.

Um die Wirksamkeit des TN-S-Systems dauerhaft zu gewährleisten, muss sicher gestellt werden, dass die Verbindung zwischen PE- und N-Leiter an der PAS (Nullung) die einzige im gesamten Netz ist. Es kann aber in der Praxis nicht ausgeschlossen werden, dass beim Anschluss neuer Geräte oder bei Schaltarbeiten im Netz versehentlich eine weitere Verbindung zwischen PE- und N-Leiter geschaffen wird. Daher sollten Änderungen im Datennetz mit der Haustechnik abgestimmt werden. Zudem sollte ein TN-S-System in regelmäßigen Abständen auf korrekte Nullung hin geprüft werden. Das kann bei den ohnehin durchzuführenden Prüfungen des Stromversorgungsnetzes und bei Verdachtsmomenten (beispielsweise länger andauernde unspezifische Störungen im Datennetz) erfolgen. Als Mindestmaßnahme ist ein TN-S-System in der Niederspannungshauptverteilung (NSHV) mit einer permanenten Differenzstromüberwachung über die drei Phasen und den N-Leiter sowie einer weiteren permanenten Stromüberwachung über den Zentralen Erdungspunkt (ZEP) auszustatten.

INF.4.M15 Nutzung von Schranksystemen (IA)

Zur Verbesserung der Betriebssicherheit von Servern, aktiven und passiven Netzkomponenten sollten diese Geräte in Schranksystemen eingebaut oder aufgestellt werden. Schranksysteme werden je nach Einsatzart häufig als 19-Zoll-Rack, Serverschrank oder auch Netzschrank bezeichnet.

Systemschränke sind nach DIN IEC 60297 "Bauweisen für elektronische Einrichtungen" und DIN 41494 "Bauweisen für elektronische Einrichtungen" genormt. Dadurch ist der Einbau beliebiger Geräte möglich, solange diese auch den genannten Normen entsprechen. Komponenten, die den oben genannten Normen entsprechen, sind häufig an dem Stichwort "19-Zoll-Einbau" erkennbar.

Schranksysteme gibt es in verschiedenen Innen- und Außenmaßen. Die größte Verbreitung haben Schränke mit einem Netto-Raumangebot von 42 Höheneinheiten (HE). Abhängig davon, ob die Schranksysteme in abgeschlossenen Verteilerräumen aufgestellt sind oder in allgemein zugänglichen Bereichen, müssen diese mit angepassten Türen, Seitenwänden und Schließungen ausgestattet werden, die dem jeweiligen Schutzbedarf entsprechen. Sockel unter den Schränken erleichtern die Einführung der erforderlichen Verkabelung. Ein weiterer Vorteil eines Sockels ist der zusätzliche Abstand zwischen dem Raumboden und den IT-Systemen. In diesem Fall führt ein möglicher Wassereintritt durch die erhöhte Positionierung der Geräte nicht automatisch zu Schäden an den IT-Systemen. Bei entsprechend abgesicherten Verteilerräumen kann auf Türen und Seitenwände nach Überprüfung der Umgebungsbedingungen verzichtet werden.

Der schrankinterne Aufbau sollte unbedingt wartungstechnischen Gesichtspunkten Rechnung tragen. Beispielsweise sollte ein schnellstmöglicher Austausch von Baugruppen in einem gepatchten Switchingsystem ohne nachteilige Beeinflussung benachbarter Systeme möglich sein. Dies setzt den vorausschauenden Einbau aller Komponenten und ein entsprechendes Management von Patchkabeln voraus. Von Vorteil ist es daher, wenn die elektrotechnische Verkabelung und die IT-Verkabelung stabil und geschützt geführt werden können. Viele Hersteller von Schranksystemen bieten Einbauteile an, mit denen die schrankinterne Kabelführung an spezifische Anforderungen und Wünsche des Anwenders angepasst werden kann. Überlängen von Patchkabeln sind zu vermeiden.

Bei der Planung der Schrankbelegung ist zu beachten, dass die Kapazität des Schrankes meistens durch die Wärmeabgabe der eingebauten Geräte und nicht durch die möglichen Einbaumaße beschränkt ist. Es kann zu Problemen der Wärmeabfuhr kommen, wenn die thermische Last der eingebauten Geräte zu groß ist.

Ähnliche Probleme können in Netzschränken entstehen, die sehr viele passive Komponenten (Patchfelder) enthalten und eine zu dichte Belegung mit Kabeln aufweisen.

In diesem Fall kann die Luftdurchströmung des Schrankes derart gestört werden, dass Bauteile oder aktive Komponenten Fehlfunktionen erleiden. Auch dieser Aspekt muss bei der Planung der Schrankbelegung berücksichtigt werden.

Bei nebeneinander aufgestellten Schränken muss zusätzlich auf die Luftführung der aktiven Komponenten in benachbarten Schränken geachtet werden. Es ist unbedingt zu vermeiden, dass die von Komponenten ausströmende Warmluft die Kaltluftzufuhr einer benachbarten Komponente beeinträchtigt. Mit der Schottung der Einzelschränke in der Schrankreihe kann dieser Problematik begegnet werden.

Damit die aktiven Komponenten innerhalb der vorgeschriebenen Temperaturbereiche betrieben werden können, sind die Schränke entsprechend auszustatten. Im einfachsten Fall reicht eine passive Kühlung des Schrankes bei ausreichend kühler Umgebungsluft im Raum aus. Diese kann bei geschlossenen Schränken durch Lüftersysteme im Schrank unterstützt werden. Sind die Wärmelasten zu groß, können aktive Kühlsysteme unterschiedlicher Bauart verwendet werden. Zu unterscheiden sind dabei Möglichkeiten der Raumkühlung einerseits und andererseits Kühlsysteme, welche an oder auf den Schränken angebracht werden können.

Um IT-Komponenten betreiben zu können, die eine sehr hohe Wärmeabgabe bei geringem Platzbedarf aufweisen, kann der Einsatz spezieller Schranksysteme mit eigenständigen Klimasystemen erwogen werden. Solche Schränke, die intern meist eine Flüssigkeitskühlung aufweisen, sollten nur nach einer sorgfältigen Bedarfs- und Risikoanalyse verwendet werden.

Jegliche Art der Klimatisierung erfordert eine genaue Planung unter Berücksichtigung aller beeinflussenden Parameter einschließlich einer entsprechenden Wirtschaftlichkeitsbetrachtung. Beim Einsatz von Schränken mit eigener Klimatisierung ist zudem darauf zu achten, dass Klimageräte an Seitenwänden oder Türen den Öffnungswinkel von Schranktüren verringern können und unter Umständen in Fluchtwege hineinragen. Das Raumlayout sollte möglichst so geplant werden, dass Klimatechnik an Schränken im Bedarfsfall nachgerüstet werden kann.

Es ist empfehlenswert, in der Institution einheitliche Vorgaben für die Ausstattung und Nutzung von Schranksystemen zu machen. Auch die Verkabelung der Schränke untereinander ist sorgfältig zu planen.

3 Weiterführende Informationen

3.1 Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "IT-Verkabelung" finden sich unter anderem in folgenden Veröffentlichungen:

[DIN4102] DIN 4102 Brandverhalten von Baustoffen und Bauteilen

[DIN41494] DIN 41494 Bauweisen für elektronische Einrichtungen

[DIN50173] DIN EN 50173 Informationstechnik - Anwendungsneutrale Kommunikationskabelanlagen

[DIN 50174] DIN EN 50174 Informationstechnik - Installation von Kommunikationsverkabelung

[DIN50310] DIN EN 50310:2017-02 Telekommunikationstechnische Potenialausgleichsanlage für Gebäude und andere Strukturen

Februar 2017

[DIN 50346] DIN EN 50346:2010-02 Informationstechnik - Installation von Kommunikationsverkabelung - Prüfen installierter Verkabelung

Februar 2010

[DIN60297] DIN IEC 60297 Bauweise für elektronische Einrichtungen

[IEC60364] DIN IEC60364- Einrichten von Niederspannungsanlagen

[IEEE8023] IEEE8023: IEEE 802.3 Standards in Lokalen Netzen

CSMA/CD, Ethernet Working Group, http://www.ieee802.org/3/, zuletzt abgerufen am 05.10.2018

[ISO11801] ISO/IEC 11801:2002-09

Informationstechnik - Anwendungsneutrale Standortverkabelung, International Organization for Standardization (Hrsg.), ISO/IEC JTC1, September 2002

[VDE100] DIN VDE 0100: Errichten von Niederspannungsanlagen

INF: Infrastruktur

Umsetzungshinweise zum Baustein INF.6 Datenträgerarchiv

1 Beschreibung

1.1 Einleitung

Datenträgerarchive sind abgeschlossene Räumlichkeiten innerhalb einer Institution, in denen Datenträger jeder Art gelagert werden. Hierzu gehören neben Datenträgern, auf denen digitale Informationen abgespeichert sind, grundsätzlich auch Papierdokumente, Filme oder sonstige Medien. Im Rahmen des IT-Grundschutzes werden an die Archivräume hinsichtlich des Brandschutzes keine erhöhten Anforderungen gestellt. Zusätzliche Anforderungen an den Brandschutz können auch durch die Behältnisse, in denen die Datenträger aufbewahrt werden, erfüllt werden.

Bei zentralen Datenträgerarchiven und Datensicherungsarchiven wird generell empfohlen. Datensicherungsschränke zu nutzen, um neben den Brandschutz, den Schutz gegen unbefugten Zugriff und die Durchsetzung von Zugangsberechtigungen zu unterstützen.

1.2 Lebenszyklus

Planung und Konzeption

Die Grundstruktur des Datenträgerarchivs und damit die wesentlichen Randbedingungen, um ihn zu nutzen, werden bei der Planung und Konzeption festgelegt. Hier bestehen naturgemäß bei der Einrichtung eines neuen Gebäudes größere Freiheiten. Wenn ein Datenträgerarchiv in einem schon existierenden Gebäude installiert werden soll, sind die verbleibenden Möglichkeiten der Strukturierung bei der Nutzung eines Gebäudes meist nur noch gering, vor allem bei angemieteten Gebäuden.

Mit der Auswahl des Raumes, in dem das Archiv untergebracht wird, stehen dessen Schutzeigenschaften schon zu einem großen Teil fest, und nachträgliche Korrekturen wie die Entfernung wasserführender Leitungen sind oft nur noch mit erheblichem Aufwand zu realisieren (siehe INF.6.M6 *Vermeidung von wasserführenden Leitungen*). Notwendige technische Installationen, wie eine Klimatisierung oder der Einsatz einer Gefahrenmeldeanlage, sollten daher nach Möglichkeit schon bei der Planung oder Auswahl des Datenträgerarchivs vorgesehen werden (siehe INF.6.M7 *Einhaltung von klimatischen Bedingungen* und INF.6.M9 *Gefahrenmeldeanlage*).

Umsetzung

Vor der Inbetriebnahme des Datenträgerarchivs sind organisatorische Regelungen festzulegen, die einen geordneten und sicheren Betrieb unterstützen (siehe INF.6. M4 *Geschlossene Fenster und abgeschlossene Türen* und INF.6.M8 *Sichere Türen und Fenster*).

Betrieb

Im laufenden Betrieb ist durch entsprechende Kontrolle zu gewährleisten, dass die vorgesehenen Regelungen in der Praxis tatsächlich angewendet werden. Hierzu gehört vor allem, dass nur die Personen Zutritt haben, die dazu berechtigt sind, und dass das Archiv abgeschlossen ist, solange sich dort niemand aufhält (siehe INF.6.M2 *Zutrittsregelung und -kontrolle*).

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Datenträgerarchiv" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

INF.6.M1 Handfeuerlöscher [Brandschutzbeauftragter, Haustechnik]

Die meisten Brände entstehen aus kleinen, anfangs noch gut beherrschbaren Brandherden. Der Sofortbekämpfung von Bränden kommt also ein sehr hoher Stellenwert zu.

Diese Sofortbekämpfung ist nur möglich, wenn Handfeuerlöscher in der jeweils geeigneten Brandklasse (siehe [DIN3]) in ausreichender Zahl und Größe (Beratung durch die örtliche Feuerwehr) im Gebäude zur Verfügung stehen. Zudem ist auf dem Instandhaltungsnachweis jedes Löschers regelmäßig zu prüfen, dass die Löscher auch regelmäßig inspiziert und gewartet werden, damit sie im Ernstfall funktionieren.

Wasserlöscher mit Eignung für Brandklasse A bis 1000 V sind durchaus für elektrisch betriebene Geräte geeignet.

Für elektronisch gesteuerte Geräte, z.B. Rechner, sollten vorzugsweise Kohlendioxyd-Löscher (Brandklasse B) zur Verfügung stehen. Die Löschwirkung wird erreicht, indem Sauerstoff verdrängt wird, deshalb ist bei Anwendung in engen, schlecht belüfteten Räumen Vorsicht geboten.

Pulverlöscher, die die Brandklassen A (feste Stoffe), B (brennbare Flüssigkeiten) und C (Gase) abdecken, sollten in Bereichen mit elektrischen und elektronischen Geräten nicht eingesetzt werden, weil die Löschschäden in der Regel unverhältnismäßig hoch sind. Es wird daher dringend empfohlen, im direkten Umfeld von Datenträgerarchiven keine Pulverlöscher, sondern ausschließlich geeignete Gaslöscher bereit zu halten. Nur so kann verhindert werden, dass in der Aufregung eines Brandes fälschlicherweise ein Pulverlöscher verwendet wird.

Die Feuerlöscher müssen regelmäßig geprüft und gewartet werden. Die Feuerlöscher müssen so angebracht werden, dass sie im Brandfall leicht erreichbar sind. Die Beschäftigten sollten sich den Standort des nächsten Feuerlöschers einprägen. Die Standorte von Löschern und Hydranten sind durch vorgeschriebene Schilder kenntlich zu machen. Tragbare Feuerlöscher sind zugelassen bis zu einem Gesamtgewicht von 20 kg. Mit den überwiegend eingesetzten Geräten von 6 und 12 kg lassen sich größere Brandherde löschen als von Laien üblicherweise angenommen wird, dies ist allerdings nur bei konsequenter Vorgehensweise gegeben. Bis zur vollständigen Entladung des Löschmittels vergehen nur wenige Sekunden. Daher sind bei entsprechenden Brandschutzübungen die Mitarbeiter in die Benutzung der Handfeuerlöscher einzuweisen und die Bedienung der Löscher auch zu üben.

INF.6.M2 Zutrittsregelung und -kontrolle [Leiter Haustechnik, Mitarbeiter, Planer]

Der Zutritt zum schutzbedürftigen Datenträgerarchiv ist zu regeln und zu kontrollieren. Die Maßnahmen reichen dabei von einer einfachen Schlüsselvergabe bis hin zu aufwendigen Identifizierungssystemen mit Personenvereinzelung, wobei auch die Nutzung eines mechanischen Schlüssels nebst Schloss eine Zutrittsregelung darstellt. Für eine Zutrittsregelung und – kontrolle ist es erforderlich, dass der von der Regelung betroffene Bereich eindeutig bestimmt wird. Die Anzahl der zutrittsberechtigten Personen muss sich auf ein Mindestmaß beschränken. Diese Personen müssen gegenseitig ihre Berechtigungen kennen, um Unbefugte als solche erkennen zu können. Die erteilten Zutrittsberechtigungen müssen dokumentiert werden. Die Vergabe von Rechten allein reicht nicht aus, wenn deren Einhaltung bzw. Überschreitung nicht kontrolliert wird. Die Ausgestaltung von Kontrollmechanismen muss nach dem Grundsatz erfolgen, dass einfache und praktikable Lösungen oft ebenso effizient sind, wie aufwendige Technik. Beispiele hierfür ist die Sensibilisierung von Berechtigten, Bekanntgabe von Berechtigungsänderungen, sichtbares Tragen von Hausausweisen ergänzt durch die Vergabe von Besucherausweisen, Begleitung von Besuchern, Verhaltensregelungen bei erkannter Berechtigungsüberschreitung und Einschränkungen des ungehinderten Zutritts für nicht Zutrittsberechtigte wie Tür mit Blindknauf, Schloss mit Schlüssel für Berechtigte und Klingel für Besucher.

INF.6.M3 Schutz vor Staub und anderer Verschmutzung [Mitarbeiter]

Generell muss sichergestellt werden, dass die Datenträger im Datenträgerarchiv ausreichend vor Staub und Verschmutzung geschützt sind. Hierfür sollten die Datenträger so verpackt werden, dass auch über eine lange Lagerzeit keine Schäden durch Staub und Verschmutzung erleiden.

In den meisten Räumlichkeiten von Unternehmen und Behörden ist Rauchen generell verboten, meistens sogar aufgrund gesetzlicher Vorgaben. So verpflichtet in Deutschland die Arbeitsstättenverordnung die meisten Institutionen, den Nichtraucherschutz am Arbeitsplatz zu gewährleisten. Auch in Gebäuden, in denen kein umfassendes Rauchverbot herrscht, muss sichergestellt werden, dass in Räumen mit IT oder Datenträgern (Serverraum, Datenträgerarchiv, aber auch Belegarchiv), in denen Brände oder Verschmutzungen, wie Beispielsweise Staub, zu hohen Schäden führen können, ein Rauchverbot erlassen wird. Dieses Rauchverbot dient gleicherweise dem vorbeugenden Brandschutz wie der Betriebssicherheit von IT mit mechanischen Funktionseinheiten.

Dabei muss sichergestellt werden, dass nicht als Folge eines Rauchverbots im Gebäude der Zutrittsschutz geschwächt wird. Es ist häufig zu beobachten, dass Außentüren in schwer einsehbaren Bereichen ständig offen stehen, weil der Nahbereich der Tür die Raucherzone bildet und die Tür aus Bequemlichkeit während der Arbeitszeiten nie geschlossen wird.

INF.6.M4 Geschlossene Fenster und abgeschlossene Türen [Haustechnik, Mitarbeiter]

Offene Fenster und Türen bieten Einbrechern ideale Einstiegsmöglichkeiten, die auch während der Betriebszeiten einer Institution genutzt werden können. Fenster und Türen müssen in Zeiten, in denen das Datenträgerarchiv nicht besetzt ist geschlossen bzw. Türen verschlossen werden. Dadurch wird verhindert, dass Unbefugte Zugriff auf darin befindliche Datenträger erlangen. Das Verschließen des Datenträgerarchivs ist insbesondere dann wichtig, wenn sich dieser im Bereich mit Publikumsverkehr befinden oder der Zutritt nicht durch andere Maßnahmen kontrolliert wird.

Brand- und Rauchschutztüren bieten ebenfalls nur im verschlossenen Zustand den gewünschten Schutz und dürfen deshalb keinesfalls durch Keile oder andere Vorrichtungen dauerhaft offen gehalten werden. Es ist sinnvoll, wenn Pförtner oder Mitarbeiter der Haustechnik regelmäßig überprüfen, ob die Fenster und Türen nach Verlassen der Räume verschlossen wurden.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Datenträgerarchiv".

INF.6.M5 Verwendung von Schutzschränken

Bei zentralen Datenträgerarchiven und Datensicherungsarchiven ist die Nutzung von Schutzschränken empfehlenswert, um den Brandschutz, den Schutz gegen unbefugten Zugriff und die Durchsetzung von Zugangsberechtigungen zu unterstützen.

INF.6.M6 Vermeidung von wasserführenden Leitungen [Haustechnik]

In Datenträgerarchiven, sollten wasserführende Leitungen aller Art vermieden werden. Die einzigen wasserführenden Leitungen sollten, wenn unbedingt erforderlich, Kühlwasserleitungen, Löschwasserleitungen und Heizungsrohre sein. Zuleitungen zu Heizkörpern sollten mit Absperrventilen, möglichst außerhalb des Datenträgerarchivs versehen werden. Außerhalb der Heizperiode sind diese Ventile zu schließen.

Sind wasserführende Leitungen unvermeidbar, müssen Vorkehrungen getroffen werden, einen Wasseraustritt möglichst frühzeitig zu erkennen bzw. die negativen Auswirkungen zu minimieren. Als Minimalschutz kann eine Wasserauffangwanne oder -rinne unter der Leitung angebracht werden, deren Ablauf außerhalb des Raumes führt. Günstig ist es, dazu den Flur zu nutzen, da so ein eventueller Leitungsschaden schnell entdeckt werden kann. Zur frühzeitigen Erkennung von Wassereinbrüchen oder undichten Leitungen hat es sich bewährt, Decken hell zu streichen. Mindestens durch Sichtprüfungen müssen die vorhandenen Wasserleitungen regelmäßig auf ihre Dichtigkeit hin überprüft werden.

Es ist zu erwägen, wasserführende Leitung durch Wassermelder zu überwachen. Dafür können besondere Meldekabel unterhalb von Leitungen verlegt werden. Werden diese an eine Wassermeldeanlage angeschlossen, kann darüber schnell und recht genau der Wasseraustritt lokalisiert werden. Eine solche Anlage muss auf eine ständig besetzte Stelle aufgeschaltet werden, um in Verbindung mit entsprechenden Reaktionsplänen und einer aktuellen Dokumentation ein schnelles Eingreifen möglich zu machen. Optional können Wassermelder mit automatisch arbeitenden Magnetventilen eingebaut werden. Diese Magnetventile sind außerhalb des Raumes bzw. Bereiches einzubauen. Damit die Ventile auch bei Stromausfall ihre Schutzfunktion erfüllen, müssen sie im stromlosen Zustand geschlossen sein.

Alle Mitarbeiter im Bereich der IT und der Haustechnik sollten darüber informiert sein, dass im Datenträgerarchiv wasserführende Leitungen problematisch sind und was zu beachten ist. Es sollten Reaktionspläne vorhanden sein, in denen beschrieben ist, welche Maßnahmen bei Wasserleckagen zu ergreifen sind.

INF.6.M7 Einhaltung von klimatischen Bedingungen [Haustechnik]

Um Datenträger zu lagern bzw. IT-Geräte dauerhaft zuverlässig zu betreiben, muss sichergestellt werden, dass die Umgebungsbedingungen innerhalb der von den Herstellern genannten Grenzen gehalten werden. Der in diesem Zusammenhang stets genutzte Begriff Klimatisierung umfasst die folgenden vier Bereiche der Luftkonditionierung:

- Lufttemperatur
- Luftfeuchtigkeit
- Frischluftanteil
- Schwebstoffbelastung

Neben der Temperatur muss oft auch die Luftfeuchtigkeit innerhalb bestimmter Grenzen gehalten werden, um elektrostatische Aufladungen (bei zu geringer Luftfeuchtigkeit) oder Oxidation und Schimmelbildung (bei zu hoher Luftfeuchtigkeit) zu vermeiden.

Der Schwebstoffgehalt der Luft wird meist schon durch die normalen Filter in Klimaanlagen hinreichend niedrig gehalten. Nur bei besonders stark belasteter Umgebungsluft oder spezieller Hardware ist hier eine weitergehende Filterung erforderlich. Um den erforderlichen Luftdurchsatz zu gewährleisten, müssen die Filter der Klimaanlage regelmäßig kontrolliert und rechtzeitig gewechselt werden.

Die vierte Komponente einer Klimatisierung, die Frischluftbeimischung, ist für den eigentlichen IT-Betrieb und der Archivierung belanglos. In dem Umfang jedoch, in dem die klimatisierten Flächen als Arbeitsplatz ausgewiesen sind, muss entsprechend der einschlägigen Arbeitsstättenverordnungen eine Frischluftbeimischung erfolgen.

INF.6.M8 Sichere Türen und Fenster [Haustechnik]

Wenn Türen und Fenster einen Übergang zwischen Sicherheitszonen bilden, sollten sie angemessenen Schutz bieten. Eine Außentür muss z. B. vor Einbrüchen schützen, ebenso müssen die erreichbaren Fenster gesichert werden. Im Innenbereich müssen Türen, die die Grenze eines Brandabschnitts bilden, selbst Brandschutzqualität haben, zudem können sie oder auch andere Innentüren eine zweite Linie des Einbruchschutzes bilden.

Sicherheitstüren und -fenster sind in Normen klassifiziert. Aus dem Schutzziel des zu sichernden Bereichs und dem Schutzbedarf der Institution lässt sich eine Auswahl der angemessenen Ausführung von Türen und Fenstern treffen:

- In der Norm DIN EN 1627:2011-09 "Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchhemmung - Anforderungen und Klassifizierung" sind die Bauelemente in Widerstandsklassen (RC, engl. Resistance Class) eingeordnet worden (siehe [DIN1627]). Türen gemäß der Klassifizierungen RC1 bis RC4 bieten aufgrund ihrer Stabilität einen höheren Schutz gegen Einbruch (z. B. bei Serverräumen, Räumen mit technische Infrastruktur sowie bei Keller- und Lieferanteneingängen). Die Widerstandsklassen RC5 und RC6 sind in der Regel nur bei sehr speziellen Erfordernissen angemessen und spielen daher beim IT-Grundschutz keine Rolle.
- Selbstschließende feuerhemmende und gegebenenfalls rauchdichte Türen (siehe [DIN4102]) verzögern die Ausbreitung eines Brandes und in der RS-Ausführung auch von Rauch.
- Sie schützen in der Ausführung als selbstschließende Rauchschutztür (siehe [DIN18095-2] die Ausbreitung von Brandrauch. Brandrauch ist so feinkörnig, dass er problemlos durch Druckausgleichs- und Lüftungsöffnungen von Festplatten hindurch kommt. Für die geringen Flughöhen von Festplattenleseköpfen ist er aber immer noch viel zu groß und verursacht dort enorme Schäden.

Es können auch mehrere Schutzeigenschaften in einer Tür kombiniert werden, es gibt beispielsweise rauchdichte Brandschutztüren, die zudem Schutz gegen Einbruch bieten.

Die Sicherungsmaßnahmen aller raumumschließenden Bauelemente müssen gleichwertig sein:

- Bei Verwendung einbruchhemmender Türen ist im Fassadenbereich die Verwendung einbruchhemmender Fenster oder Fassadenelemente (siehe [DIN 1627) zu erwägen.
- Weiterhin ist es z. B. nicht zweckmäßig, eine einbruchhemmende Tür der höchsten Widerstandsklasse in eine Gipskartonwand einzubauen.
- Beim Einbau einer feuerhemmenden oder rauchdichten Tür ist darauf zu achten, dass auch die umgebende Wand gleichwertig feuerhemmend und rauchdicht ist und nicht durch offene Oberlichter oder ungeschottete Kabeldurchführungen ein Bypass besteht.

Der Einsatz von Sicherheitstüren ist hinsichtlich des Brandschutzes über den von der Bauaufsicht und der Feuerwehr vorgeschriebenen Bereich hinaus besonders bei schutzbedürftigen Räumen wie dem Datenträgerarchiv sinnvoll. Bei hochschutzbedürftigen Räumen ist ein ausgewogenes Schutzkonzept zu erstellen, welches den Einbau von Sicherheitstüren und die Gefahrenmeldung und Alarmierung zur Prüfung und Intervention berücksichtigt. Denn hat ein potentieller Angreifer ein ganzes Wochenende Zeit für einen Einbruchsversuch, wird ihn auch eine hochwertige einbruchhemmende Tür nicht von seinem Ziel abhalten, Daten oder Einrichtung zu entwenden oder zu zerstören.

Für die Ausstattung von Rechenzentren sollte für die Türen inklusive deren Einbausituation die Widerstandsklasse RC3 (siehe [DIN 1627]) als Mindestwert angesetzt werden. Lediglich wenn für die Sicherheit ganz besonders günstige Bedingung vorliegen, insbesondere falls die Interventionszeit hilfeleistender Kräfte kurz ist (maximal 2 Minuten), kann in Ausnahmefällen eine RC 2-Tür ausreichen. Liegt die Interventionszeit hilfeleistender Kräfte hingegen bei 5 Minuten und höher, ist sogar eine RC 3-Tür als unzureichend anzusehen und es empfiehlt sich der Einbau von RC 4-Türen. Sinngemäß gelten die gleiche Überlegungen natürlich auch für alle anderen, die RZ-Hülle bildenden Bauelemente.

Hinweis: Ziel eines Einbruches könnte es auch sein, Daten oder IT-Systeme zu manipulieren. Daher sollten zentrale IT-Systeme nach Einbrüchen auf ihre Integrität überprüft werden.

Es ist dafür zu sorgen, dass Brand- und Rauchschutztüren auch tatsächlich geschlossen und nicht (unzulässigerweise) z. B. durch Keile offen gehalten werden. Alternativ können Türen mit einem automatischen Schließmechanismus, der im Alarmfall aktiviert wird, eingesetzt werden.

Außerdem ist regelmäßig zu prüfen, dass die Sicherheitstüren und -fenster funktionstüchtig sind. Sie müssen in einem ordentlichen mechanischen Zustand sein, sicher öffnen und schließen und überwachende Installationen wie Schließkontakte müssen funktionieren.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

INF.6.M9 Gefahrenmeldeanlage [Haustechnik] (CIA)

Eine Gefahrenmeldeanlage (GMA) besteht aus einer Vielzahl lokaler Melder, die mit einer Zentrale kommunizieren, über die auch der Alarm ausgelöst wird. Ist eine Gefahrenmeldeanlage für Einbruch, Brand, Wasser oder auch Gas vorhanden und lässt sich diese mit vertretbarem Aufwand entsprechend erweitern, sollten zumindest die Kernbereiche der IT (Serverräume, Datenträgerarchive, Räume für technische Infrastruktur u. ä.) in die Überwachung durch diese Anlage mit eingebunden werden. So lassen sich Gefährdungen wie Feuer, Einbruch, Diebstahl frühzeitig erkennen und Gegenmaßnahmen einleiten. Um dies zu gewährleisten, ist die Weiterleitung der Meldungen an eine ständig besetzte Stelle (Pförtner, Wach- und Sicherheitsdienst, Feuerwehr, etc.) unumgänglich. Dabei muss sichergestellt sein, dass diese Stelle auch in der Lage ist, technisch und personell auf den Alarm zu reagieren. Hierbei sind die Aufschaltrichtlinien der jeweiligen Institutionen und die Anforderungen der "Notruf- und Serviceleitstellen" (siehe [DIN50518])zu beachten.

Es sollte ein Konzept für die Gefahrenerkennung, Weiterleitung und Alarmierung für die verschiedenen Gebäudebereiche erstellt werden. Dieses muss an Veränderungen bei der Nutzung angepasst werden. Eine Gefahrenmeldeanlage ist ein komplexes Gesamtsystem, das dem Gebäude und dem Risiko entsprechend geplant und installiert werden muss. Planung, Installation und Wartung einer Gefahrenmeldeanlage sollte daher durch Experten durchgeführt werden. Falls diese nicht im eigenen Haus vorhanden sind, sollte auf externe Unterstützung zurückgegriffen werden. So gibt es beispielsweise eine Vielzahl unterschiedlicher Meldesysteme, die entsprechend der Sicherheitsanforderungen und der Umgebung ausgewählt werden müssen. Zur Einbruchserkennung können z. B. Bewegungsmelder, Glasbruchsensoren, Öffnungskontakte, Videokameras u. a. eingesetzt werden.

Die Melder können untereinander auf verschiedene Arten vernetzt werden. In Abhängigkeit von Art und Größe der zu schützenden Bereiche und der geltenden Richtlinien müssen passende Systeme ausgewählt und installiert werden. Bei der Planung oder Erweiterung einer GMA sollte darauf geachtet werden, dass die Trassen für die Vernetzung ausreichend dimensioniert sein müssen und möglichst wenig Änderungen an der Trassenbelegung vorgenommen werden sollten.

Um die Schutzwirkung der GMA aufrechtzuerhalten, ist eine regelmäßige Wartung und Funktionsprüfung (siehe [DIN0833-1]) vorzusehen.

Ist keine GMA vorhanden oder lässt sich die vorhandene nicht nutzen, kommen als Minimallösung lokale Gefahrenmelder in Betracht. Diese arbeiten völlig selbständig, ohne Anschluss an eine Zentrale. Die Alarmierung erfolgt vor Ort oder mittels einer einfachen Zweidrahtleitung (eventuell Telefonleitung) an anderer Stelle.

Es gibt Räume wie Serverraum, Datenträgerarchiv, die einen erhöhten Schutzbedarf haben. Wenn keine zentrale GMA vorhanden ist, sind dort lokale Gefahrenmelder zu installieren. Bei der Verwendung lokaler Gefahrenmelder für die Früherkennung muss dafür gesorgt werden, dass ein Alarm auch außerhalb der betroffenen Räume wahrgenommen wird. Die Meldung kann über verschiedene Wege erfolgen und sollte an eine Stelle weitergeleitet werden, die rund um die Uhr besetzt ist. Beispielsweise gibt es Lösungen, die über die TK-Anlage oder Funk Mitarbeiter über ein Mobiltelefon alarmieren können.

Vor der Planung einer GMA muss ein konsistentes Schutzkonzept für das betrachtete Gebäude erarbeitet werden. Bei der Planung von Gefahrenmeldeanlagen für private bzw. gewerbliche Objekte sollte mit dem Sachversicherer geklärt werden, ob eine Minderung der Versicherungsprämie, insbesondere für die Einbruch-Diebstahlversicherung in Frage kommt.

3 Weiterführende Informationen

3.1 Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter entgegen.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Datenträgerarchiv" finden sich unter anderem in folgenden Veröffentlichungen:

[DIN0833-2] DIN VDE 0833-2:2017-10: Gefahrenmeldeanlagen für Brand, Einbruch und Überfall

Teil 2: Festlegungen für Brandmeldeanlagen, Oktober 2017

[DIN1627] DIN EN 1627:2011-09 Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchshemmung - Anforderung und Klassifizierung

September 201

[DIN18095-2] DIN 18095-2:1991-03: Türen, Rauchschutztüren

Begriffe und Anforderungen

[DIN3] DIN EN 3 Tragbare Feuerlöscher

[DIN4102] DIN 4102 Brandverhalten von Baustoffen und Bauteilen

[VdS3138-1] VdS 3138-1:2013-13: Notruf- und Serviceleitstellen

INF: Infrastruktur

Umsetzungshinweise zum Baustein INF.7 Büroarbeitsplatz

1 Beschreibung

1.1 Einleitung

Ein Büroarbeitsplatz ist der Bereich innerhalb der Institution, in dem sich ein oder mehrere Mitarbeiter aufhalten, um dort ihre Aufgaben zu erledigen. Die Aufgaben können aus den verschiedensten Tätigkeiten bestehen, die auch teilweise oder ganz IT-unterstützt sein können: Erstellung von Schriftstücken, Bearbeitung von Karteien und Listen, Durchführung von Besprechungen und Telefonaten, Lesen von Akten und sonstigen Unterlagen. Da sich ein Büroarbeitsplatz innerhalb der Institution befindet, können grundlegende infrastrukturelle Sicherheitsvorkehrungen wie Zugangskontrolle zum Gebäude oder Brandschutz vorausgesetzt werden.

1.2 Lebenszyklus

Für Büroarbeitsplätze sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung bis hin zu ihrer Nutzung. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Planung und Konzeption

Büroarbeitsplätze müssen geeignet ausgewählt und genutzt werden (siehe INF.7.M1 *Geeignete Auswahl und Nutzung eines Büroarbeitsplatzes).* Auch sollte der Arbeitsplatz ergonomisch eingerichtet sein, da Mitarbeiter so effizienter arbeiten und Sicherheitsanforderungen besser umsetzen können (siehe INF.7.M5 *Ergonomischer Arbeitsplatz).* Auf eine sogenannte fliegende Verkabelung sollte verzichtet werden (siehe INF.7.M3 *Fliegende Verkabelung).*

Beschaffung

Für Geräte und deren Peripherie an Arbeitsplätzen, bei denen die Mitarbeiter den Zutritt nicht selber steuern können, also Bereiche mit Publikumsverkehr oder Großraumbüros, können Diebstahlsicherungen vorgesehen werden, mit denen sich z. B. Laptops schützen lassen. Andernfalls ist die Gefahr relativ groß, dass solche Geräte in einem unbewachten Augenblick verschwinden (siehe INF.7.M8 *Einsatz von Diebstahlsicherungen).*

Umsetzung

Auch für Büroarbeitsplätze sollte festgelegt werden, wer unter welchen Bedingungen Zutritt erhalten darf (siehe INF.7.M4 *Zutrittsregelung und -kontrolle*). Insbesondere ist zu entscheiden, für welche Bereiche Publikumsverkehr vorgesehen wird und welche nur den Mitarbeitern der Institution offen stehen.

Betrieb

Die bearbeiteten Informationen müssen am Büroarbeitsplatz sorgfältig behandelt werden. Dazu gehört, dass die vom Arbeitgeber vorgesehenen Regelungen über die Arbeitsumgebung eingehalten und Arbeitsmaterialien sicher aufbewahrt werden (siehe INF.7.M6 *Aufgeräumter Arbeitsplatz* und INF.7.M7 *Geeignete Aufbewahrung dienstlicher Unterlagen*).

Es ist auch festzulegen, ob die Mitarbeiter ihre Büros grundsätzlich verschließen müssen, wenn sie abwesend sind (siehe INF.7.M2 *Geschlossene Fenster und abgeschlossene Türen*). Je nach den baulichen Gegebenheiten muss auch dafür gesorgt werden, dass kein Zutritt über nach außen gehende Türen (z.B. Balkone, Terrassen) bzw. durch ungesicherte Fenster möglich ist.

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Büroarbeitsplatz" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

INF.7.M1 Geeignete Auswahl und Nutzung eines Büroraumes [Mitarbeiter, Vorgesetzte]

Lage und Ausstattung eines Büroarbeitsplatzes müssen für die dort durchgeführten Tätigkeit geeignet sein. Auch müssen Büroräume in einem Gebäude so verteilt sein, dass dabei die grundsätzlichen Bedingungen und Arbeitsabläufe und der Schutzbedarf der Tätigkeit aufeinander abgestimmt sind.

Büroarbeitsplätze mit Publikumsverkehr müssen so platziert sein, dass sie von den Kunden und Besuchern erreicht werden können, ohne dass diese sicherheitsrelevanten Bereiche durchschreiten müssen. Auf der anderen Seite müssen Büroarbeitsplätze, in denen schutzbedürftigen Dokumente bearbeitet und aufbewahrt werden, sich vorzugsweise dort befinden, wo Besucher, aber auch Mitarbeiter anderer Abteilungen keinen freien Zugang haben.

INF.7.M2 Geschlossene Fenster und abgeschlossene Türen [Mitarbeiter]

Offene Fenster und Türen bieten Angreifern ideale Einstiegsmöglichkeiten, die auch während der Betriebszeiten einer Institution genutzt werden können. Fenster und nach außen gehende Türen (Balkone, Terrassen) müssen in Zeiten, in denen ein Büroarbeitsplatz nicht besetzt ist, verschlossen werden.

Es wird empfohlen, die Türen nicht besetzter Räume zu verschließen. Dadurch wird verhindert, dass Unbefugte auf darin befindliche Unterlagen und -Einrichtungen zugreifen können. Es ist besonders dann wichtig, einzelne Büros abzuschließen, wenn sich diese in Bereichen mit Publikumsverkehr befinden oder der Zutritt nicht durch andere Maßnahmen kontrolliert wird. Wenn Büroarbeitsplätze, in denen keine schutzbedürftigen Dokumente bearbeitet werden und in denen es keinen Publikumsverkehr gibt, nur kurzzeitig verlassen werden (z. B. um etwas zu kopieren), müssen diese nicht abgeschlossen werden. Von außen erreichbare Fenster und nach außen gehende Türen müssen jedoch trotzdem verschlossen werden.

In manchen Fällen können Büros nicht abgeschlossen werden, z. B. in Großraumbüros. Dann sollte der Mitarbeiter seine vertraulichen Unterlagen in einem Schrank oder im Schreibtisch wegschließen, bevor er seinen Platz verlässt (Clean-Desk-Politik).

Keine Ausnahme darf bei Brand- und Rauchschutztüren zugelassen werden. Solche Türen schützen nur, wenn sie geschlossenen sind und dürfen deshalb keinesfalls durch Keile oder andere Vorrichtungen dauerhaft offen gehalten werden.

Diese Regelungen sollten in einer geeigneten Anweisung festgehalten werden. Alle Mitarbeiter sind verpflichtet, diese Anweisung umzusetzen. Es ist sinnvoll, wenn Pförtner oder Mitarbeiter der Haustechnik regelmäßig überprüfen, ob die Fenster und Außentüren geschlossen und Bürotüren verschlossen wurden.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Büroarbeitsplatz".

INF.7.M3 Fliegende Verkabelung

Kabel können schnell zu Stolperfallen werden. Sie sollten daher nicht quer durch den Büroarbeitsplatz verlegt werden, sondern Steckdosen und Stromversorgung sollten dort zu finden sein, wo sie benötigt werden. Sollten die Kabel dennoch durch den Raum verlegt werden müssen, sollten sie z. B. mit einem Kabelteppich abgedeckt werden.

INF.7.M4 Zutrittsregelungen und -kontrolle

Der Zutritt zu schutzbedürftigen Büroarbeitsplätzen ist zu regeln und zu kontrollieren. Die möglichen Maßnahmen reichen dabei von einer einfachen Schlüsselvergabe bis hin zu aufwändigen Identifizierungssystemen mit Personenvereinzelung. Für eine Zutrittsregelung und -kontrolle ist es erforderlich, dass der von der Regelung betroffene Bereich eindeutig bestimmt wird. Nur die Personen, für die es unbedingt nötig ist, sollten Zutrittsberechtigungen für die Büroräume erhalten. Dies gilt besonders für Räume, in denen schutzbedürftige Informationen bearbeitet oder aufbewahrt werden. Die zutrittsberechtigten Mitarbeiter sollten gegenseitig ihre Berechtigungen kennen, um Unbefugte als solche erkennen zu können.

Die erteilten Zutrittsberechtigungen sollten dokumentiert werden. Auch sollten die vergebenen Berechtigungen regelmäßig kontrolliert und aktualisiert werden.

Insgesamt sollten die Kontrollmechanismen so einfach, praktikabel und effizient wie möglich sein. Oft ist es gar nicht notwendig, dafür aufwändige Technik einzuführen. Einfache und effiziente Kontrollmechanismen sind z. B.

- Berechtigte sensibilisieren,
- Berechtigungsänderungen bekanntgegeben,
- alle Mitarbeiter zu verpflichten, Hausausweise sichtbar zu tragen, für Besucher sollten leicht zu identifizierende Besucherausweise erhalten,
- Besucher begleiten,
- genaue Verhaltensregelungen bei erkannter Berechtigungsüberschreitung festzulegen und
- den ungehinderten Zutritt für nicht Zutrittsberechtigte einzuschränken(z. B. Tür mit Blindknauf, Schloss mit Schlüssel nur für Berechtigte und Klingel für Besucher).

INF.7.M5 Ergonomischer Arbeitsplatz [Leiter Haustechnik]

Schlecht ausgestattete Arbeitsplätze belasten die Mitarbeiter und können zu gesundheitlichen Beschwerden führen. Durch einen ergonomischen Arbeitsplatz lassen sich die Belastungen jedoch verringern und die Arbeit wird zudem effizienter. So bringt es nicht nur gesundheitliche Vorteile für den Arbeitnehmer, sondern hat auch ein wirtschaftlicheres Arbeiten und besser umgesetzte Sicherheitsmaßnahmen zur Folge. Daher sollte jeder Arbeitsplatz ergonomisch gestaltet werden. Bei Computerarbeitsplätzen sollten beispielsweise Stuhl, Tisch, Bildschirm und Tastatur individuell einstellbar sein, um eine möglichst fehlerfreie Bedienung der IT zu ermöglichen und zu fördern. Das beinhaltet unter anderem, dass Rückenlehne, Sitzhöhe und Sitzfläche des Stuhls verstellbar sein sollten, aber auch, dass die Arbeitsmittel so angeordnet werden können, dass für die jeweilige Arbeitsaufgabe eine möglichst geringe Belastung entsteht.

Ein entsprechend ausgestatteter Büroarbeitsplatz erleichtert es auch, Sicherheitsmaßnahmen einzuhalten. Gibt es verschließbare Schreibtische oder Schränke, so können Datenträger, Dokumentationen, Unterlagen und Zubehör darin verschlossen werden.

INF.7.M6 Aufgeräumter Arbeitsplatz [Mitarbeiter]

Jeder Mitarbeiter sollte dazu angehalten werden, seinen Arbeitsplatz aufgeräumt zu hinterlassen. Benutzer sollten dafür sorgen, dass Unbefugte nicht auf Dokumente, IT-Anwendungen oder Daten zugreifen können. Alle Mitarbeiter sollten ihre Arbeitsplätze sorgfältig überprüfen und sicherstellen, dass dort keine schützenswerten Informationen frei zugänglich sind und die Verfügbarkeit, Vertraulichkeit oder Integrität von Daten nicht negativ beeinflusst werden kann. Es darf nicht möglich sein, dass Unbefugte auf Datenträger, wie USB-Sticks, Festplatten, Unterlagen oder Ausdrucke zugreifen können. Auch Passwörter dürfen auf keinen Fall sichtbar oder leicht auffindbar im Büro aufbewahrt werden, z. B. auf einem Klebezettel am Monitor oder unter der Schreibtischauflage.

Besonders bei geplanter Abwesenheit eines Mitarbeiters, z. B. längeren Besprechungen, Dienstreisen, Urlaub oder Fortbildungsveranstaltungen, ist der Arbeitsplatz so aufzuräumen, dass keine schutzbedürftigen Datenträger oder Unterlagen unverschlossen am Arbeitsplatz zurückgelassen werden. Dafür benötigen die Mitarbeiter ausreichend dimensionierte und verschließbare Verstaumöglichkeiten, z. B. stabile Schränke.

Vorgesetzte sollten sporadisch Arbeitsplätze überprüfen, ob dort schutzbedürftige Informationen offen zugreifbar sind, und die Mitarbeiter auf mögliche Mängel hinweisen.

INF.7.M7 Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger [Leiter Haustechnik, Mitarbeiter]

Dienstliche Unterlagen und Datenträger dürfen nur autorisierten Personen zugänglich sein. Es sollte allen Mitarbeitern möglich sein, in ihrem Büro wichtige und vor allem schutzbedürftige Datenträger und Dokumente wegzuschließen. Dazu können beispielsweise verschließbare Schreibtische, Rollcontainer oder Schränke genutzt werden. Die Mitarbeiter sollten darauf hingewiesen werden, dass schutzbedürftige Unterlagen und Datenträger verschlossen aufzubewahren sind.

Die Schlösser dieser Behältnisse sollten mindestens Angriffen mit einfach herzustellenden oder einfach zu erwerbenden Nachschließmitteln (Büroklammer, Dietrich) standhalten. Es sollten Möbelschlösser mit mindestens vier Zuhaltungen und mit möglichst hoher Anzahl an Schließvarianten eingesetzt werden. Zudem ist darauf zu achten, dass der Verschluss nicht leicht umgangen werden kann, z. B. indem einfach die Rückwand des Möbelstücks entfernt wird. Insgesamt sollte die Schutzwirkung des Behältnisses den Sicherheitsanforderungen der darin zu verwahrenden Unterlagen und Datenträger entsprechen.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

INF.7.M8 Einsatz von Diebstahlsicherungen [Leiter IT, Mitarbeiter] (CIA)

Diebstahlsicherungen sind überall dort einzusetzen, wo große Werte zu schützen sind bzw. dort, wo andere Maßnahmen nicht umgesetzt werden können, wie etwa bei Laptops im mobilen Einsatz. Diebstahlsicherungen sind außerdem dort sinnvoll, wo Publikumsverkehr herrscht oder es viele wechselnde Benutzer gibt. Dabei sollte immer bedacht werden, dass die zu schützenden Werte nur zu einem kleinen Teil aus den Wiederbeschaffungskosten für das Gerät bestehen, sondern bei Laptops und ähnlichen IT-Systemen der Wert der darauf gespeicherten Daten berücksichtigt werden muss. Mit Diebstahlsicherungen sollten je nach zu schützendem Objekt nicht nur das IT-System selber, sondern auch Monitor, Tastatur und anderes Zubehör ausgestattet werden.

Auf dem Markt sind die unterschiedlichsten Diebstahlsicherungen (mechanische oder elektrische) erhältlich. Weiterführende Informationen

3 Weiterführende Informationen

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Büroarbeitsplatz" finden sich unter anderem in folgenden Veröffentlichungen:

[27001A12.2] ISO/IEC 27001:2013

Information technology - Security technigues - Information security management systems - Requirements, insbesondere Annex A, A.12.2 Protection from malware, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/ SC 27, Oktober 2013

[ArbStättV] Arbeitsstättenverordnung

Bundesministerium für Arbeit und Soziales (BMAS), http://www.bmas.de/DE/Service/Gesetze/arbeitsstaettenverordnung.html, zuletzt abgerufen am 05.10.2018

[BildscharbV] Bildschirmarbeitsschutzverordnung (BildscharbV)

https://www.arbeitsschutzgesetz.org/bildscharbv/, zuletzt abgerufen am 05.10.2018

[DIN1627] DIN EN 1627:2011-09 Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchshemmung - Anforderung und Klassifizierung

September 201

[ISFCF19] The Standard of Good Practice for Information Security

Area CF19 Physical and Environmental Security, Information Security Forum (ISF), June 2018

[NIST80053PEP] Assesing Security and Privacy Controls for Federal Information Systems and Organizations

NIST Special Publication 800-53, Revision 4, insbesondere Appendix F-PS Page F-2013, Family: Physical and environmental protection, April 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf, zuletzt abgerufen am 05.10.2018

INF: Infrastruktur

Umsetzungshinweise zum Baustein INF.8 Häuslicher Arbeitsplatz

1 Beschreibung

1.1 Einleitung

Telearbeiter, freie Mitarbeiter oder Selbstständige arbeiten typischerweise von häuslichen Arbeitsplätzen aus. Im Gegensatz zum Arbeitsplatz in einer Büroumgebung nutzen Mitarbeiter bei einem häuslichen Arbeitsplatz einen Arbeitsplatz im eigenen Wohnumfeld. Dabei muss ermöglicht werden, dass die berufliche Sphäre hinreichend von der privaten getrennt ist. Wenn Mitarbeiter dauerhaft häusliche Arbeitsplätze benutzen, müssen zudem diverse rechtliche Anforderungen erfüllt sein, beispielsweise müssen sie arbeitsmedizinischen und ergonomischen Bestimmungen entsprechen.

Bei einem häuslichen Arbeitsplatz kann nicht die gleiche infrastrukturelle Sicherheit vorausgesetzt werden, wie sie in den Büroräumen einer Institution anzutreffen ist, so ist z. B. oft der Arbeitsplatz auch für Besucher oder Familienangehörige zugänglich. Deshalb müssen Maßnahmen ergriffen werden, mit denen sich ein mit einem Büroraum vergleichbares Sicherheitsniveau erreichen lässt.

1.2 Lebenszyklus

Planung und Konzeption

Wenn Mitarbeiter vom häuslichen Arbeitsplatz aus arbeiten dürfen, muss der Arbeitsplatz geplant und konzipiert werden. Er ist dabei so einzurichten, dass ein für die geplante Tätigkeit ausreichendes Sicherheitsniveau analog zur Büroumgebung erreicht wird (siehe INF.8.M4 *Geeignete Einrichtung des häuslichen Arbeitsplatzes*).

Betrieb

Der häusliche Arbeitsplatz sollte immer so abgeschlossen werden, dass er möglichst keinem Einbruchsrisiko ausgesetzt ist (siehe INF.8.M3 *Schutz vor unbefugtem Zutritt am häuslichen Arbeitsplatz*). Auch sollten dienstliche Unterlagen und Datenträger weggeschlossen werden und nicht offen herumliegen (siehe INF.8.M1 *Sichern von dienstlichen Unterlagen am häuslichen Arbeitsplatz*).

Wie und welche Arbeitsmaterialien zwischen dem häuslichen Arbeitsplatz und der Institution hin und her transportiert werden dürfen, muss ebenfalls geregelt werden (siehe INF.8.M2 *Transport von Arbeitsmaterial zum häuslichen Arbeitsplatz*).

Aussonderung

Gerade am häuslichen Arbeitsplatz ist es wichtig, Datenträger und Ausdrucke sorgsam zu entsorgen und nicht einfach in den Hausmüll zu werfen (siehe INF.8.M5 *Entsorgung von vertraulichen Informationen am häuslichen Arbeitsplatz*).

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Häuslicher Arbeitsplatz" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

INF.8.M1 Sichern von dienstlichen Unterlagen am häuslichen Arbeitsplatz

Jeder Mitarbeiter sollte dazu angehalten werden, seinen häuslichen Arbeitsplatz aufgeräumt zu hinterlassen. Die Mitarbeiter im häuslichen Umfeld müssen dafür sorgen, dass Unbefugte nicht auf IT-Anwendungen, Daten, Datenträger oder Unterlagen zugreifen können. Alle Mitarbeiter müssen ihre Arbeitsplätze überprüfen und sicherstellen, dass keine sensitiven Informationen frei zugänglich sind, sodass die Verfügbarkeit, Vertraulichkeit und Integrität von Daten nicht negativ beeinflusst werden kann.

Wenn ein Mitarbeiter während der Arbeitszeit nur kurz den häuslichen Arbeitsplatz verlässt, ist es ausreichend, den Raum, sofern möglich, zu verschließen und/oder den Bildschirm so zu sperren, dass Zugriffe nur nach erfolgreicher Authentisierung möglich sind. Ist ein Raum nicht verschließbar, sollten sensible Unterlagen auch bei kurzer Abwesenheit verschlossen werden. Ist ein Mitarbeiter länger abwesend, zum Beispiel, wenn er auf Dienstreise oder im Urlaub ist, muss er seinen Arbeitsplatz so aufräumen, dass keine schutzbedürftigen Datenträger oder Unterlagen unverschlossen herumliegen. Dafür benötigen die Mitarbeiter ausreichend dimensionierte und abschließbare Staumöglichkeiten, wie z. B. sichere Rollcontainer mit Schlössern.

Auch Passwörter dürfen auf keinen Fall leicht auffindbar (z. B. auf einem Klebezettel am Monitor oder unter der Schreibtischauflage) aufbewahrt werden. Auch sollten keine Trivialpasswörter benutzt werden.

Vorgesetzte und Mitarbeiter des Sicherheitsmanagements sollten die Mitarbeiter darauf hinweisen, dass sie ihren häuslichen Arbeitsplatz korrekt aufräumen müssen.

INF.8.M2 Transport von Arbeitsmaterial zum häuslichen Arbeitsplatz [Haustechnik]

Damit dienstliche Aufgaben an einem häuslichen Arbeitsplatz erledigt werden können, müssen dort alle nötigen Informationen vorhanden sein. Akten, Datenträger und andere Unterlagen müssen dabei sicher transportiert werden. Dafür ist die Art und Weise zu regeln, wie Datenträger und Unterlagen zwischen dem häuslichen Arbeitsplatz und der Institution ausgetauscht werden. Folgende Punkte sind daher mindestens zu betrachten bzw. zu regeln:

- Welche Akten, Datenträger und Unterlagen dürfen über welchen Transportweg (z. B. Postweg, Kurier, Paketdienst) ausgetauscht werden?
- Welche Schutzmaßnahmen sind beim Transport zu beachten?
  - Dazu gehört es auch, eine geeignete Verpackung auszuwählen.
  - Informationen auf digitalen Datenträgern sind zu verschlüsseln, bevor sie transportiert werden.
- Welche Akten, Datenträger und Unterlagen dürfen nur persönlich transportiert werden?

Da es sich bei Schriftstücken, Dokumenten und Akten oftmals um Unikate handelt, muss bei der Auswahl eines geeigneten Austauschverfahrens der mögliche Schaden im Falle eines Verlustes beachtet werden. Sofern möglich und zulässig, sollten vor dem Datenträgeraustausch Kopien angefertigt werden.

Alle betroffenen Mitarbeiter müssen darüber informiert sein, wie Akten und Datenträger zu transportieren und dabei angemessen zu schützen sind.

INF.8.M3 Schutz vor unbefugtem Zutritt am häuslichen Arbeitsplatz [Haustechnik]

Institutionen müssen regeln, was Mitarbeiter tun müssen, um ihren häuslichen Arbeitsplatz vor unbefugtem Zutritt dauerhaft zu schützen. Die Regeln sind den Mitarbeitern in geeigneter Form bekannt zu machen.

In Abhängigkeit von den häuslichen Verhältnissen sind geeignete Maßnahmen festzulegen, die sicherstellen, dass Mitbewohner oder Besucher zu keiner Zeit auf dienstliche IT und Unterlagen zugreifen können. Diese Maßnahmen sind in sinnvollen zeitlichen Abständen, mindestens aber bei einer Änderung der häuslichen Verhältnisse zu überprüfen.

Zum Schutz vor unbefugtem Zutritt am häuslichen Arbeitsplatz sollten z. B. folgende Punkte beachtet werden:

- Innen- und Außentüren müssen in Zeiten, in denen ein häuslicher Arbeitsplatz nicht besetzt ist, abgeschlossen werden. Dadurch wird verhindert, dass Unbefugte auf darin befindliche Unterlagen und IT-Einrichtungen zugreifen. Dies ist insbesondere dann wichtig, wenn sich die häuslichen Arbeitsplätze in Bereichen mit Publikumsverkehr befinden oder der Zutritt nicht durch andere Maßnahmen kontrolliert wird.
- Ebenso müssen Fenster und nach außen gehende Türen (Balkone, Terrassen) in Zeiten, in denen ein häuslicher Arbeitsplatz nicht besetzt ist, geschlossen werden. Im Keller- und Erdgeschoss und, je nach Fassadengestaltung, auch in den höheren Etagen, bieten offene Fenster und Türen Einbrechern ideale Einstiegsmöglichkeiten, die auch während der Betriebszeiten des häuslichen Mitarbeiters genutzt werden können.
- Türen, die flurseitig über einen Blindknauf verfügen, müssen nicht abgeschlossen werden. Voraussetzung hierfür ist allerdings, dass die befugten Mitarbeiter ihren Schlüssel zum häuslichen Arbeitsplatz stets mit sich führen.
- Bei laufendem Rechner kann darauf verzichtet werden die Tür abzuschließen, wenn der Mitarbeiter den häuslichen Arbeitsplatz nur kurzzeitig verlässt und auf den PC nur nach erfolgreicher Authentisierung zugegriffen werden kann. Bei ausgeschaltetem Rechner kann das Büro offen bleiben, wenn sich der Rechner nur mithilfe eines Passwortes booten lässt. Die gleiche Funktion erfüllen Zugangsmechanismen, die auf Token oder Chipkarten basieren. Sollten schützenswerte Unterlagen am Arbeitsplatz liegen, ist die Tür jedoch abzuschließen.

Gemeinsam mit den Basismaßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Häuslicher Arbeitsplatz".

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Häuslicher Arbeitsplatz".

INF.8.M4 Geeignete Einrichtung des häuslichen Arbeitsplatzes [Haustechnik]

Bei der Auswahl eines häuslichen Arbeitsplatzes ist darauf zu achten, dass er geeignet eingerichtet werden kann, ergonomischen Anforderungen gerecht wird und notwendige Maßnahmen zum Einbruchsschutz vorhanden sind oder sich nachrüsten lassen.

Einrichtung

Für den häuslichen Arbeitsplatz ist ein eigenes Arbeitszimmer wünschenswert. Zumindest sollte der häusliche Arbeitsplatz von der übrigen Wohnung durch eine abschließbare Tür abtrennbar sein, damit sich dort befindliche Unterlagen und IT-Systeme außerhalb der Bereiche befinden, in denen sich weitere Bewohner, Angehörige oder Besucher aufhalten. Bei spontanen Besuchen kann so der Arbeitsplatz kurzfristig verlassen und vor unbefugtem Zugriff geschützt werden.

Die Einrichtung sollte unter Berücksichtigung von Ergonomie, Sicherheit und Gesundheitsschutz ausgewählt werden. Das bedeutet unter anderem:

- ausreichend Platz für Möbel und Bildschirmarbeitsplatz,
- regelbare Raumtemperatur und ausreichende Lüftungsmöglichkeiten,
- Abschirmung gegenüber Lärmquellen,
- Tageslicht sowie ausreichend künstliche Beleuchtung,
- Sichtschutz des Monitors, falls er durch ein Fenster beobachtet werden könnte,
- Vermeidung von störenden Blendungen, Reflexen oder Spiegelungen am Arbeitsplatz und
- Anschlüsse für Telefon und Strom.

Die dienstlich genutzte IT sollte vom Arbeitgeber bereitgestellt werden, um Sicherheitsrichtlinien durchsetzen zu können. Nur dann kann z. B. per Dienstanweisung ausgeschlossen werden, dass die IT für private Zwecke benutzt wird.

Am häuslichen Arbeitsplatz müssen dieselben Vorschriften und Richtlinien bezüglich der Gestaltung des Arbeitsplatzes und der Arbeitsumgebung beachtet werden wie in der Institution. Ein häuslicher Arbeitsplatz muss also für die jeweiligen Aufgaben ausreichend ausgestattet sein, d. h. es muss nicht nur geeignetes Mobiliar, sondern es sollten auch angemessene Schutzvorkehrungen wie beispielsweise abschließbare Schränke vorhanden sein.

Mitarbeiter mit einem häuslichen Arbeitsplatz sollten regelmäßig befragt werden, ob der Arbeitsplatz ihren gesundheitlichen und betrieblichen Ansprüchen genügt. Stichprobenhafte Kontrollbesuche seitens der Institution sollten nur durchgeführt werden, wenn sie vorher mit dem Mitarbeiter abgesprochen wurden.

Einbruchsschutz

Erfahrungsgemäß wählen Einbrecher ihre Ziele danach aus, wie hoch Risiko und Aufwand im Verhältnis zum erwarteten Gewinn sind. Daher sollten alle Maßnahmen zum Einbruchsschutz beim häuslichen Arbeitsplatz darauf zielen, die Erfolgsaussichten von Tätern zu minimieren. Eventuell reichen die vorhandenen Sicherheitsmaßnahmen am häuslichen Arbeitsplatz bereits aus. Sollte das nicht der Fall sein, müssen die gängigen Maßnahmen zum Einbruchsschutz jeweils an die örtlichen Gegebenheiten und den vorliegenden Schutzbedarf angepasst werden. Dazu gehören beispielsweise:

- einbruchhemmende Türen und Fenster, beispielsweise mit der Widerstandsklasse RC2 (nach DIN EN 1627:2011-09 "Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchhemmung - Anforderungen und Klassifizierung") oder höherwertig, wenn die Gefährdungslage es erforderlich macht,
- Rollladensicherungen bei einstiegsgefährdeten Türen oder Fenstern,
- besondere Schließzylinder, Zusatzschlösser und Riegel,
- gegebenenfalls Sicherung von Kellerlichtschächten,
- Verschluss von nicht benutzten Nebeneingängen.

Empfehlungen hierzu können die örtlichen Beratungsstellen der Kriminalpolizei abgeben.

Während der Planung, bei der Umsetzung und später im Betrieb sollte eine fachkundige Person regelmäßig begutachten, ob der Einbruchsschutz durchgängig ist und möglichen Überwindungsversuchen überall einen gleichwertigen Widerstand entgegensetzt.

Den Mitarbeitern am häuslichen Arbeitsplatz ist bekanntzugeben, welche Regelungen und Maßnahmen zum Einbruchsschutz beachtet werden müssen, also beispielsweise dass Türen, Fenster oder Rollladensicherungen abends abgeschlossen werden müssen (siehe dazu auch INF.8.M3 *Schutz vor unbefugtem Zutritt am häuslichen Arbeitsplatz*).

Auch direkt am häuslichen Arbeitsplatz kann es sinnvoll sein, einbruchhemmende Elemente einzubauen, zum Beispiel bei einem erhöhten Schutzbedarf.

Ergonomischer Arbeitsplatz

Die Belastungen durch dauerhafte Tätigkeiten an schlecht ausgestatteten häuslichen Arbeitsplätzen sind nicht zu unterschätzen, da sie zu gesundheitlichen Beschwerden führen können. Durch einen ergonomischen Arbeitsplatz können diese Belastungen jedoch verringert werden. Eine verbesserte Ergonomie bedeutet zudem eine effektivere Arbeitsweise. Das bringt nicht nur gesundheitliche Vorteile für den Arbeitnehmer, sondern hat auch ein wirtschaftlicheres Arbeiten und eine verbesserte Umsetzung von Sicherheitsmaßnahmen zur Folge.

Daher sollte jeder Arbeitsplatz ergonomisch gestaltet werden. Bei Computerarbeitsplätzen müssen beispielsweise Stuhl, Tisch, Bildschirm und Tastatur individuell einstellbar sein, um eine möglichst fehlerfreie Bedienung der IT zu ermöglichen und zu fördern. Das beinhaltet unter anderem, dass Rückenlehne, Sitzhöhe und Sitzfläche des Stuhls verstellbar sein müssen, aber auch, dass die Arbeitsmittel so angeordnet werden können, dass für die jeweilige Arbeitsaufgabe eine möglichst geringe Belastung entsteht.

Auch die am häuslichen Arbeitsplatz eingesetzten IT-Systeme, vor allem der Bildschirm, müssen ergonomisch aufgestellt werden. So sollte beispielsweise der Bildschirm immer im rechten Winkel zum Fenster aufgestellt werden, um die direkte Lichteinstrahlung darauf zu vermeiden. Außerdem sollte an IT-Systemen ein ungestörtes Arbeiten möglich sein. Mitarbeitern im häuslichen Bereich sollten andere Personen nicht ständig über die Schulter blicken können. Damit lässt sich auch verhindern, dass Informationen unbefugt eingesehen werden.

Ein entsprechend ausgestatteter Arbeitsplatz erleichtert es auch, Sicherheitsmaßnahmen einzuhalten. Wenn Datenträger, Dokumentationen, Unterlagen und Zubehör eingeschlossen werden sollen, muss es dafür verschließbare Schreibtische oder Schränke geben.

INF.8.M5 Entsorgung von vertraulichen Informationen am häuslichen Arbeitsplatz [**Haustechnik**]

Betriebsmittel oder Sachmittel am häuslichen Arbeitsplatz (z. B. Druckerpapier, USB-Festplatten, DVDs, USB-Sticks, SD-Karten, aber auch spezielle Tonerkassetten) werden irgendwann nicht mehr benötigt oder müssen ausgesondert werden. Wenn sie schützenswerte Daten enthalten, müssen sie so entsorgt werden, dass keine Rückschlüsse auf vorher gespeicherte Daten möglich sind. Bei funktionstüchtigen Datenträgern sollten die Daten sicher gelöscht werden. Nicht funktionierende oder nur einmal beschreibbare Datenträger müssen mechanisch zerstört werden (siehe dazu auch CON.6 *Löschen und Vernichten*).

Eine spezielle Sicherheitsrichtlinie sollte regeln, wie schutzbedürftiges Material entsorgt werden soll. Falls erforderlich müssen am häuslichen Arbeitsplatz die dafür benötigten Entsorgungseinrichtungen vorhanden sein, z. B. Aktenvernichter.

Es ist auch möglich, die schützenswerten Betriebsmittel durch den Mitarbeiter am häuslichen Arbeitsplatz sammeln zu lassen und für die Entsorgung die Entsorgungseinrichtungen am Standort der Institution bereitzustellen.

Wird schutzbedürftiges Material gesammelt, um es später zu entsorgen, muss es sicher verschlossen und vor unberechtigtem Zugriff geschützt werden.

Soweit in der Institution keine umweltgerechte und sichere Entsorgung durchgeführt werden kann, sind damit beauftragte Dienstleister darauf zu verpflichten, die erforderlichen Sicherheitsmaßnahmen einzuhalten. Ein Mustervertrag findet sich unter den Hilfsmitteln zum IT-Grundschutz auf den BSI-Webseiten [MVED]. Es sollte regelmäßig durch die Institution geprüft werden, ob der Entsorgungsvorgang der beauftragten Dienstleister verlässlich ist.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

INF.8.M6 Umgang mit dienstlichen Unterlagen bei erhöhtem Schutzbedarf am häuslichen Arbeitsplatz [Informationssicherheitsbeauftragter (ISB)] (CIA)

Wenn Mitarbeiter mit dienstlichen Unterlagen arbeiten müssen, für die ein erhöhter Schutzbedarf besteht, sollte überlegt werden, ob von einem häuslichen Arbeitsplatz nicht ganz abzusehen ist. Wenn es dennoch unabdingbar ist, sollten möglichst dem Schutzbedarf angemessene Diebstahlsicherungen für die Speichersysteme der dienstlichen Unterlagen und verschließbare Schränke, Tresore, Rollcontainer sowie Schreibtische genutzt werden, um die dienstlichen Unterlagen geeignet wegzuschließen.

Die dienstlichen Unterlagen und Datenträger mit erhöhtem Schutzbedarf dürfen am häuslichen Arbeitsplatz nur autorisierten Personen zugänglich sein. Außerhalb der Nutzungszeit müssen sie so aufbewahrt werden, dass kein Unbefugter darauf zugreifen kann.

Damit die Anforderungen erfüllt werden, müssen die Mitarbeiter am häuslichen Arbeitsplatz darauf hingewiesen werden, dass Unterlagen und Datenträger mit erhöhtem Schutzbedarf verschlossen aufzubewahren sind.

Die Schlösser der verschließbaren Schränke, Rollcontainer sowie Schreibtische müssen mindestens Angriffen mit einfach herzustellenden oder einfach zu erwerbenden Nachschließmitteln (Büroklammer, Dietrich etc.) standhalten. Es sollten Möbelschlösser mit mindestens vier Zuhaltungen und mindestens 1000 Schließvarianten eingesetzt werden. Zudem ist darauf zu achten, dass der Verschluss nicht leicht umgangen werden kann, z. B. indem eine Rückwand entfernt wird. Insgesamt sollte die Schutzwirkung des Behältnisses den Sicherheitsanforderungen der darin zu verwahrenden Unterlagen und Datenträger entsprechen.

An häuslichen Arbeitsplätzen müssen deshalb für den Schutz- und Platzbedarf ausreichende verschließbare Behältnisse (Schreibtisch, Rollcontainer, Schrank, Tresor) mit angemessener Schutzwirkung vorhanden sein.

Um den Schutz der Datenträger und IT-Systeme mit vertraulichen Informationen zu erhöhen, sollten diese auch im häuslichen Umfeld so gesichert werden, dass Angreifer sie nicht einfach mitnehmen können, also beispielsweise mit Diebstahlsicherungen versehen werden.

3 Weiterführende Informationen

3.1 Wissenswertes

Je nach Branche, eingesetzter Technik oder anderen Rahmenbedingungen können sich für einen Informationsverbund weitere (benutzerdefinierte) Anforderungen ergeben. Zu diesen können beispielsweise die folgenden Maßnahmen gehören.

Zu den wichtigsten Grundpfeilern der Informationssicherheit in einer Institution gehören deren Mitarbeiter. Selbst die aufwendigsten technischen Sicherheitsvorkehrungen sind ohne das richtige Verhalten der Mitarbeiter wertlos. Ein Bewusstsein dafür, was Informationssicherheit für die Institution und deren Geschäftsprozesse bedeutet und der richtige Umgang der Mitarbeiter mit den zu schützenden Werten und Informationen der Institution sind dafür wesentlich.

Die für die Institution ausgewählten Sicherheitsmaßnahmen sollten sich daher immer an den Mitarbeitern orientieren. Dabei sollte deren Wissen und Umgang mit Informationen und IT einbezogen werden. Zur Beurteilung, wie sich Mitarbeiter aus Sicherheitssicht verhalten, können die Faktoren analysiert werden, die zu diesem Verhalten beitragen. Darauf aufbauend kann untersucht werden, wo die personelle und organisatorische Sicherheit noch verbessert werden kann, beispielsweise durch Sensibilisierung und Schulung zur Informationssicherheit.

Folgende Aspekte sollten berücksichtigt werden:

Sicherheitskultur

Der Begriff Sicherheitskultur umfasst die sicherheitsbezogenen Einstellungen, Werte und grundlegenden Überzeugungen einer Institution und aller ihrer Mitarbeiter. Zur Sicherheitskultur gehört auch, wie offen der Umgang mit Fragen zur Informationssicherheit in der Institution gelebt wird. So ist für die effektive und effiziente Behandlung von Sicherheitsvorfällen eine vertrauensvolle und offene Kommunikationskultur wichtig, damit Sicherheitsvorfälle auch umgehend weitergemeldet und lösungsorientiert angegangen werden.

- Wie ist der Umgang in der Behörde oder dem Unternehmen mit geschäftsrelevanten Informationen und mit Risiken generell? Ist die Institution eher risiko-orientiert oder eher risiko-vermeidend? Werden Informationen eher freizügig oder nur restriktiv weitergegeben?
- Wie sind die Anforderungen an Genauigkeit und Präzision? Sind kleinere Fehler beispielsweise in Texten tragbar, weil diese ohnehin noch mehrere Abstimmprozesse durchlaufen müssen? Kann ein Eingabefehler bereits zu folgenschweren Schäden führen?Wie sind die Ansprüche an Verfügbarkeit? Gibt es eine Vielzahl enger Termine? Können Bearbeitungszeiten für Anfragen und Geschäftsprozesse flexibel festgelegt werden? Sind kleinere Terminüberschreitungen oder -änderungen im Allgemeinen tragbar oder führen sie zu harten Konsequenzen?
- Wie sind die Ansprüche an Verfügbarkeit? Gibt es eine Vielzahl enger Termine? Können Bearbeitungszeiten für Anfragen und Geschäftsprozesse flexibel festgelegt werden? Sind kleinere Terminüberschreitungen oder -änderungen im Allgemeinen tragbar oder führen sie zu harten Konsequenzen?

Stark beeinflusst wird die Sicherheitskultur einer Institution davon, in welcher Branche diese tätig ist. In Hochsicherheitsbereichen wird naturgemäß weniger offen mit Informationen umgegangen als in Forschungseinrichtungen.

Wissen und Können

- Wie gut kennen sich die Mitarbeiter mit IT aus? Ist IT- und Internet-Nutzung eher eine Notwendigkeit, um Geschäftsprozesse effektiver gestalten zu können, oder sind Leben und Arbeiten ohne IT und Internet nicht mehr vorstellbar?
- Welche Erfahrungen und Kenntnisse haben die Mitarbeiter über Informationssicherheit und Datenschutz? Wie sind deren Fähigkeiten zu IT-basierten Sicherheitsmaßnahmen wie Verschlüsselung? Wie ist das Wissen in den verschiedenen Bereichen der Institution verteilt?
- Wie ist der gelebte Umgang der Mitarbeiter mit Fragen der Informationssicherheit und des Datenschutzes? Wie sehen die Mitarbeiter den Bedarf, Informationen vor Veränderungen oder unbefugter Weitergabe zu schützen?Können Mitarbeiter aktiv ihre Ideen und Vorstellungen zur Informationssicherheit in den Sicherheitsprozess einbringen?
- Können Mitarbeiter aktiv ihre Ideen und Vorstellungen zur Informationssicherheit in den Sicherheitsprozess einbringen?

Sicherheitsrichtlinien

- Passen die Sicherheitsrichtlinien der Institution zu den Geschäftsprozessen und der internen Sicherheitskultur? Sind sie einfach umzusetzen? Sind sie praxisnah und den aktuellen Umgebungsbedingungen angepasst? Behindern sie Arbeitsläufe? Unterstützen sie erwünschte Verhaltensweisen?

Anwendungen und IT

- Ermöglichen die vorhandenen IT-, ICS- und IoT-Komponenten einen Umgang mit den geschäftsrelevanten Informationen, der sowohl deren Schutzbedarf als auch den festgelegten Sicherheitsvorgaben entspricht?

Leitungsebene

- Wie steht die Leitungsebene zur Informationssicherheit? Nehmen Vorgesetzte ihre Vorbildfunktion wahr? Gibt es Wünsche der Leitungsebene zur Verbesserung der Sicherheitsprozesse?

Kulturelle Hintergründe

- Auch die kulturellen Hintergründe können den Umgang mit zu schützenden Informationen und mit Sicherheitsvorgaben generell beeinflussen. Daher sollte untersucht werden, ob es regionale und nationale Unterschiede im Umgang mit Informationssicherheit gibt. Vor allem sollte auch ergründet werden, welche unterschiedlichen Herangehensweisen an Informationssicherheit es in den verschiedenen Bereichen der Institution gibt. Auch einzelne Abteilungen können bereits eigene Regeln und Verhaltensweisen im Umgang mit geschäftsrelevanten Informationen entwickeln.

Veränderungen

- Alle Arten von weitreichenden Veränderungen für die Beschäftigten können deren Umgang mit Informationen, Geschäftsprozessen, IT und sonstigen Geräten ändern. Dazu gehören beispielsweise Umstrukturierungen, Entlassungen, Wechsel von Aufgaben oder Vorgesetzten.

Sollte sich bei der Analyse herausstellen, dass sich Mitarbeiter anders verhalten als es aus Sicherheitssicht sinnvoll ist, gibt es verschiedene Wege, um hiermit umzugehen. Es kann z. B. versucht werden, das Verhalten zu ändern. Andererseits kann es in vielen Fällen einfacher sein, die Sicherheitsvorgaben oder Arbeitsabläufe umzugestalten und sicherer zu machen.

Die Verantwortlichen für Sensibilisierungs- und Schulungsprogramme sollten klären, ob und in welchem Umfang sie eigene Mitarbeiter oder externe Anbieter als Trainer einsetzen wollen. Außerdem muss die Form der Ausbildung festgelegt werden. Sofern ein Programm mehrere Sensibilisierungs- und Schulungsmaßnahmen umfasst, sollte ein Schulungskoordinator ernannt werden. Darüber hinaus sollten verschiedene Angebote von Schulungsanbieter daraufhin verglichen worden, welche inhaltlich, qualitativ und preislich am besten geeignet sind. Die durchgeführten Sensibilisierungs- oder Schulungsmaßnahmen sollten von den Teilnehmern bewertet und diese Erfahrungen regelmäßig intern ausgewertet werden.

Wenn eigene Mitarbeiter als Trainer eingesetzt werden sollen, müssen diese das benötigte Fachwissen haben und dazu fähig sein, dieses Wissen auch zielgruppengerecht zu vermitteln. Neben den erforderlichen Informationssicherheitskenntnissen müssen die Trainer über ausgeprägte didaktische, methodische und kommunikative Fähigkeiten verfügen. Speziell für Sensibilisierungsmaßnahmen sind außerdem ausreichende Kenntnisse über die Institution, deren Sicherheitskultur sowie die Geschäftsprozesse erforderlich. Wichtig ist, dass Trainer die Sprache ihres jeweiligen Zielpublikums beherrschen, also die zu schulenden Informationssicherheitsaspekte in die jeweiligen Arbeits- und Projektzusammenhänge stellen können. Interne Trainer müssen die erforderliche Zeit bekommen, um Sensibilisierungs- und Schulungsmaßnahmen nicht nur durchführen, sondern auch vorbereiten und auswerten zu können.

Aus Kosten- oder Qualifikationsgründen kann es zumindest zu Beginn vorteilhafter sein, die Schulung durch externe Fachkräfte durchführen zu lassen. Schon in der Planungsphase muss geklärt werden, welche finanziellen Ressourcen dafür verfügbar sind. Die externen Trainer sollten sorgfältig anhand von inhaltlichen, qualitativen und preislichen Kriterien ausgewählt und auf ihre Aufgabe vorbereitet werden. Insbesondere müssen ihnen die erforderlichen institutionsinternen Hintergründe vermittelt werden.

Auch bei externer Durchführung von Sensibilisierungs- oder Schulungsmaßnahmen sind interne Ressourcen erforderlich. Es sollte ein verantwortlicher Schulungskoordinator benannt werden, der

- qualifizierte Schulungsanbieter auswählt,
- Lerninhalte und -methoden vorgibt sowie den Trainern erforderliche Informationen zur Verfügung stellt,
- die interne Schulungsplanung, -vorbereitung und -durchführung koordiniert,
- die Kommunikationsschnittstelle zwischen Trainern und eigenen Mitarbeitern bildet,
- die Teilnehmerbewertungen analysiert und geeignete Verbesserungsmaßnahmen festlegt, gegebenenfalls zusammen mit den Trainern.

Die Schulungskoordination kann der Informationssicherheitsbeauftragter oder auch ein Mitarbeiter aus der Personalabteilung übernehmen. Der Informationssicherheitsbeauftragte und die Personalabteilung müssen hierbei auf jeden Fall eng zusammenarbeiten.

Erfahrungsgemäß gibt es eine Reihe von externen Anbietern, die geeignete Sensibilisierungs- oder Schulungsmaßnahmen in einer Form anbieten, die den Bedürfnissen der Institution entsprechen oder die mit vertretbarem Aufwand angepasst werden können.

Bei Sensibilisierungs- oder Schulungsmaßnahmen, die in mehreren Zyklen eine größere Zahl von Mitarbeitern erreichen sollen, bietet es sich an, über ein "Train the Trainer"-Konzept nachzudenken. Hierbei werden die initialen Maßnahmen entweder von geeigneten internen Mitarbeitern oder externen Trainern mit dem Ziel durchgeführt, dass die Teilnehmer dieser Maßnahmen später selbst eine Trainerrolle übernehmen. Dies kann für diese Mitarbeiter einen sehr positiven Effekt auf ihre eigene Sensibilisierung und Motivation für Informationssicherheit haben. Darüber hinaus können sie ihre eigenen Erfahrungen in die Trainingsmaßnahmen einbringen. Gerade bei Trainingsthemen, die Aspekte der Kultur und bestimmter Verhaltensweisen innerhalb der Institution beinhalten, kann ein interner Trainer aufgrund seiner tieferen Kenntnis interner Prozesse und Bekanntheit bei den Teilnehmern die Akzeptanz und den Lernerfolg des Trainings erhöhen. Sofern das "Train the Trainer"-Konzept eingesetzt werden soll, müssen die initialen Maßnahmen neben den vorgesehenen Fachinhalten auch Anleitungen zur methodisch-didaktischen Lehrstoffvermittlung beinhalten.

Die durchgeführten Sensibilisierungs- oder Schulungsmaßnahmen sollten von den Teilnehmern abschließend bewertet werden. Diese Erfahrungen sollten regelmäßig intern ausgewertet werden.

Viele Sicherheitsschulungen empfinden Teilnehmer als trocken, was negative Auswirkungen auf den gewünschten Lerneffekt mit sich bringt. Eine gute Möglichkeit, den Lehrstoff aufzulockern, sind Plan- oder Rollenspiele. An solche Spiele erinnern sich die Teilnehmer meist länger und prägnanter als an klassische Folienpräsentationen. Auch tragen sie dazu bei, die Bedrohungen stärker zu verdeutlichen und typische Schwachstellen, aber auch Lösungsmöglichkeiten in der eigenen Arbeitsumgebung aufzuzeigen. Sie ermöglichen es den Teilnehmern, Situationen zu üben, um dann im Ernstfall routinierter zu agieren. Es sollte geprüft werden, ob die restlichen Sensibilisierungs- und Schulungsinhalte durch den Einsatz von Planspielen unterstützt werden können.

Planspiele können aus praktischen Beispielen, z. B. anhand aktueller Vorfälle aus den Medien, selbst zusammengestellt oder bei Schulungsdienstleistern in Auftrag gegeben werden. Dabei sind die Inhalte der Planspiele möglichst an die eigene Institution anzupassen. Dadurch können sich die Mitarbeiter besser mit den aufgezeigten Lösungen identifizieren. Durch die Simulation z. B. von Sicherheitsvorfällen, die geschäftskritische Prozesse beeinträchtigen können, sind die Mitarbeiter im Ernstfall gut vorbereitet.

Genau wie bei Schulungen ist bei diesen Formaten die zielgruppengerechte Planung von Inhalten sehr wichtig. Die Teilnehmer sollen die Relevanz der Rollenspiele erkennen und in ihrem Arbeitsumfeld unmittelbar davon profitieren können.

Bei allen Bemühungen, die Mitarbeiter auf die Bedeutung von Informationssicherheit aufmerksam zu machen, soll eine positive und konstruktive Grundstimmung bewahrt werden. Ständige Angst vor Sicherheitsvorfällen kann einerseits zur Verdrängung von Sicherheitsproblemen und andererseits zu Panikreaktionen verleiten.

Die folgenden Beispiele zeigen, dass Planspiele von sehr einfach zu realisierenden Übungen, die im Rahmen einer Schulung durchgeführt werden können, bis hin zu komplexen Simulationsübungen reichen können. Die Aufgabe der verantwortlichen Planer ist es nun, entsprechend den Erfordernissen der unterschiedlichen Zielgruppen die geeigneten Szenarien zu entwickeln.

Tragen von Mitarbeiterausweise

Durch kurze Rollenspiele können Mitarbeiter sehr gut üben, wie sie sich verhalten sollen, wenn sie innerhalb der Institution organisationsfremde Personen antreffen. Es kann eingeübt werden, wie die Mitarbeiter optimal auf diese Situation reagieren können, beispielsweise indem sie anbieten, die Externen zum Gesprächspartner zu begleiten. Auch der Umgang mit Besuchern, die die Hausregeln kennen, aber verweigern, kann trainiert werden, beispielsweise wenn ein Besucher das Tragen eines Ausweises ablehnt, weil er persönlich mit dem Geschäftsführer bekannt sei.

Social

Im Rahmen von Simulationen können Mitarbeiter üben, wie sie sich bei Social-Engineering-Angriffen verhalten sollen. Dazu werden die ausgewählten Zielgruppen wie z. B. IT-Betreuer und verschiedene Administratorengruppen in einer gemeinsamen Simulation mit vermeintlich harmlosen Anfragen konfrontiert. Erst durch das fachübergreifende Betrachten dieser Anfragen wird deutlich, dass hier ein Angriff vorliegt. Ziel der Simulation ist es, diese Zusammenhänge durch entsprechende Übungen herauszufinden, um im Anschluss in definierter Art und Weise reagieren zu können. Diese Art von Simulation lässt sich in der Praxis sehr gut durch Workshops mit Moderationsmaterialien wie Pinnwand und Moderationskarten durchführen.

Simulationsübungen

Besonders wichtig sind Simulationen, in denen die Behandlung von Sicherheitsvorfällen bis hin zu Notfallsituationen geübt wird. Sie sollen Mitarbeiter in die Lage versetzen, zugeordnete Rollen und Verantwortlichkeiten innerhalb eines Szenarios auch unter erschwerten Bedingungen (Anspannung, Häufung von Anweisungen, unklare oder oft wechselnde Sachlage, Ressourcenmangel, Kommunikationsprobleme etc.) möglichst sicher wahrzunehmen. Das Ziel von Simulationen liegt primär im Training persönlicher Fähigkeiten anhand repräsentativer Szenarien, die dann in möglichst vielen Vorfallsituationen genutzt werden können. Daher sollte eine Simulation von einem erfahrenen Trainer geleitet werden, der nach ihrer Durchführung im Rahmen eines Reviews mit den Teilnehmern ihre Erfahrungen diskutiert und vertieft.

Bei der Konzeption von Sensibilisierungs- und Schulungsprogrammen ist die Lehrstoffsicherung wichtig, da nur dauerhaft präsentes Wissen auch zu den gewünschten Verhaltensänderungen führt. Nach Sensibilisierungs- und Schulungsaktivitäten sind die Teilnehmer in der Regel mit viel neuem Wissen und neuen Fertigkeiten ausgestattet. Wenn sie dieses Wissen im Anschluss an die Veranstaltungen nicht abrufen oder anwenden, besteht die Gefahr, dass sie es wieder ganz oder teilweise vergessen. Damit sich das Bewusstsein für Informationssicherheit bei den Mitarbeitern dauerhaft verbessert, sollten die Inhalte von Sensibilisierungs- und Schulungsmaßnahmen regelmäßig wiederholt bzw. angewendet werden. Dies wird durch die Lehrstoffsicherung unterstützt, die sowohl während der Schulung, am Ende einer Schulung als auch im Zeitraum danach durchgeführt werden sollte.

Die Auswahl von Maßnahmen zur Lehrstoffsicherung ist auf die jeweilige Organisationskultur und -größe abzustimmen.

Beispiele für Maßnahmen zur Lehrstoffsicherung sind:

- schriftliche oder mündliche Tests während der Schulung oder/und zum Abschluss
- Quizfragebögen mit Gewinnmöglichkeiten zu Schulungsinhalten
- Intranet-basierte Befragungen zu den Inhalten der durchgeführten Schulungen
- Nutzung von Teambesprechungen etc. für die Diskussion aktueller Aspekte der Informationssicherheit
- Durchführung von Plan- oder Rollenspielen (siehe ORP.3.M11 Durchführung von Planspielen zur Informationssicherheit)
- regelmäßige Wiederholung von Seminaren
- kurze Hinweise im Intranetergänzende Kurzvorträge, z. B. im Rahmen anderer interner Veranstaltungen
- ergänzende Kurzvorträge, z. B. im Rahmen anderer interner Veranstaltungen

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Häuslicher Arbeitsplatz" finden sich unter anderem in folgenden Veröffentlichungen:

[27001] ISO/IEC 27001:2013

Information technology-Security techniques-Information security management systems-Requirements, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/SC 27, Oktober 2013

[DIN1627] DIN EN 1627:2011-09 Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchshemmung - Anforderung und Klassifizierung

September 201

[ISF] The Standard of Good Practice for Information Security:

Information Security Forum (ISF), June 2018

[NIST80053] Security and Privacy Controls for Federal Information Systems and Organizations

NIST Special Publication 800-53, Revision 4, April 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf , zuletzt abgerufen am 30.08.2018

INF: Infrastruktur

Umsetzungshinweise zum Baustein INF.9 Mobiler Arbeitsplatz

1 Beschreibung

1.1 Einleitung

Mithilfe von immer leistungsfähigeren IT-Geräten, wie Laptops, Smartphones oder Tablets, können Mitarbeiter nahezu an jedem Platz bzw. von überall arbeiten. Das bedeutet, dass dienstliche Aufgaben häufig nicht mehr nur in Räumen und Gebäuden der Institution erfüllt werden müssen, sondern an wechselnden Arbeitsplätzen in unterschiedlichen Umgebungen erledigt werden. Ob in Hotelzimmern, in Zügen oder bei Kunden, das mobile Arbeiten verändert die Dauer, Lage und Verteilung der Arbeitszeiten.

In mobilen Arbeitsplatz-Umgebungen kann die Sicherheit der Infrastruktur, wie sie in einer Büroumgebung anzutreffen ist, nicht vorausgesetzt werden. Daher sind Sicherheitsanforderungen erforderlich, die eine mit einem Büroraum vergleichbare Sicherheitssituation herbeiführen.

1.2 Lebenszyklus

Planung und Konzeption

Bevor ein Mitarbeiter einen mobilen Arbeitsplatz benutzt, muss entschieden werden, ob der Platz dafür überhaupt geeignet ist. Dafür benötigen die Mitarbeiter Auswahlkriterien, die von der Institution zu definieren sind (siehe INF.9.M1 *Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes).*

Die Sicherheit mobiler Arbeitsplätze basiert größtenteils auf geeigneten organisatorischen Regelungen und personellen Maßnahmen. Daraus ergeben sich Anforderungen, die in den Maßnahmen INF.9.M2 *Regelungen für mobile Arbeitsplätze und* INF.9.M8 *Sicherheitsrichtlinie für mobile Arbeitsplätze* erläutert werden.

Umsetzung

Für alle Arbeiten von unterwegs ist zu regeln, welche Informationen außerhalb der Institution transportiert und bearbeitet werden dürfen und welche Schutzvorkehrungen dabei zu treffen sind (siehe INF.9.M2 *Regelungen für mobile Arbeitsplätze*). Dabei ist auch zu klären, unter welchen Rahmenbedingungen Mitarbeiter mit mobilen IT-Systemen auf interne Informationen ihrer Institution zugreifen dürfen.

Betrieb

Beim mobilen Arbeiten müssen nicht nur die mitgenommenen IT-Systeme (zum Beispiel Laptops, Smartphones oder Tablets), sondern auch die unterwegs bearbeiteten Informationen sorgfältig behandelt werden. So sollten die vom Arbeitgeber vorgesehenen Regelungen über die Arbeitsumgebung eingehalten sowie die Arbeitsmaterialien sicher aufbewahrt werden (siehe INF.9.M3 *Zutritts- und Zugriffsschutz* und INF.9.M4 *Arbeiten mit fremden IT-Systemen).*

Bei erhöhtem Schutzbedarf sind zusätzlich die Maßnahmen wie Diebstahlsicherungen (siehe INF.9.M10 *Einsatz von Diebstahlsicherungen)* oder gesicherte Kommunikationsverbindungen (siehe INF.9.M11 *Verbot der Nutzung unsicherer Umgebungen*) zu beachten.

Aussonderung

Gerade in fremden Infrastruktur-Umgebungen ist es wichtig, Datenträger und Ausdrucke sorgsam zu entsorgen und nicht einfach in den Müll zu werfen. Für eine sichere Aussonderung ist es daher erforderlich, neben den Anforderungen aus INF.9.M6 *Entsorgung von vertraulichen Informationen* auch die Anforderungen aus dem Baustein OPS.1.2.7 *Verkauf/Aussonderung von IT* zu berücksichtigen.

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Mobiler Arbeitsplatz" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

INF.9.M1 Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes [Benutzer, Vorgesetzte]

Dank immer kleinerer und leistungsfähigerer IT-Systeme ist es heutzutage möglich, nahezu überall zu arbeiten. Dadurch kann jeder beliebige Ort oder Platz (weltweit) als mobiler Arbeitsplatz genutzt werden. Zum Beispiel ist es möglich in Hotelzimmern, in Bahnen, in Flugzeugen oder in Räumlichkeit beim Kunden zu arbeiten.

Solche mobilen Arbeitsplätze können vom Benutzer nur sehr beschränkt eingerichtet werden und müssen oft wie vorgefunden genutzt werden. Daher sollte jeder mobile Benutzer entscheiden können, ob eine Umgebung als mobiler Arbeitsplatz geeignet ist. Benutzer sollten deshalb für die Auswahl mit praktischen Handreichungen unterstützt werden.

Gründe, die gegen einen mobilen Arbeitsplatz sprechen, sind beispielsweise:

- Die zu bearbeitenden Informationen sind zu vertraulich, um außerhalb der geschützten Büroumgebung bearbeitet zu werden (siehe auch INF.9.M2 *Regelungen für mobile Arbeitsplätze*).
- Die Umgebung erlaubt es nicht, ohne Einsichtnahme Dritter zu arbeiten, zum Beispiel in engen Sitzplätzen in Bahnen oder Flugzeugen.
- Es ist weder eine Stromversorgung noch eine Netzanbindung vorhanden.
- Die Nutzung von mobilen IT-Geräten ist verboten, zum Beispiel im Flugzeug oder in fremden Büroräumen.

Gründe, die für einen mobilen Arbeitsplatz sprechen, sind beispielsweise:

- Da viele mobile IT-Systeme durch Stürze zerstört werden, sollte ein stabiler Platz vorhanden sein, um diese abzustellen.
- Die Umgebung sollte nicht zu laut sein und ein angemessenes Arbeitsklima ermöglichen.
- Die Umgebung sollte ausreichend beleuchtet sein. Das Monitorlicht alleine reicht auf Dauer nicht. Störende Blendungen, Reflexionen oder Spiegelungen sollten vermieden werden.
- Der Monitor sollte so aufgestellt werden können, dass getätigte Eingaben für Dritte nicht einsehbar sind. Für Laptops gibt es Monitorfolien, die eine Einsichtnahme von der Seite verhindern.
- Die Umgebung sollte außerdem gewährleisten, dass die mobilen IT-Systeme nicht beeinträchtigt werden, sie sollte also nicht zu feucht, zu kalt oder zu warm sein. Der Mitarbeiter wird zwar solche Bedingungen auch um seines eigenen Wohlbefindens willen meiden, während er die Geräte benutzt. Damit die Geräte aber auch entsprechend geeignet aufbewahrt werden, sollten Regelungen festgelegt sein.
- Mobile Geräte sollten bei erhöhtem Schutzbedarf gegen Diebstahl geschützt werden (siehe auch INF.9.M10 *Einsatz von Diebstahlsicherungen*). Die Umgebung sollte hierfür die notwendigen Voraussetzungen bieten. Es muss zum Beispiel möglich sein, das Kabelschloss an einen festen Gegenstand anzuschließen, um den befestigen Laptop gegen eine einfache Wegnahme zu sichern. Wenn möglich, sollten Fenster und Türen des mobilen Arbeitsplatzes ge- und verschlossen werden, wenn der Mitarbeiter den Raum verlässt. Das ist beispielsweise bei Hotelzimmern oder Besprechungsräumen oft möglich.

In fremden Umgebungen wie Hotels ist es auch empfehlenswert, sich über das richtige Verhalten bei Bränden oder anderen Notfällen zu informieren, zum Beispiel über Warntöne und Fluchtwege.

INF.9.M2 Regelungen für mobile Arbeitsplätze [Benutzer, Leiter IT]

Für alle Arbeiten unterwegs ist zu regeln, welche Informationen (Akten, Datenträger, IT-Systeme) außerhalb des Unternehmens bzw. der Behörde transportiert und bearbeitet werden dürfen und welche Schutzvorkehrungen dabei zu treffen sind.

IT-Systeme und Datenträger, die außerhalb der eigenen Institution eingesetzt werden, sind eher Risiken ausgesetzt, als solche, die sich innerhalb geschützter Räumlichkeiten befinden. Deswegen müssen folgende Punkte geregelt werden:

- Die Benutzer müssen darüber informiert sein, welche Informationen mit mobilen IT-Systemen unterwegs verarbeitet werden dürfen. Die Daten sollten dementsprechend klassifiziert sein, um den Benutzern Einschränkungen transparent zu machen. Dienstgeheimnisse dürfen nur dann auf mobilen IT-Systemen verarbeitet werden, wenn hierfür geeignete und freigegebene Sicherheitsmechanismen eingesetzt werden.
- IT-Systeme oder Datenträger, die vertrauliche Informationen enthalten, sollten möglichst komplett verschlüsselt werden. Wenn IT-Systeme eine Verschlüsselungsfunktion ohne weitere Hilfsmittel ermöglichen, ist es empfehlenswert, dass diese Funktionen immer genutzt werden. Dies gilt auch dann, wenn lediglich wenig vertrauliche Daten auf den IT-Systemen enthalten sind. Informationen, die ein hohes Maß an Sicherheit verlangen (zum Beispiel Angebote, Konstruktionsdaten, Wirtschaftsdaten der Institution) sollten stets verschlüsselt auf dem mobilen IT-System abgelegt werden.
- Beim Einsatz mobiler IT-Systeme ist zu klären, ob mobile Mitarbeiter von unterwegs auf interne Daten ihrer Institution zugreifen dürfen. Ist dies vorgesehen, muss der Zugriff angemessen geschützt werden.
- Es muss geklärt werden, ob mobile IT-Systeme auch für private Zwecke benutzt werden dürfen, beispielsweise für die private Kommunikation oder Computerspiele.
- Die Benutzer sollten darauf hingewiesen werden, wie sie sorgfältig mit den mobilen IT-Systemen und Datenträgern umgehen sollten, um einem Verlust oder Diebstahl vorzubeugen und eine lange Lebensdauer zu gewährleisten. Zu diesen Maßnahmen zählen die sorgsame Aufbewahrung außerhalb von Büro- oder Wohnräumen und das Beachten der Empfindlichkeiten gegenüber zu hohen oder zu niedrigen Temperaturen.
- Die Verwaltung, Wartung und Weitergabe von mobilen IT-Systemen und Datenträgern sollte geregelt werden.
- Wechseln die Benutzer, müssen alle benötigten Passwörter gesichert weitergegeben werden.
- IT-Systeme und Datenträger müssen stets sicher aufbewahrt werden. Bei Dienstreisen sollten sie nicht unbeaufsichtigt gelassen werden. Insbesondere sollten sie nicht in Fahrzeugen zurückgelassen werden.
- IT-Systeme wie Laptops, Tablets oder Smartphones und deren Anwendungen können im Allgemeinen durch PINs oder Passwörter abgesichert werden. Diese Mechanismen sollten prinzipiell genutzt werden.
- Es sollte protokolliert werden, wann und von wem, welche IT-Komponenten außer Haus eingesetzt wurden.
- Es sollte geregelt werden, wie mobile IT-Systeme oder Datenträger zu entsorgen sind (siehe INF.9.M6 *Entsorgung von vertraulichen Informationen*).

Zusätzlich sollte für die Benutzer ein kurzes und übersichtliches Merkblatt über die sichere Nutzung von mobilen IT-Systemen erstellt werden.

Mobile IT-Systeme sollten möglichst nicht unbeaufsichtigt bleiben. Falls ein mobiles IT-System in einem Kraftfahrzeug zurückgelassen werden muss, sollte es von außen nicht für Dritte sichtbar sein. Da ein sichtbares mobiles IT-System einen Wert darstellt, der potenzielle Diebe anlocken könnte, sollten diese generell abgedeckt oder im Kofferraum eingeschlossen werden.

Werden mobile IT-Systeme in fremden Büroräumen benutzt, sind auch die geltenden Sicherheitsregelungen der besuchten Institution zu beachten.

In Räumlichkeiten außerhalb der eigenen Institution, wie beispielsweise Hotelzimmern, sollten mobile IT-Systeme nicht ungeschützt liegen. Auch sollten alle Passwort-Schutzmechanismen aktiviert werden. Wenn möglich, sollten IT-Geräte in einem Schrank oder Rollcontainer eingeschlossen werden, um Gelegenheitsdiebe zu behindern.

Mitnahme mobiler IT

Weiterhin muss die Mitnahme von Datenträgern und IT-Komponenten klar geregelt werden. Dabei muss festgelegt werden,

- welche IT-Komponenten beziehungsweise Datenträger außer Haus mitgenommen werden dürfen,
- wer IT-Komponenten beziehungsweise Datenträger außer Haus mitnehmen darf,
- welche grundlegenden Sicherheitsmaßnahmen dabei beachtet werden müssen (beispielsweise Virenschutz, Verschlüsselung vertraulicher Daten, Aufbewahrung).

Die Art und der Umfang der anzuwendenden Sicherheitsmaßnahmen für extern eingesetzte IT-Komponenten hängen einerseits vom Schutzbedarf der darauf gespeicherten Anwendungen und Daten ab und sind andererseits abhängig von der Sicherheit der Einsatz- beziehungsweise Aufbewahrungsorte.

Grundsätzlich sollte für alle IT-Komponenten, die extern eingesetzt werden sollen, eine entsprechende Genehmigung eingeholt werden.

Es sollte möglichst stichprobenartig überprüft werden, ob die Regelungen für die Mitnahme von Datenträgern und IT-Komponenten eingehalten werden. Das bietet sich vor allem bei größeren Institutionen an, bei denen der Zutritt zu den Liegenschaften durch Pförtner beziehungsweise Sicherheitsdienste kontrolliert wird.

Sensibilisierung der Benutzer

Je kleiner und leichter IT-Systeme werden, desto leichtfertiger wird erfahrungsgemäß damit umgegangen. Daher sollten Mitarbeiter für den Wert mobiler IT-Systeme und den Wert der darauf gespeicherten Informationen sensibilisiert werden. Da es bei mobilen IT-Systemen eine große Bandbreite von Varianten und Kombinationsmöglichkeiten gibt, sollten sie vor allem über die spezifischen Gefährdungen und Maßnahmen der von ihnen benutzten Geräte aufgeklärt werden. Das kann sowohl Smartphones als auch Tablets oder Laptops mit ihren jeweils unterschiedlichen Schnittstellen betreffen.

Die Mitarbeiter sollten auch darüber aufgeklärt werden, dass sie vertrauliche Informationen unterwegs nicht mit jedem austauschen und unterwegs auch nicht in Hör- und Sichtweite von Externen darüber sprechen sollten. Insbesondere sollte die Identität jedes Kommunikationspartners vor detaillierten Auskünften hinterfragt werden. Die Sensibilisierung der Benutzer sollte im Rahmen der Bausteinanforderungen von *ORP.3 Sensibilisierung und Schulung zur Informationssicherheit* erfolgen.

INF.9.M3 Zutritts- und Zugriffsschutz [Mitarbeiter]

Fenster und nach außen gehende Türen (zum Beispiel Balkone, Dachterrassen) müssen in Zeiten, in denen ein Raum nicht besetzt ist, geschlossen werden. Auch Außentüren sind abzuschließen. Im Keller- und Erdgeschoss und, je nach Fassadengestaltung, auch in den höheren Etagen, bieten offene Fenster und Türen Einbrechern ideale Einstiegsmöglichkeiten, die auch während der Betriebszeiten eines mobilen Arbeitsplatzes genutzt werden. Daher ist es notwendig Mitarbeiter darauf hinzuweisen, dass Fenster und Türen zu schließen sind, wenn die Räume verlassen werden.

Die Türen nicht besetzter Räume sollten abgeschlossen werden. Dadurch wird verhindert, dass Unbefugte auf darin befindliche Unterlagen und IT-Einrichtungen zugreifen können. Einzelne Büroräume abzuschließen, ist insbesondere dann wichtig, wenn sich diese in Bereichen mit Publikumsverkehr befinden oder der Zutritt nicht durch andere Maßnahmen kontrolliert wird. Türen müssen nicht abgeschlossen werden, wenn diese flurseitig über einen Blindknauf verfügen. Voraussetzung hierfür ist allerdings, dass die befugten Mitarbeiter ihren Schlüssel stets mit sich führen.

Wird während der normalen Arbeitszeiten sichergestellt, dass die Räume nur kurzzeitig leer stehen, kann von einer zwingenden Regelung für Büroräume sowie für Besprechungs-, Veranstaltungs- und Schulungsräumen unter Umständen abgesehen werden.

In Besprechungs-, Veranstaltungs- und Schulungsräumen gibt es meistens keine Möglichkeit, Unterlagen, IT-Systeme und Ähnliches gesondert einzuschließen. Daher sollte es möglich sein, solche Räume zumindest dann, wenn alle Teilnehmer einer Veranstaltung den Raum verlassen, abzuschließen oder ihn durch einen internen Mitarbeiter beaufsichtigen zu lassen.

In manchen Fällen, zum Beispiel in Großraumbüros, können die Türen nicht abgeschlossen werden. Dann sollte alternativ jeder Mitarbeiter vor seiner Abwesenheit seine Unterlagen (gemäß der Clean-Desk-Politik) und den persönlichen Arbeitsbereich verschließen. Dazu zählen beispielsweise der Schreibtisch, Schrank, Client, Laptop und das Telefon.

Türen müssen nicht abgeschlossen werden, wenn keine schutzbedürftigen Gegenstände wie Unterlagen oder Datenträger offen ausliegen und keine unbefugten Zugriffe auf die IT-Systeme im Raum (und die damit vernetzten IT-Systeme) möglich sind.

Bei laufendem Rechner müssen Türen nicht abgeschlossen werden, wenn Zugriffe nur nach erfolgreicher Authentisierung möglich sind, also zum Beispiel ein passwortunterstützter Sperrbildschirm aktiviert ist. Bei ausgeschaltetem Rechner kann darauf verzichtet werden, den Raum zu verschließen, wenn beim Booten des Rechners ein Passwort eingegeben werden muss. Die gleiche Funktion erfüllen Zugangsmechanismen, die auf Token oder Chipkarten basieren.

Der aufgeräumte Arbeitsplatz

Jeder Mitarbeiter sollte dazu angehalten werden, seinen Arbeitsplatz aufgeräumt zu hinterlassen. Die Benutzer müssen dafür sorgen, dass Unbefugte keinen Zugang zu Anwendungen oder Zugriff auf Daten erhalten. Alle mobilen Mitarbeiter müssen sicherstellen, dass keine vertraulichen Informationen frei zugänglich sind und die Verfügbarkeit, Vertraulichkeit oder Integrität von Daten nicht negativ beeinflusst werden kann. Es darf nicht möglich sein, dass Unbefugte auf Datenträger oder Unterlagen zugreifen können.

Für eine kurze Abwesenheit während der Arbeitszeit ist es ausreichend:

- den Raum, sofern möglich, zu verschließen.
- den Bildschirm so zu sperren, dass Zugriffe nur nach erfolgreicher Authentisierung möglich sind.

Bei geplanter Abwesenheit eines Mitarbeiters (zum Beispiel längere Besprechungen, Dienstreisen, Urlaub, Fortbildungsveranstaltungen) ist der Arbeitsplatz so aufzuräumen, dass keine schutzbedürftigen Datenträger oder Unterlagen unverschlossen am Arbeitsplatz zurückgelassen werden. Dafür benötigen die Mitarbeiter ausreichend dimensionierte und verschließbare Staumöglichkeiten, wie zum Beispiel stabile Schränke.

Auch Passwörter dürfen auf keinen Fall sichtbar aufbewahrt werden. Klebezettel am Monitor oder an einem leicht zu erratenden Ort wie zum Beispiel unter der Schreibtischauflage oder in der unverschlossenen Schreibtischschublade sind ungeeignet. Ebenfalls sollten eindeutige Hinweise für das schnelle Erraten ausgeschlossen werden. Daher sollten die Passwörter keine Namen von Familienangehörigen enthalten. Trivialpasswörter wie aufeinanderfolgende Buchstaben und Zahlen sind ebenfalls zu vermeiden.

Die allgemeinen Arbeitsplatzanforderungen sind im Baustein INF.8 *Häuslicher Arbeitsplatz* beschrieben und sollten beachtet werden.

INF.9.M4 Arbeiten mit fremden IT-Systemen [Benutzer, Vorgesetzte]

Häufig ist es erforderlich, unterwegs mithilfe fremder IT-Systeme auf digitale Informationen zugreifen zu können. Zum Beispiel ist das notwendig, um Terminkalender abzugleichen, E-Mails zu verschicken oder einzelne Dateien abzurufen. Hierfür ist es meist das einfachste, fremde IT-Systeme oder Kommunikationsanbindungen zu benutzen, also beispielsweise:

- aus einem Internet-Café,
- in einem Büro der besuchten Institution oder
- über einen WLAN-Hotspot im Hotel, im Zug oder am Flughafen.

Hierbei sollte sich aber jeder Benutzer darüber im Klaren sein, dass es sich um fremd-administrierte IT handelt und daher zusätzliche Sicherheitsmaßnahmen zu ergreifen sind. Daher sollte immer davon ausgegangen werden, dass das Sicherheitsniveau der fremden IT-Umgebung nicht bekannt ist und damit als niedrig eingeschätzt werden muss. Jeder Mitarbeiter sollte wissen, dass fremde Rechner und fremde IT-Umgebungen grundsätzliche höhere Sicherheitsrisiken darstellen. Selbst wenn das Sicherheitsniveau einen ausgezeichneten Eindruck macht, kann dies ein Trugschluss sein.

Daher sollten Benutzer folgende Empfehlungen beachten, bevor sie mit fremden IT-Systemen arbeiten oder Dienstleistungsangebote nutzen:

- Sie sollten sich über vorhandene Sicherheitsmaßnahmen informieren.
- Sie sollten sich genau überlegen, wie sie mit fremden IT-Systemen arbeiten. Sie sollten sich dabei an den Vorgaben und Regelungen für mobile Arbeitsplätze orientieren und fremde IT-Systeme oder Dienstleistungsangebote nicht für alle denkbaren Aktionen und Daten benutzen.
- Sobald die Arbeit beendet wurde, sollten bei einem fremden Rechner grundsätzlich alle währenddessen entstandenen temporären Daten gelöscht werden. Das ist allerdings meistens nicht einfach, da bei vielen Betriebssystemen temporäre Daten an vielen Stellen entstehen. Außerdem kann es bei fremden IT-Systemen auch vorkommen, dass die Zugriffsrechte es nicht zulassen, dass die entstandenen Daten gelöscht werden. Zumindest sollte der Zwischenspeicher (Cache) gelöscht werden.
- Auf keinen Fall sollten Browser-Funktionen zur Auto-Vervollständigung von Benutzernamen und Passwörtern genutzt werden, damit nachfolgende Benutzer sich nicht einfach unter diesem Benutzernamen irgendwo anmelden können.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Mobiler Arbeitsplatz".

INF.9.M5 Zeitnahe Verlustmeldung [Mitarbeiter]

Mitarbeiter müssen ihrer Institution umgehend melden, wenn Dokumente, IT-Systeme oder Datenträger verloren oder gestohlen wurden. Hierfür muss es klare Meldewege und Ansprechpartner innerhalb der Institution geben. Das gilt auch für private Geräte, die dienstlich genutzt werden.

Auf Laptops, Smartphones, Tablets, PDAs und ähnlichen Geräten, aber auch auf mobilen Datenträgern wie USB-Sticks können sich vertrauliche Daten befinden, nach deren Verlust umgehend gehandelt werden muss, beispielsweise:

- Zugangsdaten wie Passwörter: Alle Zugangsdaten der betroffenen IT-Systeme müssen umgehend geändert werden.
- Als vertraulich eingestufte Informationen (z. B. Patientenakten): Alle betroffenen Bereiche (z. B. Fachabteilung, Kunden etc.) müssen benachrichtigt werden, um entsprechende Maßnahmen ergreifen zu können.

Falls möglich, sollten, nachdem mobile Endgeräte verloren gegangen sind, auch Maßnahmen ergriffen werden, mit denen sich die Geräte sperren, löschen oder lokalisieren lassen. Die meisten Mobile-Device-Management-(MDM)-Lösungen (siehe SYS.3.2.2 *Mobile Device Management*) bieten diese Funktionen an. Dafür sind vorher klare Regeln zu definieren und entsprechende Maßnahmen in Absprache mit dem Benutzer, dessen Endgerät verloren ging, unverzüglich zu ergreifen.

Tauchen verlorene Geräte wieder auf, sollten sie auf eventuelle Manipulationen untersucht werden, z. B. ob Schrauben geöffnet, Siegel entfernt wurden oder sich das Gewicht gegenüber dem Auslieferungszustand geändert hat. Besteht ein Verdacht, sollte das Gerät entweder gleich entsorgt oder von einem Spezialisten weiter untersucht werden. Um sicherzustellen, dass sich keine manipulierte Software auf den wiedererlangten Geräten befindet, müssen diese zumindest neu installiert werden.

INF.9.M6 Entsorgung von vertraulichen Informationen [Haustechnik, Mitarbeiter]

Betriebsmittel oder Sachmittel am häuslichen Arbeitsplatz (z. B. Druckerpapier, USB-Festplatten, DVDs, USB-Sticks, SD-Karten, aber auch spezielle Tonerkassetten) werden irgendwann nicht mehr benötigt oder müssen ausgesondert werden. Wenn sie schützenswerte Daten enthalten, müssen sie so entsorgt werden, dass keine Rückschlüsse auf vorher gespeicherte Daten möglich sind. Bei funktionstüchtigen Datenträgern sollten die Daten sicher gelöscht werden. Nicht funktionierende oder nur einmal beschreibbare Datenträger müssen mechanisch zerstört werden (siehe dazu auch CON.6 *Löschen und Vernichten*).

Die Art der Entsorgung schutzbedürftigen Materials sollte in einer speziellen Sicherheitsrichtlinie geregelt werden. In der Institution müssen die dafür benötigten Entsorgungseinrichtungen vorhanden sein.

Wird vertrauliches Material vor der Entsorgung gesammelt, so ist die Sammlung vor unberechtigtem Zugriff zu schützen.

Die ordnungsgemäße Entsorgung schützenswerter Betriebs- und Sachmittel muss den Anforderungen des Bausteins OPS.1.2.7 Verkauf/Aussonderung von IT entsprechen.

Entsorgung von Datenträgern und Dokumenten auf Reisen

Auch unterwegs gibt es häufig Material, das aus verschiedensten Gründen entsorgt werden sollte. Schon allein die notwendigen Entsorgungen, damit das Reisegepäck tragbar bleibt, müssen in diesem Kontext beachtet werden. Während in der eigenen Institution Entsorgungsverfahren für alte oder unbrauchbare Datenträger und Dokumente existieren, sind diese unterwegs nicht immer möglich. Daher ist vor jeder Entsorgung von ausgedienten Datenträgern und Dokumenten genau zu überlegen, ob diese schützenswerte Informationen enthalten könnten. Ist das der Fall, müssen die Datenträger und Dokumente im Zweifelsfall wieder mit zurücktransportiert werden. Das gilt auch, wenn die Datenträger defekt sind, da IT-Experten auch hieraus noch wertvolle Informationen zurückgewinnen können. Ebenso ist bei Einrichtungen zur Datenvernichtung in fremden Institutionen Vorsicht geboten, da hier nicht unbedingt ersichtlich ist, wer die Entsorgung durchführt beziehungsweise wie zuverlässig sie ist.

Die Anforderungen an die Entsorgung von Datenträgern und Dokumenten sind im Baustein OPS.1.2.7 *Verkauf/Aussonderung von IT* abgebildet. Sie sollten generell bei der Gestaltung der Sicherheitsrichtlinien und Regelungen zum Informationsschutz im Themenkomplex Entsorgung von Datenträgern und Dokumenten einbezogen werden.

INF.9.M7 Rechtliche Rahmenbedingungen für das mobile Arbeiten [Leiter Personal, Personalabteilung]

Institutionen müssen verschiedene arbeitsrechtliche und arbeitsschutzrechtliche Rahmenbedingungen für das mobile Arbeiten beachten und festlegen. Strittige Punkte sollten entweder durch Betriebsvereinbarungen oder durch zusätzlich zum Arbeitsvertrag getroffene individuelle Vereinbarungen zwischen dem mobilen Mitarbeiter und dem Arbeitgeber geklärt werden. In diesen Vereinbarungen sind beispielsweise folgende Punkte zu regeln:

- Freiwilligkeit der Teilnahme an der mobilen Arbeit
- Mehrarbeit und Zuschläge
- Aufwendungen für Fahrten zwischen Betrieb, häuslicher Wohnung, Kunden
- Aufwendungen zum Beispiel für Strom, Heizung, Miete
- Haftung (bei Diebstahl oder Beschädigung der IT, aber auch bei Arbeitsunfall oder Berufskrankheit)
- Beendigung der mobilen Arbeit

INF.9.M8 Sicherheitsrichtlinie für mobile Arbeitsplätze [Leiter IT]

Die für die mobile Arbeit notwendigerweise umzusetzenden Sicherheitsmaßnahmen für den Umgang mit Informationen und mit der Informations- und Kommunikationstechnik, sind zusätzlich in einer Sicherheitsrichtlinie für das mobile Arbeiten zu dokumentieren.

Folgende Aspekte sollten darin beachtet werden:

Arbeitszeitregelung: Es sollte geregelt sein, wie die Arbeitszeiten auf Tätigkeiten innerhalb und außerhalb der Institution verteilt sind. Ebenso sollten feste Zeiten festgelegt werden, an denen der Mitarbeiter erreichbar ist (siehe INF.M7 *Rechtliche Rahmenbedingungen für das mobile Arbeiten*).

Reaktionszeiten: Es sollte geregelt sein, in welchen Abständen die mobilen Mitarbeiter aktuelle Informationen abrufen (zum Beispiel wie häufig E-Mails gelesen werden) und in welchem Zeitraum sie darauf zu reagieren haben.

Vertretungsregelung: Für jeden mobilen Mitarbeiter sollte ein Vertreter bestimmt werden, der über die laufenden Aktivitäten informiert sein muss, damit er auch kurzfristig die Vertretung übernehmen kann. Dazu müssen die Arbeitsergebnisse durch die mobilen Mitarbeiter immer sorgfältig dokumentiert werden. Eventuell sind sporadische oder regelmäßige Treffen zwischen dem mobilen Mitarbeiter und seinem Vertreter sinnvoll. Ergänzend muss geregelt werden, wie der Vertreter im unerwarteten Vertretungsfall auf die Daten auf den IT-Systemen und Anwendungen zugreifen kann oder die vorhandenen Unterlagen am mobilen Arbeitsplatz einsehen kann. Dieser Vertretungsfall sollte probeweise durchgespielt und ausgewertet werden. Die Auswertung sollte durch den mobilen Mitarbeiter und seine Vertretung erfolgen.

Umgang mit vertraulichen Informationen: Bei der mobilen Arbeit werden Informationen sowohl analog (zum Beispiel auf Papier) als auch digital (zum Beispiel auf Datenträgern) bearbeitet. Unabhängig davon, in welcher Form Informationen vorliegen, müssen sie vor unbefugtem Zugriff und anderen Sicherheitsrisiken geschützt werden. Daher ist der komplette Lebenszyklus schützenswerter Informationen angemessen abzusichern.

Meldeweg: Die mobilen Mitarbeiter sind zu verpflichten, sicherheitsrelevante Vorkommnisse unverzüglich an eine im Vorfeld zu bestimmende Stelle in der Institution zu melden.

Arbeitsmittel: Es sollte festgeschrieben werden, welche Arbeitsmittel die mobilen Arbeiter einsetzen können und welche nicht genutzt werden dürfen (zum Beispiel nicht freigegebene Software). So kann ein E-Mail-Anschluss zur Verfügung gestellt werden, aber die Nutzung von anderen Internet-Diensten untersagt werden. Weiterhin könnte die Nutzung von Datenträgern, wie beispielsweise DVDs oder USB-Sticks untersagt werden, wenn der mobile Arbeitsplatz es nicht erfordert.

Transport von Dokumenten und Datenträgern: Die Art und Absicherung des Transportes von Dokumenten und Datenträgern zwischen mobilen Arbeitsplätzen, Räumlichkeiten von Kunden und der Institution ist zu regeln. Vertrauliche Daten auf digitalen Datenträgern sollten nur verschlüsselt transportiert werden (siehe INF.9.M2 *Regelungen für mobile Arbeitsplätze* und INF.9.M9 *Verschlüsselung tragbarer IT-Systeme und Datenträger*).

Datensicherung: Die mobilen Mitarbeiter sind zu verpflichten, regelmäßige Datensicherungen der lokal gespeicherten Daten durchzuführen. Darüber hinaus sollte vereinbart werden, dass jeweils eine Generation der Datensicherungen in der Institution hinterlegt wird, damit eine höhere Verfügbarkeit gewährleistet ist.

Synchronisation von Datenbeständen: Datenbestände, die sowohl in der Institution als auch an mobilen Arbeitsplätzen bearbeitet werden sollen, müssen geeignet synchronisiert werden. Das Vorgehen bei der Synchronisation muss genau geplant werden, damit es nicht zu Konflikten und damit zu einem Datenverlust kommen kann, wenn zwei Benutzer den gleichen Datensatz in gespiegelten Datenbeständen geändert oder gelöscht haben. Es empfiehlt sich, hierfür geeignete Software einzusetzen.

Datenschutz: Die mobilen Mitarbeiter sind darauf zu verpflichten, einschlägige Datenschutzvorschriften einzuhalten. Sie sind auf die notwendigen Maßnahmen bei der Bearbeitung von personenbezogenen Daten am mobilen Arbeitsplatz und bei Kunden hinzuweisen.

Datenkommunikation: Es sollte festgelegt sein, welche Daten auf welchem Weg übertragen werden sollen und welche Daten nicht oder nur verschlüsselt elektronisch zu übermitteln sind. Ebenso ist zu regeln, welche Dokumente zwischen Institution, mobilem Arbeitsplatz und den Kunden transportiert werden dürfen und wie diese dabei geschützt werden.

Entsorgung: Die Sicherheitsrichtlinie muss Regelungen enthalten, wie Mitarbeiter mit ausgedienten Datenträgern und Dokumenten umgehen sollen. (siehe INF.9.M6 *Entsorgung von vertraulichen Informationen* und *ORP.3 Sensibilisierung und Schulung zur Informationssicherheit*).

Sensibilisierung: Alle Mitarbeiter sollten regelmäßig für den ordnungsgemäßen Umgang mit mobiler IT sensibilisiert werden (siehe INF.9.M2 *Regelungen für mobile Arbeitsplätze*).

Die Regelungen sind jedem mobilen Mitarbeiter auszuhändigen. Entsprechende Merkblätter sind regelmäßig zu aktualisieren.

Informationsschutz auf Geschäfts- und Privatreisen

Mitarbeiter müssen mit vertraulichen Informationen auch auf Geschäfts- oder Privatreisen sorgfältig umgehen. Bei Auslandsreisen sollten daher die Anforderungen des Bausteins CON.6 *Informationssicherheit auf Auslandsreisen* berücksichtigt werden.

INF.9.M9 Verschlüsselung tragbarer IT-Systeme und Datenträger [Benutzer]

Um zu verhindern, dass schützenswerte Informationen durch unberechtigte Dritte eingesehen werden können, sollte sichergestellt werden, dass alle schützenswerten Informationen entsprechend den internen Richtlinien abgesichert sind.

Mobile Datenträger und IT-Systeme sollten nach unternehmensinternen Verfahren und Regelungen verschlüsselt werden, um schützenswerte Daten vor unbefugten Zugriff zu schützen. Dies gilt insbesondere für wiederbeschreibbare Datenträger. Es besteht die Möglichkeit, Datenträger nur partiell zu verschlüsseln. Im Rahmen der Benutzerfreundlichkeit empfiehlt es sich allerdings, den gesamten Datenträger zu verschlüsseln. Eine Verschlüsselung des Datenträgers erreicht man entweder mit Software, wie z. B. BitLocker von Microsoft oder FileVault von Apple, oder auch mit spezieller Hardware. Um die Daten zu entschlüsseln, ist ein kryptographischer Schlüssel notwendig, der in Form einer separaten Chipkarte oder eines USB-Tokens verwendet werden sollte. Hierbei sollte der Benutzer den kryptographischen Schlüssel und den verschlüsselten Datenträger bzw. Client getrennt voneinander aufbewahren.

Zudem ist es wichtig, Vorkehrungen gegen Datenverlust zu treffen, um Fehlfunktionen (z. B. Stromausfall, Abbruch der Verschlüsselung) systemseitig abzufangen. Darüber hinaus sind folgende Anforderungen sinnvoll:

- Der genutzte Verschlüsselungsalgorithmus sollte den Anforderungen der Institution entsprechen.
- Das Schlüsselmanagement muss mit den Funktionen des mobilen IT-Systems harmonisieren.
- Das mobile IT-System muss die sicherheitskritischen Parameter wie Schlüssel sicher verwalten. So dürfen Schlüssel (auch mittlerweile nicht mehr benutzte) nie ungeschützt, das heißt auslesbar oder unverschlüsselt, abgelegt werden. Sie müssen möglichst getrennt vom verschlüsselten Gerät aufbewahrt werden.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

INF.9.M10 Einsatz von Diebstahlsicherungen (CIA)

Diebstahlsicherungen sind überall dort einzusetzen, wo große Werte zu schützen sind beziehungsweise dort, wo andere Maßnahmen nicht umgesetzt werden können. Das trifft zum Beispiel bei Laptops im mobilen Einsatz zu. Diebstahlsicherungen sind außerdem dort sinnvoll, wo Publikumsverkehr herrscht oder die Fluktuation von Benutzern sehr hoch ist. Dabei sollte immer beachtet werden, dass die zu schützenden Werte nur zu einem kleinen Teil aus den Wiederbeschaffungskosten für das Gerät bestehen, sondern bei Laptops und ähnlichen IT-Systemen der Wert der darauf gespeicherten Daten berücksichtigt werden muss.

Arten von Diebstahlsicherungen

Auf dem Markt sind die unterschiedlichsten Diebstahl-Sicherungen erhältlich. Diese können zunächst in mechanische und elektronische Sicherungen unterteilt werden.

Zu den mechanischen Sicherungen gehören unter anderem Kabelsicherungen, Gehäusesicherungen (um das Gehäuse gegen Öffnung zu schützen), Sicherheitsplatten und Sicherheitsgehäuse. Es gibt hier zum einen Hardware-Sicherungen, die dem Diebstahl von IT-Geräten vorbeugen, z. B. indem das Gerät mit dem Schreibtisch verbunden wird. Es gibt zum anderen auch eine Reihe von Sicherungsmechanismen, die verhindern sollen, dass das Gehäuse geöffnet wird. Damit soll vorgebeugt werden, dass Angreifer Teile stehlen oder sicherheitsrelevante Einstellungen manipulieren, wie zum Beispiel Sicherheitskarten entfernen.

Bei der Beschaffung mechanischer Sicherungen ist die Wahl eines guten Schlosses wichtig, das über eine auf die jeweiligen Bedürfnisse abgestimmte Schließanlage verfügt. Je nach Produkt sind verschiedene Schließanlagen möglich:

- gleichschließend: Ein Schlüssel passt zum Beispiel auf alle Gerätesicherungen einer Institution oder Abteilung. Das hat den Vorteil, dass der Aufwand für die Schlüsselverwaltung geringer ist. Es bedeutet jedoch, dass sehr viele gleichartige Schlüssel im Umlauf sein können und dass im Schadensfall häufig keine Beweissicherung möglich ist.
- verschiedenschließend: Jede Gerätesicherung hat einen individuellen Schlüssel. Das hat den Nachteil, dass der Aufwand für die Schlüsselverwaltung höher ist. Es hat aber den Vorteil, dass es weniger Schlüsseldubletten gibt.
- Hauptschlüsselsystem: Jede Gerätesicherung hat einen individuellen Schlüssel, kann zusätzlich aber auch durch einen Hauptschlüssel geöffnet werden. Das hat den Vorteil, dass der Aufwand für die Schlüsselverwaltung geringer ist. Es hat aber den Nachteil, dass solche Systeme teurer in der Anschaffung sind.

Die meisten Notebooks oder einige andere Geräte haben einen kleinen Schlitz, der mit einem Ketten- oder Schloss-Symbol gekennzeichnet ist. Diese kleine Öffnung befindet sich seitlich oder hinten am Gerät. Es gibt eine breite Palette von Kabelsicherungen und anderen Produkten, die diese Öffnung für die Sicherung von Geräten nutzt.

Bei Kabelsicherungen muss dann nur eine Kabelschlinge um ein solides Objekt in der Nähe des Gerätes gelegt werden. Anschließend wird das zugehörige Schloss durch die entstandene Lasche gezogen und abgeschlossen. Für Geräte, die diese Öffnung nicht haben oder bei denen sie nicht widerstandsfähig genug ist, gibt es Sicherungsprodukte, bei denen eine stabile Platte auf das Gerät geklebt wird. An dieser wird dann das Sicherungskabel befestigt.

Daneben gibt es elektronische Sicherungen, die beispielsweise einen akustischen Abschreckungs-Alarm am Gerät selber auslösen, der potenzielle Diebe dazu bringen soll, das Gerät liegenzulassen.

Bei Neuanschaffung von IT-Geräten sollte darauf geachtet werden, dass sie Ösen am Gehäuse besitzen, um sie an anderen Gegenständen befestigen zu können.

INF.9.M11 Verbot der Nutzung unsicherer Umgebungen (CIA)

Um die Gefährdungen und Sicherheitslücken bei erhöhtem Schutzbedarf zu minimieren, sollten Mindestkriterien für die Arbeitsumgebung festgelegt werden. Diese sollten vorwiegend die sichere mobile Verarbeitung von Informationen mit erhöhtem Schutzbedarf gewährleisten.

Die Mindestkriterien sollten dabei die folgenden Themenbereiche abdecken:

Einsicht und Zugriff durch Dritte: Es ist sicherzustellen, dass Bildschirminhalte und Ausdrucke möglichst nicht durch Dritte mitgelesen werden. Vor allem Zubehörteile wie Blickschutzfolien können es Dritten erschweren, Bildschirminhalte einzusehen. Da der Zugriff auf vertrauliche Informationen durch unbefugte Personen generell verhindert werden sollte, sind auch die Anforderungen der Maßnahme INF.9.M10 *Einsatz von Diebstahlsicherungen* zu berücksichtigen.

Geschlossene, abschließbare oder bewachte Räume: Je nach Schutzbedarf der Informationen sollten die Informationen entweder in geschlossenen, abschließbaren oder bewachten Räumen aufbewahrt werden. Falls mehrere Optionen zur Auswahl stehen, sollte bei erhöhtem Schutzbedarf immer die Option mit dem größtmöglichen Schutz ausgewählt werden.

Gesicherte Kommunikationsmöglichkeiten (IT / Telefon): Die Kommunikationsmöglichkeiten beim mobilen Arbeiten sollten immer entsprechend dem Schutzbedarf abgesichert werden. Sicherheitslösungen durch ein Virtual Private Network (VPN) oder Mobile Device Management (MDM) sollten daher angemessen auf das mobile Arbeiten bei erhöhtem Schutzbedarf abgestimmt sein. Ebenso sollte bei einer etablierten VPN-Lösung auch der Baustein NET.4.2 *VoIP* beachtet werden, um entsprechend den dort genannten Anforderungen sichere Vorgaben für mobile Endgeräte erstellen zu können. Die für das mobile Arbeiten prinzipiell notwendigen Kommunikationsbausteine befinden sich in den Schichten SYS.3 *Mobile Devices* und NET (*Netze und Kommunikation*). Sofern bestimmte Kommunikationsmöglichkeiten einem Outsourcing-Verhältnis unterliegen, sind auch die Anforderungen aus der Schicht OPS.2 *IT-Betrieb von Dritten* zu berücksichtigen.

Ausreichende Stromversorgung: Für die Arbeitsdauer mit mobilen Endgeräten ist immer die Stromversorgung zu gewährleisten. Daher sollten die Benutzer auch mit geeigneten Netzteilen für die Geräte ausgestattet sein. Gerade bei häufigen Reisen bieten sich zusätzliche Akkumulatoren an, die eine längere Stromversorgung garantieren. Für die Benutzung von Powerbanks sollte die Institution spezielle Regelungen festlegen, die dem jeweiligen Schutzbedarf entsprechen. Das ist notwendig, da Powerbanks die gleichen Sicherheitslücken aufweisen, wie normale USB-Sticks. Daher sollten möglichst nur geprüfte und abgesicherte Powerbanks der Institution durch die Benutzer verwendet werden.

3 Weiterführende Informationen

3.1 Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2 Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Mobiler Arbeitsplatz" finden sich unter anderem in folgenden Veröffentlichungen:

[27001A6.2.1] ISO/IEC 27001:2013

Information technology - Security techniques - Information security management systems - Requirements, insbesondere Annex A, A.6.2.1 Mobile device policy, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/SC 27, Oktober 2013

[ISFPA2] Standard of Good Practice for Information Security

Area PA2 Mobile Computing, Information Security Forum (ISF), June 2018

[NIST80046] Guide to Enterprise Telework, Remote Access and Bring Your Own Device (BYOD) Security

NIST Special Publication 800-46, Revision 2, Juli 2016, http://dx.doi.org/10.6028/NIST.SP.800-46r2, zuletzt abgerufen am 05.10.2018

INF: Infrastruktur

Umsetzungshinweise zum Baustein INF.10 Besprechungs-, Veranstaltungs- und Schulungsräume

1 Beschreibung

1.1 Einleitung

In der Regel hat jede Institution einen oder mehrere Räume, in denen Besprechungen, Schulungen oder sonstige Veranstaltungen durchgeführt werden können. Hierfür sind oft speziell ausgestattete Räume vorgesehen. Besprechungs-, Veranstaltungs- und Schulungsräume zeichnen sich im Wesentlichen dadurch aus, dass sie von wechselnden Personen bzw. Personenkreisen, Personal und Besuchern genutzt werden. Dauerhaft werden sie vom gleichen Personenkreis meist nur kurze Zeit genutzt. Mitgebrachte IT-Systeme werden dabei häufig gemeinsam mit Geräten der Institution betrieben, wie fremde Laptops an fest verbauten Beamern. Aus diesen unterschiedlichen Nutzungsszenarien heraus ergibt sich eine Gefährdungslage, die kaum mit denen anderer Räume vergleichbar ist.

1.2 Lebenszyklus

Planung und Konzeption

Die Nutzungsmöglichkeiten von Besprechungs-, Veranstaltungs- und Schulungsräumen variieren sehr stark. Da hiervon auch die erforderlichen Sicherheitsmaßnahmen abhängen, sollte zunächst eine Nutzungsübersicht erstellt werden, in der die geplanten Einsatzszenarien berücksichtigt werden (siehe INF.10.M1 *Sichere Nutzung von Besprechungs, Veranstaltungs- und Schulungsräumen*).

Basierend auf dem Nutzungskonzept sollten geeignete Räumlichkeiten ausgewählt und ausgestattet werden (siehe INF.10.M4 *Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen).*

Wenn auf das LAN oder das Internet zugegriffen werden soll, müssen die entsprechenden Zugänge zu den Datennetzen in Besprechungs-, Veranstaltungs- und Schulungsräumen sorgfältig abgesichert werden (siehe INF.10.*Einrichtung sicherer Netzzugänge*).

Umsetzung

Es müssen Regeln für die Sicherheit in Besprechungs-, Veranstaltungs- und Schulungsräume festgelegt sowie technisch und organisatorisch umgesetzt werden. Alle Mitarbeiter müssen darüber informiert werden, welche Regeln für die Nutzung zu beachten sind (siehe INF.10.M1 *Sichere Nutzung von Besprechungs-, Veranstaltungs- und Schulungsräumen* und *INF.10.M8 Erstellung eines Nutzungsnachweises für Räume*).

Betrieb

Auch in Besprechungs-, Veranstaltungs- und Schulungsräumen muss mit den Einrichtungen und der vorhandenen Technik sorgfältig umgegangen werden. Dazu gehören die Einhaltung der von der Institution vorgesehenen Regelungen über die Arbeitsumgebung und eine sichere Aufbewahrung der Arbeitsmaterialien (siehe INF.10.M1 *Sichere Nutzung von Besprechungs-, Veranstaltungs- und Schulungsräumen).*

Aussonderung

Gerade in Besprechungs-, Veranstaltungs- und Schulungsräumen mit häufig wechselnden Benutzern ist es wichtig, Arbeitsmaterialien wie Datenträger und Papiere sorgsam zu entsorgen und nicht einfach liegen zu lassen *(*siehe INF.10.M1 *Sichere Nutzung von Besprechungs-, Veranstaltungs- und Schulungsräumen).*

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Besprechungs-, Veranstaltungs- und Schulungsräume" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

INF.10.M1 Sichere Nutzung von Besprechungs-, Veranstaltungs- und Schulungsräumen [Haustechnik, Leiter IT]

Für die Nutzung dieser Räume und die darin vorhandene Technik sollte es in jeder Institution feste Regeln geben. Diese sollten unter anderem Verhaltenshinweise genereller Art für die Benutzer umfassen, aber auch solche, um fest installierte sowie mitgebrachter Geräte, Datenträgern und Arbeitsmaterialien benutzen zu können. Es muss geklärt werden, unter welchen Rahmenbedingungen Externe mitgebrachte IT-Systeme, wie Mobiltelefone und Laptops, einsetzen dürfen. Vorhandene Festnetz-Telefonanschlüsse müssen vor Missbrauch geschützt werden, beispielsweise indem externe Nummern nur angewählt werden können, nachdem ein geeignetes Passwort eingegeben wurde. Im Raum sollten die Telefonnummern von Ansprechpartnern für Probleme, wie IT-Support oder zur Schlüsselverwaltung, ausgehängt oder ausgelegt sein. Die Ansprechpartner müssen jederzeit während der üblichen Bürozeiten erreichbar sein. Wenn im Raum Beamer und weitere Geräte fest eingerichtet sind, müssen erforderliche Sicherheitsmaßnahmen zum Schutz dieser Geräte vor Diebstahl getroffen werden. Beispielsweise können diese mit Diebstahlsicherungen, wie Stahlkabel, versehen werden. Auch verschließbare Schränke für Materialien sind sinnvoll. Nach Ende jeder Veranstaltung sollten die Materialien entfernt werden, die vertrauliche Informationen enthalten könnten. Daher sollte z. B. benutztes Flipchart-Papier mitgenommen und die Tafeln gesäubert werden. Auch im Papierkorb entsorgte vertrauliche Entwürfe dürfen nicht vergessen werden. Werden die Räume verlassen, sollten Materialien in Schränken verschlossen und der Raum an sich verschlossen werden. Verlassen die Mitarbeiter, die die Besucher beaufsichtigen, den Raum, muss der Besuch von einem anderen internen Mitarbeiter beaufsichtigt werden.

Zudem ist festzulegen, wer für die Administration der vorhandenen Schulungs- und Präsentationsrechner zuständig ist. Außerdem sollten Hinweise auf Fluchtwege und das richtige Verhalten bei Bränden nicht vergessen werden (siehe INF.1. *Allgemeines Gebäude*).

INF.10.M2 Beaufsichtigung von Besuchern [Mitarbeiter]

Personen, die nicht der Institution angehören sollten, außer in Räumen, die ausdrücklich dafür vorgesehen sind, nicht unbeaufsichtigt sein. Wird es erforderlich, einen Externen allein in Besprechungs-, Veranstaltungs- und Schulungsräumen zurückzulassen, sollte der Besucher in der Zeit von einem anderen internen Mitarbeiter beaufsichtigt werden.

INF.10.M3 Geschlossene Fenster und Türen [Mitarbeiter]

Fenster und nach außen gehende Türen (Balkone, Terrassen) müssen in Zeiten, in denen ein Raum nicht besetzt ist, geschlossen werden. Außentüren sollten generell abgeschlossen werden. Im Keller- und Erdgeschoss und, je nach Fassadengestaltung, auch in den höheren Etagen, bieten offene Fenster und Türen Einbrechern ideale Einstiegsmöglichkeiten, die auch während der Betriebszeiten einer Institution missbraucht werden können.

Mitarbeiter sollten darauf hingewiesen werden, dass generell Fenster und in Räumlichkeiten, in denen sich IT-Systeme und sensitive Dokumente befinden, zusätzlich die Türen beim Verlassen abgeschlossen werden müssen.

Brand- und Rauchschutztüren bieten nur im verschlossenen Zustand Schutz und dürfen deshalb keinesfalls durch Keile oder andere Vorrichtungen dauerhaft offen gehalten werden.

Es ist sinnvoll, dass Pförtner oder Mitarbeiter der Haustechnik regelmäßig überprüfen, ob die genannten Regeln eingehalten werden. Es wird empfohlen, die Schlüssel für die Besprechungs-, Veranstaltungs- und Schulungsräume von einer zentralen Stelle zu verwalten (z. B. Pforte oder innerer Dienst).

Gemeinsam mit den Basismaßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich Besprechungs-, Veranstaltungs- und Schulungsraum.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Besprechungs-, Veranstaltungs- und Schulungsräume".

INF.10.M4 Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen

Von der geplanten Nutzung von Besprechungs-, Veranstaltungs- und Schulungsräumen hängt nicht nur die Wahl der Ausstattung, sondern auch die erforderlichen Sicherheitsmaßnahmen ab. Daher sollte zunächst dokumentiert werden, welche Nutzungsarten für welche Räume vorgesehen sind, um basierend auf den Anforderungen aus den geplanten Einsatzszenarien die Einrichtung auszuwählen und organisatorische und technische Nutzungsregelungen festzulegen.

Die Lage von Besprechungs-, Veranstaltungs- und Schulungsräumen sollte möglichst so gewählt werden, dass Fremde nicht unnötig das Haus durchqueren müssen. Der Weg zu einem Besprechungs-, Veranstaltungs- und Schulungsraum sollte möglichst nicht in die Nähe von oder gar durch besonders sicherheitsrelevante Bereiche führen. Ebenso sollten Besprechungs-, Veranstaltungs- und Schulungsräume so ausgewählt und eingerichtet sein, dass sie zu möglichst geringen Störungen des normalen Betriebs führen.

INF.10.M5 Fliegende Verkabelungen

In Besprechungs-, Veranstaltungs- und Schulungsräumen sollten die Stromanschlüsse so verteilt sein, dass sie sich dort befinden, wo auch die IT-Systeme angeschlossen werden können, ohne das Kabel über Boden oder Tische verlegt werden müssen. Sollten dennoch Kabel über Laufwege verlegt werden, sollten diese mit Kabelschächten, Teppichen oder Klebeband abgedeckt bzw. fixiert werden.

INF.10.M6 Einrichtung sicherer Netzzugänge [Leiter IT]

In Besprechungs-, Veranstaltungs- und Schulungsräumen sind einerseits häufig IT-Systeme wie Beamer, Schulungs- oder Präsentationsrechner fest installiert, andererseits werden dorthin auch mobile IT-Systeme wie Laptops mitgebracht. Dabei ist oft auch gewünscht, dass diese IT-Systeme miteinander, mit dem Internet oder dem institutionsinternen Intranet vernetzt werden können.

Da fremde IT-Systeme aber immer als nicht vertrauenswürdig betrachtet werden sollten, sollte eine Anbindung von durch Besucher mitgebrachten IT-Systemen an interne LANs unterbunden werden. Das Datennetz für Besucher sollten von dem der Institution getrennt werden.

Es muss sichergestellt werden, dass Dritte den Datenverkehr bei der LAN-Nutzung durch Mitarbeiter nicht mitlesen bzw. mitschneiden können.

Es sollte darauf verzichtet werden, fremden Mitarbeitern einen Zugang zum Internet anzubieten, der das institutionsinterne Netz als Vermittlungsnetz nutzt. Es kann z. B. aufgrund von Konfigurationsfehlern nie ausgeschlossen werden, dass fremde Mitarbeiter trotz eingeschränkter Zugriffsmöglichkeiten auf schutzwürdige Informationen oder Anwendungen zugreifen können.

Die Stromversorgung in Besprechungs-, Veranstaltungs- und Schulungsräumen sollte aus der Unterverteilung heraus getrennt von den anderen Räumen der Institution aufgebaut werden. Es wird empfohlen jeweils Überspannungsschütze in der Elektro-Unterverteilung zu verbauen und die Stromkreise zu separieren.

INF.10.M7 Sichere Konfiguration von Schulungs- und Präsentationsrechnern [Leiter IT]

Um Sicherheitsprobleme und die unerwünschte Nutzung von dedizierten Schulungs- und Präsentationsrechnern zu vermeiden, sollten die IT-Systeme sicherheitskritisch konfiguriert werden. Dazu gehört:

- Grundinstallation: Nur die notwendigen Pakete sollten eingespielt werden,
- Löschen nicht benötigter Programme: wie beispielsweise Spiele,
- Virenscanner: Es sollten geeignete Produkte installiert werden.

Vor dem Einsatz von Schulungs- und Präsentationsrechnern sollte festgelegt werden, welche Anwendungen und Kommunikationsschnittstellen in der jeweiligen Schulung genutzt werden sollen. Wird vorher eine Standardkonfiguration für die Schulungsrechner festgelegt, kann der Installationsaufwand minimiert und ein Mindestniveau an Sicherheit für die IT-Systeme gewährleistet werden. Vor jeder Schulung muss überprüft werden, ob die IT-Systeme für die Zwecke der Schulung geeignet konfiguriert sind. Um hier auf langwierige Prüfungen verzichten zu können, ist es sinnvoll, Schulungsrechner vor jedem Einsatz über entsprechend vorbereitete Pakete zurückzusetzen (siehe *INF.10.M9 Zurücksetzen von Schulungs- und Präsentationsrechnern*).

Von Schulungsrechnern sollten Informationen, wie Schulungs- oder Prüfungsunterlagen, nicht unkontrolliert kopiert werden können. Zudem sollte es auch nicht möglich sein, zusätzliche Dateien oder Programme aufzuspielen. Daher sollten einerseits Zugriffsrechte für die Benutzer dieser Rechner restriktiv vergeben und andererseits das Überspielen von Daten auf externe Medien verhindert werden.

INF.10.M8 Erstellung eines Nutzungsnachweises für Räume

Für die Räume, in denen Schulungen an IT-Systemen oder besonders vertrauliche Besprechungen stattfinden, sollte ein Nutzungsnachweis erstellt werden. Aus diesem Nachweis sollte hervorgehen, wer die Räume zu welchem Zeitpunkt genutzt hat. Dabei kann ein Raumbuchungssystem hilfreich sein. Mithilfe dieses Raumbuchungssystems kann dann auch eine Überschneidung vermieden werden. Es sollte nachträglich ersichtlich sein, wer die Räume genutzt hat. Ein Nutzungsnachweis kann auch für normale Besprechungsräume von Vorteil sein.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

INF.10.M9 Zurücksetzen von Schulungs- und Präsentationsrechnern [IT-Betrieb] (CA)

Bei IT-Systemen, die von wechselnden Personen genutzt werden, kann es häufiger zu Problemen mit dem Betriebssystem oder den Anwendungen kommen, die nur durch den Leiter der IT wieder behoben werden können. Dies kann z. B. durch Softwarefehler, Konfigurationsänderungen, Aufspielen neuer Software oder Computer-Viren verursacht werden.

Damit die Administratoren bei den oben beschriebenen Problemen auf Schulungs- und Präsentationsrechnern nicht zeitaufwendig nach Fehlern suchen müssen, sollte eine Software-Reinstallation der Standardkonfiguration vorgenommen werden. Dabei ist es hilfreich, wenn sich die Systeme weitestgehend gleichen, zumindest in Bereichen mit ähnlicher Aufgabenstellung.

Eine Software-Reinstallation kann auf verschiedene Weise durchgeführt werden, so gibt es z. B. spezielle Programme, die eine vorgegebene Konfiguration, von einem Server auf den neu zu installierenden Arbeitsplatzrechnern überspielen. Hierbei ist zu beachten, dass solche Arbeiten meist in zweierlei Hinsicht zeitkritisch sind: Die Neueinrichtung sollte möglichst schnell erfolgen können, damit das IT-System wieder verfügbar ist, und das Netz sollte möglichst wenig belastet werden. Dies ist insbesondere bei Schulungsrechnern oder PC-Pools wichtig.

Eine weitere Möglichkeit besteht darin, spezielle Hard- oder Software einzusetzen, die das IT-System nach einem Neustart auf einen definierten Ausgangszustand zurücksetzt und alle durch Benutzer vorgenommenen Änderungen damit verwirft.

INF.10.M10 Mitführungsverbot von Mobiltelefonen (C)

Wenn ausgeschlossen werden soll, dass vertrauliche Besprechungen und Gespräche mit Mobiltelefonen abgehört oder aufgenommen werden, sollten diese nicht in den Gesprächen mitgeführt werden. Es reicht als Schutz nicht immer aus, die Mobiltelefone in den Standby oder Flugmodus zu bringen bzw. auszuschalten. Wenn sie entsprechend manipuliert sind, könnten sie über Funk unbemerkt eingeschaltet werden. Es kann mit einem geeigneten Detektor überprüft werden, ob das Mitführungsverbot eingehalten wird.

3 Weiterführende Informationen

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den Baustein "Besprechungs-, Veranstaltungs- und Schulungsräume" finden sich unter anderem in folgenden Veröffentlichungen:

[27001] ISO/IEC 27001:2013

Information technology-Security techniques-Information security management systems-Requirements, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/SC 27, Oktober 2013

[DIN1627] DIN EN 1627:2011-09 Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchshemmung - Anforderung und Klassifizierung

September 201