Bundesamt
für Sicherheit in der
Informationstechnik

Integration und IT-Revision von Netzübergängen

Teil I: Leitfaden

Version 1.0

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, 53175 Bonn • Postfach 20 03 63, 53133 Bonn
Tel.: + 49 (0) 1888 9582-0 • Fax: + 49 (0) 1888 9582-400 • Internet: www.bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik

Postfach 20 03 63

53133 Bonn

Internet: http://www.bsi.bund.de

Vorwort

Organisationsinterne Netze sind häufig mit externen Netzen – wie beispielsweise dem Internet – verbunden. So genannte Netzübergänge – in Form spezieller Technologien und Systeme – ermöglichen die ungehinderte Datenübertragung zwischen den Netzen. Aber sie unterbinden auch nicht erlaubte Formen der Kommunikation. Das Ziel: die internen Netze vor Angriffen von außen zu schützen.

Das BSI hilft mit diesem Leitfaden IT-Planern und Administratoren ein solches System aus Soft- und Hardwarekomponenten sicher einzurichten. Ein Phasenmodell unterstützt z. B. bei der Erstellung eines Sicherheitskonzepts und geht auf die verschiedenen Sicherheitsanforderungen im Umfeld von Netzwerkübergängen ein. Ist der Übergang in Betrieb, ist es notwendig zu überprüfen, ob das System ordnungsgemäß arbeitet und auf veränderte Anforderungen reagieren kann. Im Mittelpunkt des Leitfadens stehen daher Inhalt und Ablauf einer umfassenden Integration und IT-Revision der Netzübergänge. Unterschiedliche Revisionsmethoden sowie ein strukturiertes Schema von Prüfmodulen werden erläutert. Checklisten, Formblätter und Dokumentationsmuster unterstützen die Verantwortlichen bei der Umsetzung.

Voraussetzung für eine erfolgreiche Revision von Netzübergängen ist jedoch ein auf die jeweiligen Anforderungen zugeschnittenes Sicherheitskonzept! Wo es fehlt, nützen auch Kontrollen wenig.

Bonn, im April 2006

Dr. Udo Helmbrecht, Präsident des BSI

Inhaltsverzeichnis

Einführung

Die Absicherung von IT- und Kommunikationskomponenten z. B. zu externen Geschäftspartnern und Kunden wird immer schwieriger. Die Gründe hierfür sind u. a. die zunehmende Komplexität von IT-Anwendungen und die immer stärkere Vernetzung von IT-Komponenten.

Um das Sicherheitsrisiko, das bei der Verbindung von IT-Netzen mit unterschiedlichem Sicherheitsniveau entsteht, minimal zu halten, ist die sichere Einrichtung (Integration) und der sichere Betrieb von Netzübergängen unerlässlich.

Bei der Integration eines Netzübergangs sind organisatorische und technische Anforderungen zu erfüllen. Diese Anforderungen ergeben sich aus den Sollvorstellungen des Unternehmens oder der Behörde sowie aus den berechtigten Interessen Dritter (z. B. rechtliche Anforderungen) gegenüber der Informationsverarbeitung (Kommunikation) und den IT-gestützten Funktionen.

Die IT-Revision wiederum prüft die Netzübergänge dahingehend, ob Sicherheitsrisiken dadurch entstanden sind, dass es eine Diskrepanz zwischen dem projektierten Soll-Zustand und dem tatsächlichem Ist-Zustand der IT-Netzübergänge gibt.

So genannte **Netzübergänge** verbinden interne Netze mit Fremdnetzen wie z. B. dem Internet. Diese Verbindungen müssen grundsätzlich zwei Funktionen bzw. Ziele erfüllen, die diametral zueinander stehen: Sie müssen Netze verbinden, d. h. festgelegte Formen der Kommunikation ermöglichen. Gleichzeitig müssen sie Netze trennen, also nicht erwünschte Kommunikationsarten zuverlässig unterbinden.

Die verbindende Funktion ist notwendig, um den Austausch von Informationen über festgelegte, eingeschränkte und kontrollierte Kommunikationspfade zu ermöglichen. Die Trennung ist wiederum nötig, wenn die zu verbindenden Netze jeweils unterschiedlichen Schutzbedarf besitzen. Auch bei gleichem Schutzbedarf ist die Einrichtung eines kontrollierten Netzübergangs erforderlich, falls die Verbreitung von sicherheitsrelevanten Informationen auf das jeweilige Teilnetz beschränkt bleiben soll.

Integration eines Netzübergangs bedeutet in dieser Studie die Verbindung mindestens zweier, vorher in den meisten Fällen nicht verbundener Netze durch den Einsatz spezieller Technologien und Systeme. Die Integration von Netzübergängen ist notwendig, um bestimmte Formen der Kommunikation zu ermöglichen, aber gleichzeitig Zugriffsmöglichkeiten in einem angeschlossenen Netz einzuschränken oder zu verhindern.

In diesem Zusammenhang sind drei zentrale Fragen zu klären:

1. Welchen Schutzbedarf haben die Informationen in den – noch getrennten – Netzen? Genauer noch: Wie groß ist der Unterschied zwischen dem erforderlichen Maß an Vertrauen in den verschiedenen Netzen? Dieser Unterschied hat direkte Konsequenzen für die Gestaltung des Netzübergangs: Reicht ein einfacher Paketfilter zur Absicherung aus oder ist eine komplexere Absicherung mit mehreren unterschiedlichen Gerätetypen und möglicherweise sogar eine Aufteilung in mehrere voneinander abgetrennte Netzbereiche notwendig (siehe Teil I, Kapitel 2)?
2. Welcher Kommunikationsbedarf besteht zwischen den Netzen?
   Trotz Trennung und Absicherung der einzelnen Netze ist eine bestimmte Form der Kommunikation gewünscht oder sogar notwendig. Diese ist zu analysieren und hat im Zusammenspiel mit dem festgestellten Schutzbedarf direkte Konsequenzen für die konkrete Gestaltung des Netzübergangs (siehe Teil I, Kapitel 2).
3. Welche gesetzlichen Vorgaben, Vorschriften oder Richtlinien müssen beachtet werden?
   In diesem Zusammenhang stellen u. a. personenbezogene Daten eine zentrale Komponente bei der Konzeption von Netzübergängen dar. Dort können Verbindungsdaten gesammelt und Perso-

nen direkt zugeordnet werden – eine Aufzeichnung und Analyse des Verhaltens von Personen ist also möglich. Diesen Möglichkeiten sind durch Gesetze Grenzen gesetzt. Sie sind außerdem konkreten Randbedingungen unterworfen.

Neben den personenbezogenen Daten stellt die abstrakte Risikoeinschätzung sowie die entsprechende Risikohandhabung bzw. -kontrolle einen weiteren Schwerpunkt bei den gesetzlichen Vorgaben dar. Unter bestimmten Bedingungen sind Firmen verpflichtet, ihre Risiken (hier: IT-Risiken) zu betrachten, auszuwerten und gegebenenfalls zu reduzieren. Einige Gesetze räumen sogar explizit die Möglichkeit der Überprüfung der Risikobetrachtung und -minderung ein.

Ist ein Netzübergang einmal – unter Beachtung aller gegebenen Randbedingungen – integriert und in Betrieb, sollte sichergestellt sein, dass alle Anforderungen auch zukünftig erfüllt und beachtet werden und ggf. auf veränderte Anforderungen reagiert wird.

Um dies sicherzustellen, müssen Überprüfungen auf Einhaltung aller Vorgaben und Anforderungen – also **IT-Revisionen** – stattfinden. Unter Berücksichtigung der Gefahrenpotenziale bei der Netzkopplung ist somit eine regelmäßige sowie bei Verdacht eines Sicherheitsvorfalls eine anlassbezogene Prüfung von Netzübergängen erforderlich.

Bei Revisionen wird zunächst untersucht, welche Anforderungen der Revisionsgegenstand zu erfüllen hat. Dazu gehören interne Vorgaben und Anforderungen wie Sicherheitskonzepte, Sicherheitsleitlinien und Betriebskonzepte. Außerdem ist zu analysieren, ob externe Vorgaben wie Gesetze und Vorschriften für den Gegenstand relevant sind.

Die IT-Revision klärt ab, inwieweit reale Netzübergänge die vorgegebenen und geplanten Sicherheitsfunktionen tatsächlich erbringen und inwieweit sie ausreichend sind. Die Revision vergleicht dabei immer nur das tatsächlich implementierte Sicherheitsniveau mit einer bestehenden Sicherheitsvorgabe (typischerweise das IT-Sicherheitskonzept). Fehlt eine solche Vorgabe, ist dies bereits das erste (schwerwiegende) Defizit. Ein solches Konzept zu erstellen ist hingegen nicht Aufgabe eines Revisors. Die IT-Revision ersetzt also niemals ein Sicherheitskonzept.

Bei der Prüfung eines Netzübergangs erschöpfen sich die Prüfaspekte einer Revision nicht in der Überprüfung der Konfiguration einzelner technischer Komponenten. Vielmehr gehören u. a. zum geordneten Betrieb eines Netzübergangs:

- eine dem Einsatzszenario angemessene sichere Architektur,
- sichere Einzelkomponenten,
- geordnete und wohl definierte Betriebsprozesse sowie
- die ausreichende Dokumentation von Architektur, Konfiguration und Betriebsprozessen.

Alle hier genannten Aspekte sollten im Rahmen einer vollständigen IT-Revision eines Netzübergangs angemessen abgedeckt werden.

Das Resultat dieser Revision sollte dann als Bericht vorliegen und sowohl die maßgeblichen Anforderungen (Soll-Zustand) als auch die tatsächlich vorgefundene Situation (Ist-Zustand) detailliert beschreiben. Darüber hinaus sind Empfehlungen abzugeben, wie vorgefundene Schwächen reduziert werden können. Das Vorgehen bei einer IT-Revision wird im Teil I, Kapitel 3 detailliert dargestellt. Umfassende Checklisten und Vorlagen zur Unterstützung der IT-Revision sind zudem in Teil II „Revisionshilfsmittel“ enthalten.

Der vorliegende Leitfaden hilft somit, das Vorgehen bei der Integration und IT-Revision eines Netzübergangs zu strukturieren. Er richtet sich in erster Linie an Mitarbeiter im Unternehmen bzw. in der Organisation, die für die Integration bzw. IT-Revision von Netzübergängen verantwortlich sind. Der Leitfaden kann aber auch von den Verantwortlichen für die IT-Sicherheit im Unternehmen oder der Organisation dazu genutzt werden, um das Sicherheitsniveau vorhandener oder geplanter Netzübergänge zu prüfen.

Inhaltsübersicht

Die Studie ist wie folgt konzipiert:

- Teil I „Leitfaden“
- Teil II „Revisionshilfsmittel“

Das erste Kapitel von Teil I „Grundlagen“ führt den Begriff „Netzübergang“ ein und erläutert verschiedene Technologien zur Absicherung von Netzübergängen. Wichtige gesetzliche Grundlagen für die Integration und IT-Revision von Netzübergängen werden genannt.

Das zweite Kapitel „Integration von Netzübergängen“ erklärt, was hier unter Integration verstanden werden soll. Es liefert schwerpunktmäßig eine Einführung in typische IT-Sicherheitsfragestellungen bei der Integration von Netzübergängen. Ein Phasenmodell für die Erstellung von Sicherheitskonzepten wird vorgestellt und insbesondere wird auf die verschiedenen Sicherheitsanforderungen in diesem Umfeld eingegangen. Diese Anforderungen bilden eine wesentliche Grundlage für die IT-Revision.

Das dritte Kapitel „IT-Revision“ bildet den Schwerpunkt der Studie. Es befasst sich mit Ablauf und Inhalten einer IT-Revision. Nach der Diskussion unterschiedlicher Revisionsmethoden (Penetrationstest, Compliance Audit, Substantive Audit) wird ein strukturiertes Schema von Prüfmodulen vorgestellt, das die Objekte einer Revision in eine Baumstruktur gliedert. In Form von Prozessdiagrammen wird der organisatorische Ablauf einer generischen IT-Revision detailliert dargestellt. Das schließt ein Rollenmodell und die Aufgabenverteilung aller bei einer Revision typischerweise Beteiligten ein.

Der Anhang des ersten Teils der Studie enthält viele Zusatzinformationen: ein Abkürzungsverzeichnis, ein Glossar, Verzeichnisse von Grafiken und Tabellen, ein Literaturverzeichnis und eine Internet-Linksammlung.

Der zweite Teil der Studie mit dem Titel „Revisionshilfsmittel“ bietet Unterstützung für die IT-Revision in Form konkreter Checklisten, Formblätter und Dokumentationsmuster an.

1 Grundlagen

Im diesem Kapitel werden Grundlagen und Begriffe erläutert, die zum Verständnis der folgenden Kapitel „Integration von Netzübergängen“ und „IT-Revision“ erforderlich sind:

- Abschnitt 1.1 erläutert den Begriff „Netzübergang“ und beschreibt einige Grundtypen für Netzübergänge.
- Abschnitt 1.2 legt die Grundlagen für die Sicherheit von Netzübergängen und beschreibt Basistechnologie für die Netzverkehrfilterung.
- Abschnitt 1.3 beschreibt relevante Gesetze und Vorschriften und deren Bedeutung sowohl für die Integration als auch für den späteren Betrieb und die IT-Revision.

1.1 Kategorien von Netzübergängen

Für die adäquate Absicherung von Netzübergängen ist es laut [BSI-GSHB04] zunächst erforderlich, die unterschiedlichen Netzarten zu bestimmen. Dies erfolgt durch die Festlegung von Sicherheitseinstufungen auf der Basis des Schutzbedarfs der Netze. Dieser Schutzbedarf ergibt sich als Konsequenz aus dem Schutzbedarf der dort gespeicherten oder transportierten Daten.

Hier sind zunächst drei Kategorien zu unterscheiden:

- **Netze mit hohem Schutzbedarf** wie interne Produktivnetze.
  Hier kann es intern Abstufungen des Schutzbedarfs geben, z. B. bei der Bewertung des Rechenzentrumsnetzes oder der Netze für die Bürokommunikation.
- **Netze mit mittlerem Schutzbedarf** wie DMZ (demilitarisierte Zone).
  Oft werden in der demilitarisierten Zone Server platziert, die öffentlich zugänglich sein sollen, jedoch nicht die Sicherheit des internen Netzes kompromittieren dürfen.
- **Netze ohne Schutzbedarf** oder Netze, die nicht unter zentraler Kontrolle stehen, wie das Internet.

Netze können entweder unter eigener Kontrolle (z. B. für die Bereitstellung eigener Web-Angebote oder Remote Access Zugänge) oder unter fremder Kontrolle stehen (z. B. ein Netzzugang für Fremdfirmen zu Support-Zwecken). Dies kommt am häufigsten bei Netzen mit mittlerem Schutzbedarf vor. Netze mit hohem Schutzbedarf erlauben in der Regel keinen Zugriff von Externen.

Zusätzlich zum Schutzbedarf liegen wesentliche Unterschiede im Bereich des Kommunikationsbedarfs. Während bei der Absicherung von Internet-Zugängen die Kommunikation über Standard-Internetanwendungen im Vordergrund steht, sind bei der Absicherung interner Netzübergänge auch andere Anwendungen und Protokolle zu berücksichtigen.

Auf Basis der Netzkategorien können die folgenden Arten von **Netzübergängen** definiert werden:

- Übergang zwischen internen Netzen.
- Übergang zwischen internen Netzen und DMZ unter eigener/fremder Kontrolle.
- Übergang zwischen internen Netzen und dem Internet.
- Übergang zwischen DMZ unter eigener/fremder Kontrolle und dem Internet.

1.2 Absicherung von Netzübergängen

Um die Kommunikation zwischen Netzen mit unterschiedlichem Sicherheitsniveau zu kontrollieren, ist der Einsatz von Sicherheitsgateways notwendig.

„Ein **Sicherheitsgateway** (oft auch Firewall genannt) ist ein System aus soft- und hardwaretechnischen Komponenten zur Gewährleistung einer sicheren Kopplung von IP-Netzen durch Einschränkung der technisch möglichen auf die in einer IT-Sicherheitsleitlinie als ordnungsgemäß definierte Kommunikation. Sicherheit bei der Netzkopplung bedeutet hierbei vor allem die ausschließliche Zulassung erwünschter Zugriffe oder Datenströme zwischen verschiedenen Netzen und die Kontrolle der übertragenen Daten. Die Verwendung des Begriffs Sicherheitsgateway anstatt des üblicherweise verwendeten Begriffs Firewall soll verdeutlichen, dass zur Absicherung von Netzübergängen heute nicht mehr ein einzelnes Gerät verwendet wird, sondern eine Menge von Rechnern und deren Konzeption, die unterschiedliche Aufgaben übernehmen, z. B. Paketfilterung, Schutz vor Viren oder die Überwachung des Netzverkehrs.“ [BSI-SICH-GW]

Die grundlegenden Komponenten eines Sicherheitsgateways werden im Folgenden kurz erläutert.

1.2.1 Paketfilter (stateful/stateless)

Sicherheitsgateways, die nur aus einem Paketfilter bestehen, kontrollieren die Kommunikation auf der Ebene der Netz- und Transportprotokolle (IP, TCP, UDP oder ICMP).

Die realisierbaren Kontrollmöglichkeiten können je nach Paketfilter unterschiedlich sein. Die Kontrolle von TCP-Verbindungen wird i. d. R. von allen Produkten gleich unterstützt. Durch Zugriffskontrolllisten wird festgelegt, welches System im externen Netz mit welchem System im internen System (und umgekehrt) eine Verbindung initiieren darf. Hierzu werden die Informationen auf TCP/IP-Ebene verwendet (IP-Adressen und Ports). Zusätzlich kann i. d. R. angegeben werden, ob bestehende Verbindungen (established connections) nicht weiter überprüft werden. Diese Einstellung erhöht die Performance von Paketfiltern, da die aktive Kontrollfunktion nur beim Verbindungsaufbau erfolgt. Pakete, die aufgrund ihrer internen Informationen zu einer bestehenden (und daher bereits geprüften) Kommunikationsbeziehung zugeordnet werden, können direkt weitergeleitet werden. Dabei verlässt sich ein **„stateless“ Paketfilter** ausschließlich auf die Angaben im jeweiligen TCP-Paket (TCP-Statusflags, z. B. SYN, ACK). Ein **„stateful“ Paketfilter** merkt sich dagegen den Status einer erfolgreich aufgebauten TCP-Kommunikation und kann daher anhand seiner Statustabelle unabhängig von den Angaben im Datenpaket entscheiden, ob das zu überprüfende Paket zu einer etablierten TCP-Kommunikation gehört oder nicht. Weitere Informationen zu diesem Thema findet man in [BSI-SICH-GW].

UDP-Pakete erfordern eine besondere Behandlung, da dieses Protokoll verbindungslos ist. Das bedeutet, dass ein Paketfilter den Zusammenhang zwischen eingehender und ausgehender Kommunikation nicht direkt erkennen kann. Sicherheitsgateways auf Paketfilter-Basis lösen dieses Problem durch die Bildung einer Assoziation zwischen dem Quell- und dem Zielsystem („stateful“ Paketfilter). Die Kontrollregeln für den Paketfilter geben an, welche Systeme eine UDP-Kommunikation initiieren dürfen. Für diese Systeme werden UDP-Pakete durchgelassen. Für den Rücktransport von Antwortpaketen bildet das Sicherheitsgateway eine zeitlich begrenzte Assoziation zwischen dem Quell- und dem Zielsystem. Antwortpakete zum Quellsystem werden nur für eine begrenzte Zeit akzeptiert. Dies ist auch bei Anwendungen erforderlich, bei denen Rückverbindungen initiiert werden, wie z. B. bei FTP.

Dynamische Protokolle wie RPC oder Corba/IIOP stellen Sicherheitsgateways vor ein prinzipielles Problem. Die Zuordnung der Portnummern bzw. IP-Adressen ist nicht statisch, sondern wird zwischen dem Quell- und dem Zielsystem dynamisch beim Start der Anwendung ausgehandelt (RPC: Portmapper-Mechanismus). Deshalb sind diese Protokolle durch ein Sicherheitsgateway nur schwer abzusichern. Ein Paketfilter, der zur Kontrolle von RPC-Protokollen eingesetzt werden soll, muss in der Lage sein, diese

Kommunikation zur Aushandlung der Portnummern zu verfolgen und zu interpretieren. Zur Kontrolle der anschließenden Kommunikation muss eine temporäre Filterregel erstellt werden, die die ausgehandelten Informationen berücksichtigt. Die Gültigkeit der Filterregel muss, wie bei UDP beschrieben, durch einen Timeout-Mechanismus begrenzt werden.

Paketfilter erlauben Kommunikationsbeziehungen auf Basis von IP-Adressen und Portnummern. Ein Paketfilter kann z. B. nicht kontrollieren, ob über TCP-Port 21 tatsächlich eine FTP-Kommunikation stattfindet oder vielleicht doch Telnet verwendet wird.

1.2.2 Application-Level-Gateway

Die Funktionen eines Sicherheitsgateways auf Anwendungsebene werden von den so genannten Application-Level-Gateways (ALG) übernommen. Implizit nehmen ALGs auch Funktionen auf den Schichten 2 bis 3 des TCP/IP Referenzmodells wahr. ALGs, auch Sicherheits-Proxies genannt, unterbrechen den direkten Datenstrom zwischen Quelle und Ziel. Bei einer Kommunikationsbeziehung zwischen Client und Server über einen Proxy hinweg nimmt der Proxy die Anfragen des Clients entgegen und leitet sie an den Server weiter. Bei einem Verbindungsaufbau in umgekehrter Richtung, also vom Server zum Client, verfährt der Proxy analog. Sämtliche Kommunikationsbeziehungen zwischen den beiden Rechnern verlaufen in diesem Fall also mittelbar über den Proxy. Diese Kommunikationsform ermöglicht es einem Proxy beispielsweise, die übertragenen Daten inhaltlich zu kontrollieren oder bestimmte Protokollbefehle zu filtern.

Für Anwendungen oder Dienste, die keine statische Portnummernzuordnung haben, wie z. B. RPC-Anwendungen, sind in der Regel keine Proxies verfügbar. Die Nutzung dieser Anwendungen kann derzeit nur über Sicherheitsgateways auf Paketfilter-Ebene (Stateful Inspection) kontrolliert werden.

1.2.3 Kombinationen aus Paketfilter und Application-Level-Gateway

Zum Schutz des Application-Level-Gateways vor Angriffen auf IP- und Anwendungsebene (Betriebssystemfunktionen) ist die Kombination mit einem Paketfilter erforderlich.

Durch das Vorfiltern der Kommunikation erhöht sich die Sicherheit des Sicherheitsgateways und die Performance der Proxies, da nur erlaubte Pakete bis auf Anwendungsebene durchgelassen werden. Der Paketfilter kann entweder im System integriert oder dem Application-Level-Gateway als separates System vorgelagert sein. Dabei ist es wünschenswert, wenn Paketfilter und Application-Level-Gateway von unterschiedlichen Herstellern stammen. Außerdem sollten, wenn möglich, beide Komponenten mit unterschiedlichen Technologien (z. B. unterschiedliche Betriebssysteme) realisiert werden. Andernfalls besteht die Gefahr, dass die Auswirkungen von Implementierungsfehlern durch den Hersteller der Sicherheitskomponenten gravierend sind, weil die Implementierungsfehler gleichzeitig an allen beteiligten Komponenten auftreten könnten.

Besonders zur Absicherung von Anbindungen an das Internet ist ein mehrstufiger Aufbau, bestehend aus einem Paketfilter, einem Application-Level-Gateway und einem weiteren Paketfilter, empfehlenswert (s. auch Kap. 2.4.1).

Detaillierte Beschreibungen zu Schwachstellen und Angriffsmöglichkeiten bezüglich Sicherheitsgateways sind im Dokument [BSI-SICH-GW] zu finden.

1.3 Einführung in bestehende Vorschriften (Behörden / Industrie)

Neben den oben genannten rein technischen Aspekten bei der Gestaltung eines Netzübergangs sind noch eine Reihe von rechtlichen Rahmenbedingungen zu beachten. Diese Rahmenbedingungen sind sowohl für die Planung und den Betrieb als auch in der Folge für die Revision von Netzübergängen relevant.

Die rechtlichen Vorgaben beziehen sich im Wesentlichen auf zwei Aspekte:

- Datenschutz personenbezogener Daten

  Personenbezogene Daten müssen in zwei unterschiedlichen Kategorien betrachtet werden:

  a. Daten, die bei der Kontrolle des Datenverkehrs an Netzübergängen über die Kommunikationsteilnehmer anfallen:
  Diese Informationen können personenbezogen sein und dazu dienen, das Verhalten dieser Personen zu kontrollieren oder zu überwachen.

  b. Direkt personenbezogene Daten, die mit Hilfe der Informationstechnik verarbeitet werden und damit besonderen Schutz erfordern:
  Netzübergänge leisten dann sowohl Zugriffsschutz als auch ggf. gesicherten Transport über nicht vertrauenswürdige Netze.

- Schutz sonstiger sensitiver Daten

  Hierbei handelt es sich um Daten, die über Netzübergänge transportiert werden oder durch sie gegen unautorisierten Zugriff geschützt werden sollen. Dieser Schutz wird in unterschiedlichen Gesetzen in Form von Risikobetrachtungen und daraus resultierenden Maßnahmen zur Minderung des Risikos gefordert. Darüber hinaus werden Maßnahmen zur Überwachung gefordert und damit letztlich auch die IT-Revision adressiert.

Insgesamt ist eine umfassende Darstellung der maßgeblichen Gesetze und Vorschriften an dieser Stelle nicht umsetzbar. Daher wird im Folgenden eine Übersicht geltender Gesetze und Vorschriften präsentiert, die in drei Klassen eingeteilt werden:

- allgemeingültige Vorschriften,
- Vorschriften und Regelungen für den öffentlichen Bereich und
- Vorschriften und Gesetze für den privatwirtschaftlichen Bereich.

1.3.1 Allgemeingültige Vorschriften

Dieser Abschnitt beschreibt Bestimmungen, die in jedem Fall – also sowohl von öffentlichen wie privatwirtschaftlichen Organisationen – zu beachten sind.

- IT-Rahmenkonzepte, IT-Sicherheitsleitlinien und Sicherheitskonzepte

  Dieser Bereich subsumiert alle organisationsintern gültigen Richtlinien und Konzepte, die bei der Einführung oder der Revision eines Sicherheitsgateways zu beachten sind. Sie sind per Definition individuell unterschiedlich und können hier nur grundsätzlich aufgeführt werden. Allerdings stellen sie in jedem Fall eine zu beachtende wesentliche Grundlage für die Einführung oder Revision eines Sicherheitsgateways dar.

- Bundesdatenschutzgesetz (BDSG - Umsetzung der EU-Datenschutzrichtlinie 95/46/EG)

  Das BDSG schützt den Einzelnen in seinem Persönlichkeitsrecht, indem es den Umgang mit personenbezogenen Daten regelt.

Dazu ist zunächst der Grundsatz zu beachten, dass Datenverarbeitungssysteme derart konzipiert und konfiguriert sein sollten, dass so wenig personenbezogene Daten wie möglich erhoben werden. Darüber hinaus muss eine Möglichkeit vorhanden sein, aufgezeichnete Daten zu anonymisieren und Pseudonyme anzulegen (§ 3a).

Die Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten kann nur durch andere Rechtsvorschriften erteilt werden oder durch die explizite Einwilligung der Betroffenen (§§ 4 und 4a).

Zu beachten ist, dass den Personen, die mit der Bearbeitung der personenbezogenen Daten beauftragt sind, untersagt ist, diese Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Die aufgezeichneten Daten unterliegen dem Datengeheimnis. Insbesondere sind Personen, die in nichtöffentlichen Stellen beschäftigt sind und mit derartigen personenbezogenen Daten operieren, auf das Datengeheimnis zu verpflichten (§ 5).

Werden personenbezogene Daten im Auftrag durch andere Stellen, z. B. einen IT-Dienstleister, erhoben, verarbeitet oder genutzt, so ist der Auftraggeber für die Einhaltung der Bestimmungen des BDSG verantwortlich (§ 11).

Personenbezogene Daten, die an einem eingesetzten Sicherheitsgateway ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes gespeichert werden, dürfen nur für diese Zwecke verwendet werden (§§ 14 und 31).

Den von der Sammlung personenbezogener Daten betroffenen Personen ist auf Antrag Mitteilung darüber zu geben, welche Daten zur Person gespeichert, an wen sie weitergeleitet und zu welchem Zweck sie gespeichert wurden (§ 19).

Der Zweck der Erhebung personenbezogener Daten ist konkret festzulegen (§ 28).

- Teledienstedatenschutzgesetz (TDDSG - Pflichten des Diensteanbieters)

  Das TDDSG regelt den Schutz personenbezogener Daten der Nutzer von Telediensten.

  Im Falle der Datenerhebung durch einen Diensteanbieter (§ 2 „Diensteanbieter: Jede natürliche oder juristische Person, die eigene oder fremde Teledienste zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt“) ist der Nutzer zu Beginn eines Nutzungsvorganges über die Art, den Umfang und den Zweck der Erhebung sowie der Verarbeitung und Nutzung personenbezogener Daten durch den Diensteanbieter zu unterrichten.

  Weitere Informationen finden Sie unter: http://bundesrecht.juris.de/tddsg/

- Telekommunikations-Datenschutzverordnung (TDSV)

  Die TDSV regelt den Schutz personenbezogener Daten der an der Telekommunikation Beteiligten bei der Erhebung, Verarbeitung und Nutzung dieser Daten durch Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste erbringen oder an deren Erbringung mitwirken (§ 1).

  Weitere Informationen finden Sie unter:

  http://www.datenschutz-berlin.de/gesetze/medien/tdsv12_2000.htm

- Staatsvertrag für Mediendienste (MDStV)

  Zweck des Staatsvertrages ist, in allen Bundesländern einheitliche Rahmenbedingungen für die verschiedenen Nutzungsmöglichkeiten der elektronischen Informations- und Kommunikationsdienste zu schaffen (§ 1).

  Weitere Informationen finden Sie unter: http://www.datenschutz-berlin.de/recht/de/stv/mdstv.htm

1.3.2 Vorschriften und Regelungen für den öffentlichen Bereich

Der öffentliche Bereich umfasst im Wesentlichen alle Bundes-, Landes- und Kommunalverwaltungen sowie sonstige Körperschaften und Anstalten des öffentlichen Rechts (unmittelbare und mittelbare Verwaltung).

Die im Folgenden genannten Richtlinien und Gesetze gelten in erster Linie für die Bundesverwaltung. Es gibt auf Landes- und Kommunalebene ähnliche Richtlinien und Gesetze, auf die hier jedoch nicht im Einzelnen eingegangen wird.

- Richtlinien für den Einsatz der Informationstechnik in der Bundesverwaltung (IT-Richtlinien)

  Die IT-Richtlinien beschreiben in erster Linie Anforderungen, die zum Zeitpunkt der Planung einer Einführung von Informationstechnologie allgemein innerhalb einer obersten Bundesbehörde relevant sind. Die beschriebenen Anforderungen sind somit zum Zeitpunkt der Integration von Bedeutung.

  Die Richtlinie fordert ein IT-Rahmenkonzept, das vor der Veranschlagung eines IT-Vorhabens im Bundeshaushaltsplan vorliegen muss. Darin sind unter anderem zu beschreiben:

  - grundsätzliche Ziele des IT-Einsatzes,
  - organisatorische und personelle Auswirkungen des IT-Einsatzes,
  - notwendige Sicherheitsmaßnahmen,
  - Aufwandsabschätzung für die Einführung sowie
  - Strategien zur Einführung der IT.

  Über das IT-Rahmenkonzept hinausgehend beschreibt die Richtlinie weitere Anforderungen:

  - Die von der einzuführenden IT betroffenen Mitarbeiter sind rechtzeitig sowie entsprechend den Systemanforderungen vorzubereiten und weiterzubilden.
  - Die sich ergebenden Risiken durch den geplanten Einsatz von IT sind zu analysieren, zu bewerten sowie entsprechende Schutzmaßnahmen zu treffen.
  - Bei der Einführung der IT sind Randbedingungen hinsichtlich Kompatibilität mit anderen Kommunikationspartnern durch die Beachtung internationaler, europäischer oder deutscher Normen einzuhalten. Ebenso ist die Flexibilität in Form von Reaktionsmöglichkeiten auf veränderte Anforderungen oder technische Weiterentwicklungen zu wahren.
  - Die Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung im Bundesministerium des Innern (KBSt) gibt als ressortübergreifendes Organ Stellungnahmen zu erstellten IT-Rahmenkonzepten ab bzw. ist zu geplanten Vorhaben zu konsultieren.

  Weitere Informationen finden Sie hier: Richtlinien für den Einsatz der Informationstechnik in der Bundesverwaltung (IT-Richtlinien) vom 18. August 1988 (Bekanntmachung vom 6. September 1988, BAnz. S. 4397; GMBl. S. 470)

- IT-Grundschutzhandbuch (IT-GSHB)

  Das IT-Grundschutzhandbuch (IT-GSHB), herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik (BSI), hat nicht den Status eines Gesetzes oder einer verbindlichen Richtlinie. Es bildet aber eine sehr umfassende Grundlage zur Grundsicherung von Informationen durch die Bereitstellung von organisatorischen, technischen und infrastrukturellen Maßnahmen. Darüber hinaus werden Maßnahmen im Umfeld Personal, Kommunikation und Notfallvorsorge beschrieben.

- (Bundes)Personalvertretungsgesetz ((B)PersVG)

Das PersVG (Bundes- oder Landesrecht) regelt für öffentliche Stellen die Zusammenarbeit zwischen der Dienststellenleitung und der gewählten Personalvertretung. In diesem Zusammenhang behandelt es Fragen der Mitbestimmung bei der Einrichtung von Systemen, die personenbezogene Daten aufzeichnen, welche zur Überwachung oder Kontrolle herangezogen werden können.

Weitere Informationen finden Sie unter: http://bundesrecht.juris.de/bpersvg/BJNR006930974.html

1.3.3 Vorschriften und Gesetze für den privatwirtschaftlichen Bereich

Der privatwirtschaftliche Bereich umfasst Organisationen wie Industrieunternehmen, Banken, Versicherungen u. Ä.. Die im Folgenden dargestellten Vorschriften und Gesetze gelten zum Teil nur für spezielle Unternehmen.

- Betriebsverfassungsgesetz (BetrVG)

  Das BetrVG regelt für nichtöffentliche oder öffentlich-rechtliche Wettbewerbsunternehmen die Zusammenarbeit zwischen Arbeitgeber und Betriebsrat und adressiert – vergleichbar dem Personalvertretungsgesetz im öffentlichen Bereich – die Mitbestimmung bei der Einrichtung von Systemen, die personenbezogene Daten aufzeichnen, welche zur Überwachung oder Kontrolle herangezogen werden können.

  Weitere Informationen finden Sie unter: http://bundesrecht.juris.de/betrvg/

- Handelsgesetzbuch (HGB) bzw. Grundsätze ordnungsgemäßer Buchführung (GoB) und die daraus abgeleiteten Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)

  HGB und GoB beschreiben grundsätzliche Anforderungen an die Ordnungsmäßigkeit und Revisionsfähigkeit der Geschäftstätigkeit einer Organisation. Die GoBS gelten für alle DV-gestützten Verfahren, die für die Rechnungslegung relevant sind. Da buchhaltungsrelevante Belege heute auch durch elektronische Vorgänge (z. B. EDI) außerhalb einer „Abteilung Buchhaltung“ entstehen und in das Buchhaltungssystem einfließen können, können die Vorgaben der GoBS weit reichende Auswirkungen nach sich ziehen.

  Weitere Informationen finden Sie unter: http://bundesrecht.juris.de/hgb/

- Kreditwesengesetz (KWG)

  Das KWG richtet sich an Kreditinstitute und Finanzdienstleistungsinstitute. Für diese Organisationen werden angemessene Sicherheitsvorkehrungen für die elektronische Datenverarbeitung bzw. Kontrollmöglichkeiten im Falle der Auslagerung von Dienstleistungen gefordert.

  Weitere Informationen finden Sie unter: http://bundesrecht.juris.de/kredwg/

Die im Folgenden dargestellten Vorschriften und Gesetze beschäftigen sich in erster Linie mit der Risikoabsicherung und -betrachtung.

- Baseler Eigenmittelempfehlung (Basel II)

  Die durch den Baseler Ausschuss für Bankenaufsicht verabschiedeten neuen Eigenkapitalvorschriften für Banken im Rahmen von Kreditvergaben, bekannt unter dem Stichwort „Basel II“, richten sich zunächst an Banken in ihrer Funktion als Kreditgeber. In Konsequenz wirken sie aber auf die potenziellen Kreditnehmer (Firmen oder auch andere Banken). Sie fordern von den Kreditgebern, sich zur eigenen Absicherung vom Vorhandensein eines angemessenen Risikomanagements bei ihren Kreditkunden zu überzeugen, das insbesondere auch die Informationsverarbeitung einbezieht.

- Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)/Aktiengesetz (AktG)

Mit dem Artikelgesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) werden die Unternehmen dazu verpflichtet, ein internes Überwachungs- oder Risikomanagement-System zu implementieren, das es ermöglicht, existenzgefährdende Entwicklungen zu erkennen. Dies ist durch Wirtschaftsprüfer im Rahmen der jährlichen Prüfung zu verifizieren.

Diese Anforderungen gelten für Aktiengesellschaften. Unter bestimmten Umständen sind jedoch darüber hinaus auch andere Kapitalgesellschaften, offene Handelsgesellschaften oder Kommanditgesellschaften davon betroffen.

Weitere Informationen finden Sie unter: http://bundesrecht.juris.de/aktg/BJNR010890965.html

- Sarbanes-Oxley Act (SOA)

  Der Sarbanes-Oxley Act gilt für alle Unternehmen, die einen der US-amerikanischen Börsenaufsicht (Securities and Exchange Commission [SEC]) unterliegenden Kapitalmarkt in Anspruch nehmen (listed companies). Damit sind auch deutsche Unternehmen betroffen, deren Aktien in den USA gehandelt werden (foreign private issuers). Ferner können auch die Tochtergesellschaften betroffen sein, sofern sie eine wesentliche Einheit der Muttergesellschaft (significant subsidiaries) darstellen.

  Weitere Informationen finden Sie unter: http://www.law.uc.edu/CCL/SOact/soact.pdf

1.4 Zusammenfassung

In diesem Kapitel wurden zunächst die Charakteristika eines Netzübergangs dargestellt: Verbindung mindestens zweier nicht verbundener Netze durch den Einsatz spezieller Technologien und Systeme. Diese speziellen Technologien und Systeme sind notwendig, um einerseits definierte Kommunikation zu ermöglichen, aber andererseits, aus Sicherheitsgründen, Zugriffsmöglichkeiten in einem angeschlossenen Netz einzuschränken oder sogar zu verhindern.

Anschließend wurden grundlegende Technologien zur Absicherung von Netzübergängen (Sicherheitsgateways bestehend aus Paketfilter, ALG und Kombinationen daraus) vorgestellt.

Ein weiterer Bestandteil dieses Kapitels ist die Beschreibung gesetzlicher und weiterer Rahmenbedingungen, die bei der Integration und IT-Revision von Netzübergängen eine Rolle spielen können.

Auf der Basis dieser Grundlagen wird im nächsten Kapitel die Integration, d. h. die Planung, Realisierung und Inbetriebnahme von Netzübergängen betrachtet. Dabei stehen Fragestellungen zur IT-Sicherheit im Vordergrund.

Ist ein Netzübergang einmal – unter Beachtung aller gegebenen Randbedingungen – integriert und in Betrieb, muss auch sichergestellt werden, dass alle Anforderungen zukünftig erfüllt und beachtet werden sowie ggf. auf veränderte Anforderungen reagiert wird.

Um dies sicherzustellen, sollen regelmäßige oder auch spontane IT-Revisionen stattfinden. Dadurch wird überprüft, ob alle Vorgaben und Anforderungen ordnungsgemäß erfüllt sind.

2 Integration von Netzübergängen

In diesem Kapitel wird erläutert, welche Anforderungen an die Integration von Netzübergängen unter dem Gesichtspunkt der IT-Sicherheit zu stellen sind. „Integration“ umfasst dabei die typischen Phasen der Einführung bzw. Änderung eines IT-Systems:

- Planen
  Welche Dienste[1] werden benötigt? Welche grundlegenden Anforderungen an die Architektur bestehen?
- Realisieren
  Welche Produkte sind geeignet? Wie wird das System gebaut, so dass es später auch optimal betrieben werden kann?
- In Betrieb nehmen
  Wie erfolgt der Übergang in die operationelle Phase? Welche organisatorischen Randbedingungen sind zu beachten?

Zweck dieses Kapitels ist es, die Aspekte der Integration von Netzübergängen unter IT-Sicherheitsgesichtspunkten zu betrachten, die für die in Kapitel 3 beschriebene IT-Revision wesentlich sind.

Wie später noch näher gezeigt wird, ist das Vorhandensein eines IT-Sicherheitskonzepts für den zu prüfenden Netzübergang von entscheidender Bedeutung. Im IT-Sicherheitskonzept werden alle wesentlichen (Soll-)Anforderungen zusammengefasst, die später, in der Revision, überprüft werden sollen (Vergleich des Soll- mit dem vorgefundenen Ist-Zustand).

Aus diesem Grund wird hier eine grundlegende Vorgehensweise zur Erstellung eines Netzsicherheitskonzepts vorgestellt und vertiefend auf die verschiedenen Anforderungen eingegangen, die bei der Integration zu beachten sind.

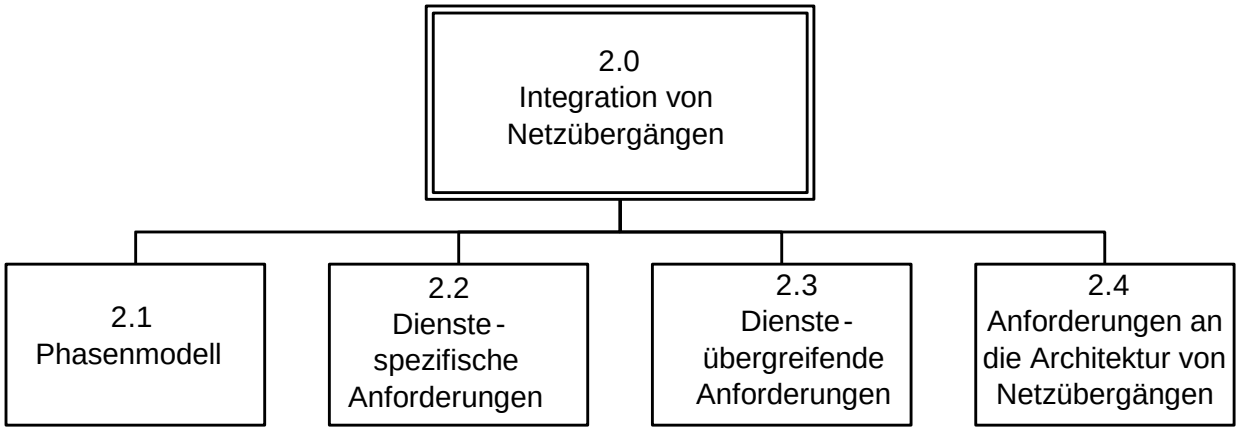


Abbildung 1: *Integration von Netzübergängen. Die Grafik verdeutlicht den Aufbau des Kapitels 2: „Integration von Netzübergängen“.*

[1] Unter dem Begriff „Dienst“ wird eine Anwendung verstanden, die in der Regel auf höherwertigen Protokollen (TCP, UDP) basiert. Einfache Dienste verwenden dabei in der Regel genau ein Anwendungsprotokoll (z. B. HTTP, POP3, SMTP). Komplexere Applikationen (z. B. Reuters, Bloomberg, Xetra) können mehrere Anwendungsprotokolle/Dienste verwenden.

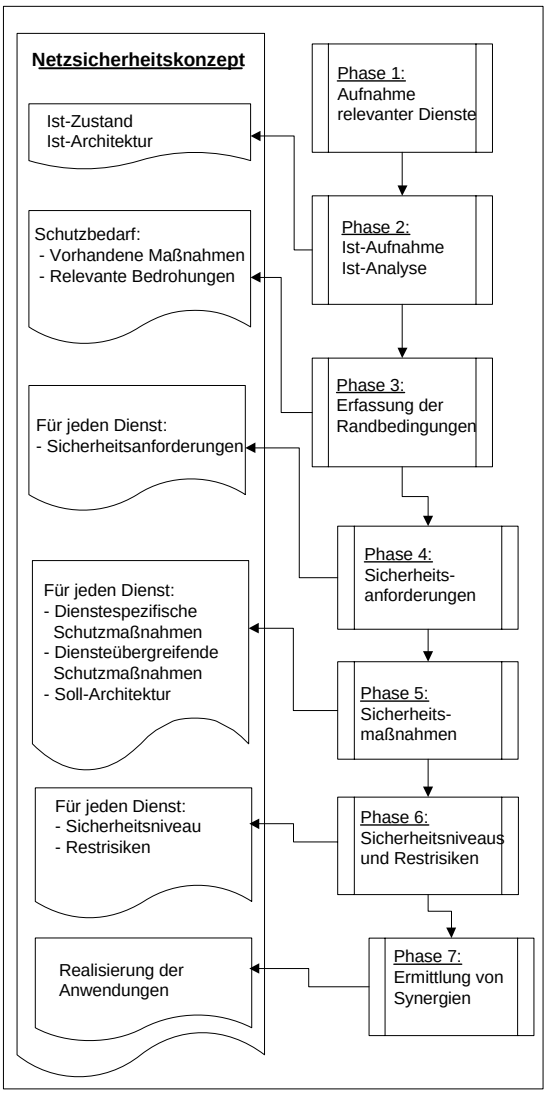
Zunächst wird kurz auf eine Vorgehensweise zum Erstellen eines Sicherheitskonzepts in Form eines Phasenmodells eingegangen.

Kernpunkt bei der Erstellung ist die systematische Berücksichtigung von Sicherheitsanforderungen an Netzübergänge (vgl. Phase 4 in Abb. 2), die daher im Anschluss an das Phasenmodell wie folgt näher betrachtet werden:

- Dienstespezifische Sicherheitsanforderungen
  Dies sind die Anforderungen, die sich aus dem Kommunikationsbedarf ableiten und für jeden eingesetzten Dienst berücksichtigt werden müssen. Sie repräsentieren den spezifischen Bedarf eines IT-Systems bzw. Netzübergangs an Sicherheit. Dienstespezifische Sicherheitsanforderungen sind daher für jeden relevanten Dienst separat zu implementieren bzw. bei der IT-Revision separat zu betrachten.
- Diensteübergreifende Sicherheitsanforderungen
  Dies sind Anforderungen, die sich unabhängig vom Kommunikationsbedarf für den Netzübergang auf Grund seiner exponierten Stellung für die Sicherheit ergeben.
- Anforderungen an die Architektur von Netzübergängen
  Dies sind Anforderungen, aus denen die Architektur für den konkret geplanten Netzübergang abgeleitet wird, wobei die vorgenannten Sicherheitsanforderungen darin einfließen bzw. zu einer Gesamtlösung zusammengefasst werden.

2.1 Phasenmodell

Basis für die Begründung, Realisierung und Revision von Sicherheitsmaßnahmen ist die Erstellung eines Sicherheitskonzepts, das nach folgendem Phasenmodell (s. Abb. 2) erstellt werden kann.



1. Alle relevanten **Anwendungen** die über das abzusichernde Netz hinweg genutzt werden, werden erfasst und ihre Funktion wird beschrieben. Beispiel: Externer Web-Zugriff mit Hilfe von Diensten wie http, https etc.
2. Die zugrunde liegenden **Dienste** (Beispiel: http(s), smtp etc.) werden auf ihre technische Realisierung hin untersucht. Dabei werden der Kommunikationsbedarf und eine ggf. vorgegebene Architektur aufgenommen.
3. Unternehmensspezifische **Randbedingungen** werden erfasst (**Schutzbedarf** der Daten, vorhandene Schutzmaßnahmen etc.).
4. Die **Anforderungen** zur Absicherung eines Dienstes werden ermittelt. Diese werden im Rahmen einer Sicherheitsleitlinie festgelegt oder aus dieser hergeleitet.
5. Zur Realisierung der Sicherheitsanforderungen wird eine **Sicherheitsarchitektur** bestimmt und die **Sicherheitsmaßnahmen** werden auf deren Einzelkomponenten abgebildet.
6. Schließlich wird für jeden Dienst das erreichbare Schutzniveau bestimmt und die verbleibenden **Restrisiken** werden aufgezeigt.
7. Zum Abschluss des Vorgehens wird geprüft, ob durch **Synergieeffekte** geforderte Einzelmaßnahmen für die Absicherung von Diensten gebündelt werden können.

Abbildung 2: *Grafische Übersicht des Integrationsprozesses. Auf der rechten Seite der Grafik sind die einzelnen Phasen des Integrationsprozesses mit den entsprechenden Inhalten zu sehen. Die linke Seite zeigt, was in den einzelnen Phasen zu beachten ist.*

Das Sicherheitskonzept dient als Basis zunächst für die Auswahl und später für die Revision von Sicherheitsmaßnahmen. Ist kein Sicherheitskonzept vorhanden, so ist für realisierte (oder auch nicht realisierte) Maßnahmen zur Absicherung von Netzübergängen keine Bewertungsgrundlage verfügbar. Es fällt dann schwer zu bewerten:

- welche Risiken durch diese Realisierung verringert werden,
- welches Restrisiko verbleibt und ob dieses tragbar ist,
- wie sich das Kosten-Nutzen Verhältnis darstellt.

Eine Revision ist daher ohne ein Sicherheitskonzept nur eingeschränkt möglich, da die Vorgaben fehlen, gegen die die realisierten Sicherheitsmaßnahmen geprüft werden sollen. Außerdem entstehen zeitliche Verzögerungen und Mehraufwendungen, wenn die Vorgaben im Zuge einer Revision erst formuliert und abgestimmt werden müssen. In einem solchen Fall können die Grundschutzkataloge [BSI-GSHB04] Abhilfe schaffen. Mit deren Hilfe kann überprüft werden, welche Maßnahmen bereits umgesetzt worden sind und welche fehlen.

Nachfolgend werden verschiedene Anforderungen vorgestellt, die es im Rahmen der Erstellung eines Sicherheitskonzepts zu berücksichtigen gilt.

2.2 Dienstespezifische Sicherheitsanforderungen

Wie bei der Vorstellung des Phasenmodells gezeigt, spielen zunächst der Kommunikationsbedarf bzw. die benötigten Dienste eine große Rolle. Es hat sich bewährt, im ersten Schritt jeden Dienst einzeln zu betrachten und anschließend eine Architektur zu entwerfen, die alle Dienste integriert.

Im Zusammenhang mit den dienstespezifischen Anforderungen werden nachfolgend diese Aspekte vorgestellt:

- Schutzbedarf
- Sicherheitsmaßnahmen

2.2.1 Schutzbedarf

Ein kontrollierter Netzübergang muss eingerichtet werden, wenn die zu verbindenden Netze jeweils unterschiedlichen Schutzbedarf besitzen. Auch bei gleichem Schutzbedarf ist die Einrichtung eines kontrollierten Netzübergangs erforderlich, falls die Verbreitung von sicherheitsrelevanten Informationen auf das jeweilige Teilnetz beschränkt bleiben soll. Der Schutzbedarf ergibt sich in Anlehnung an das Grundschutzhandbuch des BSI aus der Einstufung bezüglich Vertraulichkeit, Integrität und Verfügbarkeit der Daten, die in dem Netz verarbeitet und transportiert werden. Als Kriterium für die Einschätzung des Schutzbedarfs wird häufig der potenzielle Schaden verwendet, der entstehen kann, wenn Daten gelöscht, manipuliert oder an Dritte bekannt gegeben werden.

Bei der Einstufung des Schutzbedarfs sind die folgenden Faktoren zu berücksichtigen:

- Verstoß gegen Gesetze/Vorschriften und Verträge,
- Beeinträchtigung des informationellen Selbstbestimmungsrechts,
- Beeinträchtigung der persönlichen Unversehrtheit,
- Beeinträchtigung der Aufgabenerfüllung,
- negative Innen- oder Außenwirkung und
- finanzielle Auswirkungen.

Die zu berücksichtigenden Maßnahmen bei der Einrichtung von Netzübergängen konzentrieren sich somit auf den Schutz der im Netz transportierten Daten im Rahmen der Kommunikation, die aufgrund der genutzten Anwendung über Netzgrenzen hinaus erforderlich ist.

Die Definition des Schutzbedarfs für die Teilnetze stellt damit auch eine wichtige Grundlage für eine IT-Revision dar. Je größer der festgestellte Schutzbedarf eingeschätzt wird, desto stärker sind auch die Anforderungen an jede der im Folgenden beschriebenen Sicherheitsmaßnahmen.

2.2.2 Sicherheitsmaßnahmen

Das Grundschutzhandbuch des BSI gibt die Möglichkeit aus dem Schutzbedarf des Netzes Sicherheitsanforderungen abzuleiten, die ein zu implementierendes Schutzsystem erfüllen muss. Steht das Grundschutzhandbuch nicht zur Verfügung oder wurde ein hoher (bzw. sehr hoher) Schutzbedarf ermittelt, muss eine detaillierte Bedrohungs- bzw. Risikoanalyse durchgeführt werden. Abhängig von der Kommunikationsbeziehung und der Richtung der Kommunikation können unterschiedliche Anforderungen definiert werden, die entweder für Netze oder individuell für die zu realisierenden Anwendungen (dienstespezifisch) gelten.

Hierbei fließt neben den Anwendungen und Kommunikationsrichtungen auch der Schutzbedarf in die Betrachtungen mit ein.

Besonderes Augenmerk sollte auf Sicherheitsmaßnahmen aus den folgenden Bereichen gelegt werden:

- **Identifikation und Authentisierung**
- **Datenflusskontrolle**
- **Beweissicherung**
- **Kryptographische Übertragungssicherung**
- **Schlüsselmanagement**

Je höher der Schutzbedarf der Daten und verwendeten Dienste, desto höher die Anforderungen an die Qualität der Umsetzung dieser dienstespezifischen Sicherheitsfunktionen. Im Folgenden werden die Bereiche kurz beschrieben. Ausführlichere Informationen zu Sicherheitsmaßnahmen aus diesen Bereichen findet man in [BSI-GSHB04].

- **Identifikation und Authentisierung**
  Die Maßnahmen zur „Identifikation und Authentisierung“ unterstützen die Absicherung von Ende-zu-Ende-Verbindungen. Sie sind geeignet, Systeme untereinander, Systeme gegenüber Benutzern und Benutzer gegenüber Systemen und Anwendungen zu identifizieren und zu authentisieren.
- **Datenflusskontrolle**
  Mit Hilfe der Funktion „Datenflusskontrolle“ kann der Übergang von Daten zwischen Teilnetzen kontrolliert werden. Im Mittelpunkt steht der Schutzbedarf der zu übertragenden Daten. Im Zusammenhang mit Netzübergängen ist der Begriff Datenflusskontrolle als Kontrolle der erlaubten Kommunikationsbeziehungen zu verstehen, die über ein Sicherheitsgateway erfolgen dürfen. Die Kommunikationsbeziehungen werden aus den Diensten selbst sowie aus den Dienstrichtungen gebildet. Es gilt:
  - Eine Kontrolle auf Anwendungsebene (Application-Level-Gateway) ist höher zu bewerten als eine Paketfilterung auf niedrigeren Protokollebenen, da eine Kontrolle auf Anwendungsebene mehr spezifische Eigenschaften des Dienstes erfassen kann.
  - Eine benutzerbezogene Kontrolle ist höher zu bewerten als eine maschinenbezogene Kontrolle der Dienstnutzung, da eine Kontrolle der Dienstnutzung auf Benutzerebene die Definition von

Regeln höherer Granularität zur Kontrolle der Dienstnutzung durch einzelne Benutzer erlaubt. Dabei ist dann das Prinzip der „niedrigsten Privilegierung“ *(least privilege principle)* besser durchsetzbar. Dies ist wesentlich bei Mehrbenutzersystemen und Benutzern mit unterschiedlichem Kommunikationsbedarf auf einer Maschine.

- **Beweissicherung**
  Unter der Funktion „Beweissicherung“ versteht man die Aufzeichnung netzspezifischer Ereignisse mit Hilfe von Protokollierungsfunktionen an den eingesetzten Systemen. Die Aufzeichnungen können unmittelbar ausgewertet oder für eine spätere Auswertung aufbewahrt werden.

  Die aufgezeichneten Ereignisse dienen

  - der frühzeitigen Erkennung sicherheitsrelevanter Vorkommnisse und
  - als Beweisgrundlage für eine spätere Tatverfolgung.

- **Kryptographische Übertragungssicherung**
  Mit Hilfe der Funktion „Kryptographische Übertragungssicherung“ kommen Mechanismen zum Einsatz, welche die Vertraulichkeit und Integrität der Daten sichern. Hierbei ist die Auswahl eines geeigneten, am Schutzbedarf der Daten orientierten, kryptographischen Verfahrens von großer Wichtigkeit. Entsprechend sorgfältig sollte die Auswahl eines kryptographischen Produktes erfolgen. Eine gute Hilfe bietet hierbei der Baustein „Kryptokonzept“ in [BSI-GSHB04].

  Hinweis: Bei VS-Netzen gelten die Anforderungen der VSA[2]. Bei datenschutzrelevanten und firmenvertraulichen Daten wird generell Verschlüsselung empfohlen.

- **Schlüsselmanagement**
  Die Funktion „Schlüsselmanagement“ stellt für andere Funktionen (hier: Kryptographische Übertragungssicherung) Mechanismen bereit, um geheime und öffentliche Schlüssel für die kryptographischen Funktionen zu verteilen.

Wenn die verbleibenden Risiken wegen fehlender Umsetzung der Anforderungen für einen Dienst oder eine Dienstrichtung nicht tolerierbar sind, muss entweder auf die Nutzung der Anwendung (oder einer Dienstrichtung) verzichtet werden oder es müssen zusätzliche Maßnahmen zur Verringerung der Risiken getroffen werden.

Bei der Revision von Netzübergängen kann anhand der Funktionalität der Produkte oder Produktkombinationen beurteilt werden, ob die Produkte die Anforderungen vollständig realisieren können oder ob Zusatzmaßnahmen erforderlich sind, um die vorhandenen Restrisiken auf ein tragbares Niveau zu reduzieren.

2.3 Diensteübergreifende Sicherheitsanforderungen

Neben den dienstespezifischen Anforderungen, die sich aus dem speziellen Einsatzzweck der Schutzsysteme an Netzübergänge ergeben, sind auch diensteübergreifende Anforderungen zu berücksichtigen.

Diensteübergreifende Sicherheitsanforderungen lassen sich nicht explizit aus den genutzten Diensten herleiten, sie wirken vielmehr allgemeinen Schwachstellen der eingesetzten Systeme und Protokolle entgegen.

Da, wie in Kapitel 1.2 „Absicherung von Netzübergängen“ beschrieben, Grundvoraussetzung für einen Netzübergang der Einsatz eines Sicherheitsgateways ist, sind von diesem die folgenden Sicherheitsanforderungen zu beachten:

---

[2] Allgemeine Verwaltungsvorschrift zum materiellen und organisatorischen Schutz von Verschlusssachen

- Schutz gegen bekannte Angriffsarten (u. a. Source-Routing, ICMP-Angriffe, Routing-Angriffe)
- Schutz gegen Schwachstellen in Dienstprogrammen
- Verbergen von Informationen des zu schützenden Netzes
- Schutz gegen Computerviren, Würmer, Trojaner
- Erkennung von internen Angriffen
- Anforderungen an die sichere Inbetriebnahme
- Anforderungen an eine sichere Administration
- Anforderungen an den sicheren Betrieb
- Anforderungen an die diensteübergreifende Beweissicherung

In einem Sicherheitskonzept ist somit darzulegen, wie der Netzübergang die o. g. Anforderungen erfüllt, d. h., welche konkreten Maßnahmen (vgl. Phase 5) hierzu vorgesehen sind.

Im Folgenden werden die einzelnen Anforderungen näher erläutert.

2.3.1 Schutz gegen bekannte Angriffsarten auf Protokollebene

Durch die Verwendung einer bestimmten Netztechnik (z. B. TCP/IP) existieren implizite Angriffsmöglichkeiten, die eingebaute Funktionalitäten einzelner Protokolle in missbräuchlicher Art und Weise verwenden oder fehlende Schutzfunktionen in Protokollen ausnutzen. Diese Angriffsarten sind weitestgehend bekannt und sollten unabhängig vom Sicherheitsgateway-Typ am Netzübergang verhindert werden. Beispiele dafür sind:

Source Routing liegt vor, wenn in IP-Paketen nicht nur Quell- und Zieladresse, sondern auch der Weg von der Quelle zum Ziel angegeben ist. Die Ausnutzung dieser Option ermöglicht es Angreifern, vorgegebene Übertragungswege zu umgehen. Insbesondere können Sicherheitsmechanismen völlig ausgehebelt werden. Daher sollte Source Routing möglichst unterbunden werden.

ICMP-Angriffe: Zum einen können über *Redirect*-Pakete die Routing-Tabellen eines Rechners geändert werden, was dazu dienen kann, vorgegebene Übertragungswege zu ändern. Zum anderen kann die Verfügbarkeit von Rechnern durch gefälschte *Destination-Unreachable*- oder *Time-Exceeded*-Pakete beeinträchtigt werden. Daher dürfen derartige Pakete die bedrohten Rechner möglichst gar nicht erst erreichen. Es gibt allerdings Szenarien, in denen die völlige Blockade von ICMP-Paketen des Typs *destination unreachable* kontraproduktiv ist, weil dadurch gewollter Netzverkehr unterbunden wird. Immer dann, wenn infolge von „überlangen“ Datenpaketen auf einer Teilstrecke im Netz Fragmentierung erforderlich, aber nicht zulässig ist, wird eine ICMP-Nachricht *(destination unreachable, fragmentation needed)* an den Absender zurückgesendet. Gelangt diese Fehlermeldung nicht zum Absender des „überlangen“ Datenpaketes zurück, bricht in der Folge die Kommunikation über diese Teilstrecke zusammen. ICMP darf daher nicht unbedacht und vollständig an allen Schnittstellen blockiert werden.

Routing-Angriffe: Wenn Router ihre Routing-Tabellen aufgrund der an sie gesendeten Routing-Informationen ändern, ergibt sich für Angreifer wieder die Möglichkeit, vorhandene Wege zu umgehen. Daher sollte das Routing des Sicherheitsgateways statisch erfolgen, d. h., die obige Änderungsmöglichkeit darf nicht bestehen.

2.3.2 Schutz gegen Schwachstellen in Dienstprogrammen[3]

Schwachstellen in Dienstprogrammen können zu vielen Formen von Sicherheitsproblemen führen. Bekannte Schwachstellen werden zusammen mit Hinweisen zu ihrer Beseitigung oder Umgehung in sog. *Advisories* veröffentlicht. Da diese auch von Angreifern gelesen werden, müssen alle systemrelevanten *Advisories* genau beachtet werden.

Um die Risiken bei der Verwendung von Dienstprogrammen zu beschränken, ist darauf zu achten, dass nur die absolute Mindestanzahl dieser Programme[4] auf dem Sicherheitsgateway installiert wird. Wenn möglich, sollten die installierten Programme in einer gesicherten Umgebung ablaufen (z. B. durch *chroot* unter UNIX erzeugt). Sie dürfen nur mit so vielen Rechten ausgestattet werden, wie für die Erfüllung ihrer Aufgaben unbedingt nötig sind *(least privilege principle)*.

2.3.3 Verbergen von Informationen des zu schützenden Netzes

Um Angreifern möglichst wenig Verwaltungsinformationen und Informationen über die interne Netzstruktur zugänglich zu machen, müssen die zuständigen Dienste restriktiv konfiguriert werden. NIS (Network Information System) sollte nicht über den Netzübergang betrieben werden. Für DNS (Domain Name Service) ist ein Server unabhängig vom internen Netz zu betreiben, der nur die absolut notwendigen Informationen bereitstellt.

2.3.4 Schutz gegen Computerviren, Würmer, Trojaner

Viren im internen Netz können zu vielen Formen von Sicherheitsproblemen führen. Daher müssen alle Anstrengungen unternommen werden, das Einschleusen von Viren zu verhindern, d. h., alle in das interne Netz eingebrachten Daten sind geeignet zu untersuchen.

Die Virenprüfung kann auf Sicherheitsgateways nicht vollständig durchgeführt werden. Zum einen ist zu beachten, dass die Untersuchung von eingehenden Daten auf Viren eine gewisse Zeit benötigt. Dies kann bei zeitkritischen Anwendungen zu Problemen führen, weil Antworten nicht rechtzeitig verschickt werden *(time out)*. Dieses Problem tritt bei der Virenprüfung auf dem Endsystem nicht auf, da hier die Kommunikation bereits abgeschlossen ist. Zum anderen ist bereits die Erkennung von Viren in eingehenden Daten ein Problem, da beliebig viele Verschlüsselungs- und Kodierungsverfahren angewendet werden können, z. B. HTTPS oder verschlüsselte E-Mail. Auch dieses Problem tritt auf den Endsystemen nicht mehr auf, da hier die eingegangenen Programme und Dokumente in ihrer vollständigen, unverschlüsselten Form vorliegen und daher mit den üblichen Verfahren geprüft werden können.

2.3.5 Erkennen von internen Angriffen

Bei der Angriffserkennung sind nicht nur Angriffe von außen zu betrachten. Ein Großteil aller Sicherheitsverletzungen wird von Innentätern initiiert. Gegen diese Art von Angriffen bieten Sicherheitsgateways am Netzübergang typischerweise keinen Schutz, da in der Regel die Kommunikation von innen nach außen gewollt ist. Die interne Seite eines Netzübergangs kann daher auch ein Angriffsziel sein, deshalb müssen auch für diese Fälle entsprechende Maßnahmen ergriffen werden, wie z. B. der Einsatz entsprechender Sensoren eines IDS.

---

[3] Ein Dienstprogramm ist ein (meist kleines) Hilfsprogramm und Bestandteil des Betriebssystems. Es dient zur Ausführung einer Hilfsfunktion, in der Regel bei der Systemverwaltung des Computers.

[4] Dies betrifft insbesondere Programme, die mit erweiterten Rechten ausgestattet sind („setuid"-Programme).

2.3.6 Anforderungen an die sichere Inbetriebnahme

Inbetriebnahme und Rekonfiguration eines Sicherheitsgateways stellen, vom Sicherheitsstandpunkt aus betrachtet, besonders kritische Phasen dar, da u. U. in der Default-Konfiguration eine Vielzahl von Diensten aktiviert sind. Daraus können sich Sicherheitsprobleme ergeben. Folglich sollten nur Dienste aktiviert sein, die für den Betrieb notwendig sind. Nicht benötigte Dienste müssen deaktiviert werden, weil sie ein erhöhtes Risiko darstellen.

2.3.7 Anforderungen an eine sichere Administration

Um Sicherheit auch bei der Administration des Sicherheitsgateways zu erreichen, ist das Prinzip der Funktionstrennung zu beachten. So ist es empfehlenswert, der Administration und der Auswertung von Protokolldaten separate Rollen zuzuweisen.

Alle administrativen Zugriffe auf das Sicherheitsgateway sollten nur über sichere Kanäle erfolgen. Dies gilt insbesondere für Fernwartung und dezentrale Verwaltung, bei denen die Identität der Administratoren durch geeignete Authentisierungsverfahren hinreichender Stärke zu prüfen ist. Wird ein separates Managementnetz eingesetzt, ist zu beachten, dass die Trennung der Netzsegmente (DMZs) im Managementnetz ebenfalls implementiert wird. Es ist zu vermeiden, dass Trennsysteme über Management- oder IDS-Netze „umgangen“ werden können. Direkte Managementverbindungen aus dem LAN in sicherheitsrelevante Teilnetze (DMZs) sind zu vermeiden. Für Zugriffe in Zonen unterschiedlichen Schutzbedarfs sind Proxy- bzw. Hop-Systeme zu verwenden. Hop-Systeme sind Gateways, auf die zuerst eine Verbindung initiiert werden muss, um auf das eigentliche Zielsystem gelangen zu können. Diese Systeme verlangen eine starke Authentisierung, bevor eine weitere (Management-)Verbindung auf das Zielsystem eingeleitet werden kann.

Alle Änderungen der Konfiguration eines Sicherheitsgateways müssen protokolliert werden. Zugriffsrechte für Objekte auf dem Sicherheitsgateway sollten restriktiv gesetzt sein.

2.3.8 Anforderungen an den sicheren Betrieb

Das *„default-deny“*-Prinzip ist zu implementieren, d. h., alles, was nicht explizit erlaubt ist, ist verboten. Insbesondere sollte nach einem „Absturz“ eines Sicherheitsgateways bis zu dessen vollständigem und ordnungsgemäßem Wiederanlauf keine Kommunikation über die zu schützenden Wege mehr möglich sein.

Falls festgestellt wird, dass die Integrität der Systemsoftware verletzt ist, ist jegliche Dienstnutzung automatisch zu sperren. Auch nach der Installation der Software ist die Konfiguration der Systeme regelmäßig zu prüfen. Aktuelle *Security Patches* zu den Systemen sind nach Erscheinen unverzüglich zu kontrollieren und bei Verträglichkeit mit dem System zu installieren.

Es ist eine aktuelle Dokumentation zu pflegen, in der alle Betriebsaspekte berücksichtigt werden. Nachfolgend werden wesentliche Prozesse des Betriebshandbuchs aufgelistet:

- Verantwortungen, Rollenverteilungen, beteiligte Partner
- Change-Management, Festlegung von Testprozeduren vor Inbetriebnahme und während des Betriebs
- Wartungszeiträume, Update-, Upgrade-Intervalle, Terminplanung für Wartungsintervalle, Kalenderplan usw.
- Dokumentation der aktuellen Konfigurationen
- Dokumentationsrichtlinien für Installationen, Updates, Konfigurationsänderungen usw.

- Regelungen für die Inbetriebnahme mit Fall-Back-Prozeduren oder nach Änderungen
- Eskalationswege im Fehlerfall, Ansprechpartner im Haus und bei externen Firmen, Wartungs- und Supportverträge inkl. Ansprechpartner
- Behebung von Funktionsstörungen
- Backup- und Wiedereinspielprozesse
- Überwachung
- Notfallvorsorge-Konzept

2.3.9 Anforderungen an die diensteübergreifende Beweissicherung

Über die Grundfunktion „Beweissicherung“ hinaus, die für jeden Dienst spezifiziert wird, gibt es bei der Aufzeichnung von Systemereignissen an Netzübergängen weitere Anforderungen und Randbedingungen, die in einem Sicherheitskonzept betrachtet werden sollten. Auf diese wird in den folgenden drei Kapiteln genauer eingegangen.

Anforderungen an die diensteübergreifende Protokollierung

Zunächst sind die jeweiligen gesetzlichen Rahmenbedingungen zu beachten. Die folgenden Gesetze können dabei für die Protokollierung relevant sein:

- Sozialgesetzbuch (SGB)[5] einschließlich der darin enthaltenen Gesetze zum Sozialdatenschutz in § 35 SGB I und SGB X
- Telekommunikationsgesetz (TKG)
- Teledienstegesetz (TDG)
- Tledienstedatenschutzgesetz (TDDSG)
- Telekommunikationsüberwachungsverordnung (TKÜV)
- Telekommunikationsdatenschutzverordnung (TDSV)

Des Weiteren können die Verwaltungsverordnungen für den Bereich des Rechnungswesens (SVRV[6] und SRVwV[7]) relevant sein.

Die genannten Gesetze und Verordnungen enthalten nicht nur Regelungen zur Protokollierung, sondern allgemeine Anforderungen zur IT-Sicherheit.

Sofern personenbezogene Daten protokolliert bzw. archiviert werden, ist zu prüfen, ob die Vorschriften des Bundesdatenschutzgesetzes (BDSG) anzuwenden sind. Die Anforderungen des BDSG spiegeln sich auch in den „Grundsätzen für eine ordnungsmäßige Datenverarbeitung (GoDV)“ wider. Das BDSG verlangt insbesondere die Zweckgebundenheit der Datenverarbeitung und in der Folge daraus die Löschung archivierter Daten nach Wegfall des Verarbeitungszwecks.

In allen Fällen ist zu prüfen, ob das jeweilige Landesrecht (LDSG) anstelle des BDSG anzuwenden ist. Wesentliche Regelungskriterien sind üblicherweise die Aufbewahrungsdauer sowie der Vertraulichkeits- und Integritätsbedarf, wobei bei Letzteren neben der Stärke auch die Zeitdauer des Schutzbedarfs eingeht.

---

[5] Einzelvorschriften aus dem SGB gehen dem BDSG vor.

[6] Sozialversicherungs-Rechnungsverordnung

[7] Allgemeine Verwaltungsvorschrift über das Rechnungswesen in der Sozialversicherung

Anforderungen an die diensteübergreifende Auswertung von Protokolldaten

Um die Auswertbarkeit der Protokolldaten zu erleichtern, ist darauf zu achten, dass Umfang und Art der protokollierten Daten so konfigurierbar sind, dass diese Daten in einem einheitlichen Format erfasst werden (z. B. im *SYSLOG*-Format von UNIX) und auf andere Systeme exportierbar sind (z. B. an einen über die serielle Schnittstelle angeschlossenen PC oder Protokolldrucker oder an eine zentrale Aufbewahrungs- und Auswertestelle). Die Protokolldaten sind zu überwachen.

Generell ist unbedingt darauf zu achten, dass die Protokollierung so manipulationssicher erfolgt, wie es den Umständen entsprechend zu fordern ist. An besonders gefährdeten Systemen sollte aus diesen Gründen die Protokollierung auf einem dedizierten System erfolgen.

Weiterhin sollte ein möglichst großer Teil der Auswertung durch geeignete Werkzeuge automatisch erfolgen können. Bei Ausfall der Protokollierung (z. B. durch erschöpftes Speichermedium) muss ein Alarm generiert und die weitere Nutzung der Dienste unterbunden werden, bis die Protokollierung wieder aktiv ist.

Anforderungen an die diensteübergreifende Generierung von Alarmen

Bei akuten Bedrohungen muss das Sicherheitsgateway in der Lage sein, zuständige Systemadministratoren auf individuell konfigurierbare Arten zu alarmieren. Dabei sollten verschiedene Alarmierungsformen möglich sein, z. B. Versenden von E-Mail, Auslösen von Aktionen mittels SNMP oder Ausführen von anderen Programmen. Welche konkreten Anlässe zu Alarmen führen, sollte ebenfalls konfigurierbar sein.

2.4 Anforderungen an die Architektur von Netzübergängen

Neben den vorgenannten Sicherheitsanforderungen sind an einen Netzübergang (Sicherheitsgateway) im Rahmen der Realisierung weitere Anforderungen zu stellen. Diese Anforderungen betreffen vor allem architekturrelevante Aspekte. Hierzu gehören:

- Mehrstufigkeit
- Verfügbarkeit der Gesamtlösung
- Management des Sicherheitsgateways
- Qualität der eingesetzten Produkte
- Support, Wartung
- Migrationsfähigkeit
- Erweiterbarkeit
- Wirtschaftlichkeit

2.4.1 Mehrstufigkeit

Vor allem beim Einsatz von Sicherheitsgateways zur Absicherung von Anbindungen an das Internet ist der Aufbau eines mehrstufigen Systems empfehlenswert, um alle Sicherheitsanforderungen umsetzen zu können. Aus den folgenden Gründen wird ein dreistufiges System empfohlen, das aus Komponenten bestehen soll, denen mindestens zwei unterschiedliche Techniken/Hersteller zugrunde liegen. Die unterschiedlichen Techniken/Hersteller sind erforderlich, damit sich ein grundsätzlicher Implementierungs- oder Konfigurationsfehler nicht auf allen Stufen des Schutzsystems auswirkt.

- Externer Paketfilter
  Der externe Paketfilter schützt das nachfolgende Application-Level-Gateway (ALG) u. a. gegen Port-Scans und Angriffe auf das Betriebssystem. Speziell bei reinen Proxy-Gateways sind Ports, die vom Betriebssystem zur Verfügung gestellt werden, erreichbar. Der Paketfilter soll nur Verbindungen aus dem Internet zulassen, die für den Betrieb erforderlich sind, wie z. B. Mail (SMTP) und DNS.
- Application-Level-Gateway
  ALGs, auch Sicherheits-Proxies genannt, unterbrechen den direkten Datenstrom zwischen Quelle und Ziel. Bei einer Kommunikationsbeziehung zwischen Client und Server über einen Proxy hinweg nimmt der Proxy die Anfragen des Clients entgegen und leitet sie an den Server weiter. Bei einem Verbindungsaufbau in umgekehrter Richtung, also vom Server zum Client, verfährt der Proxy analog. Sämtliche Kommunikationsbeziehungen zwischen den beiden Rechnern verlaufen in diesem Fall also mittelbar über den Proxy. Diese Kommunikationsform ermöglicht es einem Proxy beispielsweise, die übertragenen Daten inhaltlich zu kontrollieren oder bestimmte Protokollbefehle zu filtern.
- Interner Paketfilter
  Der interne Paketfilter wird als „last line of defense“ betrachtet, wenn Application-Level-Gateway und externer Paketfilter versagen. Ferner bietet er einen gewissen Schutz gegen Angriffe von innen. Durch Fehlkonfigurationen oder Softwarefehler auf dem Application-Level-Gateway besteht die Möglichkeit, dass ein Angreifer Zugriff auf dieses System oder ein anderes in der DMZ erhält. Der interne Paketfilter sollte nur die Verbindungen zulassen, die an das Application-Level-Gateway gerichtet sind und die laut Sicherheitskonzept erlaubt sind.

2.4.2 Verfügbarkeit der Gesamtlösung

Neben der Verfügbarkeit auf Diensteebene spielt auch die Verfügbarkeit des Gesamtsystems eine Rolle. Da Nichtverfügbarkeit des Sicherheitsgateways i. d. R. auch die Nichtverfügbarkeit der geschützten Netzverbindung bedeutet (oder zumindest bedeuten sollte), ist es besonders wichtig, bei notwendigen Wartungsarbeiten am Sicherheitsgateway mögliche Offline-Zeiten kalkulieren zu können. Je seltener Offline-Zeiten erforderlich sind und je kleiner diese Zeitspanne ausfällt, desto besser für die Gesamtverfügbarkeit des Überganges. Die Offline-Zeiten lassen sich u. a. durch die gute Vorbereitung der Wartungsarbeiten minimieren.

2.4.3 Management des Sicherheitsgateways

Je einfacher das Sicherheitsgateway zu administrieren ist, desto leichter fällt es, den Überblick über die Konfiguration zu behalten, und desto weniger wahrscheinlich werden zufällige Fehler in der Konfiguration, welche die Sicherheit negativ beeinflussen. Daher ist es empfehlenswert, dass eine intuitiv bedienbare und übersichtlich gestaltete Administrationsoberfläche zur Verfügung steht. Allgemeine Grundsätze der Softwareergonomie sollten beachtet worden sein (z. B. Benutzerführung durch Menüs, Sicherheitsabfragen vor sicherheitsrelevanten Änderungen).

Darüber hinaus sollten zur Administration und zur Systemüberwachung möglichst wenige Systemprivilegien erforderlich sein.

2.4.4 Qualität der eingesetzten Systeme

An die Sicherheitsgateways wird eine Reihe von allgemeinen Qualitätsanforderungen gestellt. Die einzelnen Systemkomponenten müssen nach Möglichkeit in einer geschützten Umgebung ablaufen, so dass bei Fehlfunktionen einzelner Komponenten Folgewirkungen begrenzt bleiben. Die Bereitstellung des Quellcodes ermöglicht eine detaillierte Untersuchung der Programme und ist daher wünschenswert.

Systeme, die mit einem Sicherheitszertifikat ausgezeichnet wurden, sind bereits von unabhängiger Seite geprüft worden, wodurch die Wahrscheinlichkeit von Sicherheitsproblemen reduziert ist.

Open-Source-Systeme bieten grundsätzlich die Möglichkeit einer qualifizierten Überprüfung durch die Offenlegung des Quellcodes.

2.4.5 Support, Wartung

Zu den üblichen Geschäftszeiten sollte eine Hotline für das Sicherheitsgateway bereitstehen, um bei der Lösung konkreter Probleme zu helfen. Für Probleme, die eine Vor-Ort-Betreuung erfordern, ist eine möglichst kurze Reaktionszeit einzuhalten. Updates zur Behebung von Programmfehlern sind so schnell wie möglich bereitzustellen. Auf gemeldete Sicherheitsprobleme sollte der Hersteller schnell reagieren und für Abhilfe sorgen.

2.4.6 Migrationsfähigkeit

Das System sollte ohne große Schwierigkeiten an neue technische Entwicklungen anzupassen sein, insbesondere an neue Kommunikationsstandards (z. B. IPv6) und größere Kommunikationsbandbreiten.

2.4.7 Erweiterbarkeit

Das Sicherheitsgateway muss unkompliziert an neue Dienste anpassbar sein (z. B. Erstellung neuer Proxies). Weitere Sicherheitsmaßnahmen (z. B. zusätzliche Authentisierungsverfahren) sollten integrierbar sein.

Zu prüfen ist, ob durch den Einsatz von Open-Source-Lösungen, bei denen der Quellcode typischerweise verfügbar ist, eigene Anpassungen an spezielle Anforderungen, z. B. in Bezug auf weniger gebräuchliche Dienste, erleichtert werden.

2.4.8 Wirtschaftlichkeit

Insgesamt muss die konzipierte Lösung auch unter wirtschaftlichen Gesichtspunkten tragbar sein. Eine Kosten-Nutzen-Analyse sollte daher in einem Sicherheitskonzept immer enthalten sein.

2.5 Zusammenfassung

Das Kapitel „Integration von Netzübergängen“ geht schwerpunktmäßig auf die Vorgehensweise zur Erstellung eines Sicherheitskonzepts im Rahmen der Planung, Realisierung und Inbetriebnahme eines Netzübergangs ein. Dies gilt nicht nur für die Neuerstellung, sondern analog auch für den Umbau bestehender Netzübergänge.

Es wurde die Bedeutung der Sicherheitsanforderungen auf unterschiedlichen Ebenen (dienstespezifisch, diensteübergreifend und Anforderungen an die Netzarchitektur) gezeigt. Insbesondere wurde dargestellt, wie mit Hilfe von Sicherheitsmaßnahmen und weiteren Anforderungen die Basis eines Sicherheitskonzepts gebildet werden kann.

Die dargestellten Anforderungen können u. a. dazu verwendet werden, für unterschiedliche Typen von Netzübergängen das richtige System auszuwählen.

Im Rahmen der Revision von Netzübergängen stellen die Sicherheitsmaßnahmen Anforderungen dar, die eingesetzte Produkte, entsprechend dem Schutzbedarf der Daten, zum Schutz eines Netzübergangs erfüllen müssen.

3 IT-Revision

Informationstechnik (IT) wird heute in allen denkbaren Bereichen der Kommunikation, der Produktion oder auch bei der Durchführung von Finanztransaktionen und bei Finanzverwaltungen eingesetzt. Kern des Einsatzes sind immer konkrete Anforderungen an die Funktionalität der eingesetzten IT. Aufgabe der Revision ist es, diese Anforderungen mit der tatsächlichen Realisierung zu vergleichen und Unterschiede oder Mängel aufzuzeigen. Des Weiteren überprüft die Revision die Aktualität des Sicherheitskonzepts und des Notfallvorsorge-Konzepts.

Nach der detaillierten Beschreibung, welche Sicherheitsanforderungen an einen Netzübergang zu stellen sind und wie diese im Rahmen eines Sicherheitskonzepts festzuschreiben sind, wird im folgenden Abschnitt die IT-Revision von Netzübergängen behandelt.

Unter IT-Revision[8] soll dabei die systematische Prüfung der Erfüllung und Umsetzung der Sicherheitsvorgaben verstanden werden.

Der Ablauf einer IT-Revision wird in diesem Leitfaden mit einem modularen Ansatz als Prozess beschrieben. Dabei werden die einzelnen Schritte einer Revision von der Vorbereitung über die Durchführung bis hin zum Abschluss in einzelne Teilschritte zerlegt. Die in den einzelnen Schritten durchzuführenden Aufgaben sowie die daran beteiligten organisatorischen Rollen und die erwarteten Ergebnisse werden im Einzelnen dargestellt.

Auch die Revisionsobjekte werden modular strukturiert[9]. Ausgehend von den Kernmodulen Szenarien, Dokumentation, Betriebsprozesse und Komponenten werden einzelne konkrete Objekte einer Revision als Blatt in einem strukturierten Baum abgebildet. Diese Darstellung erleichtert die Gliederung einer Revision und hilft sowohl bei der Durchführung als auch bei der Erfassung und Bearbeitung neuer, bislang nicht behandelter Objekte, beispielsweise bei einer neuen IT-Komponente.

Zu Beginn des Kapitels werden grundlegende Revisionsmethoden diskutiert.

---

[8] Der Begriff IT-Revision soll im Kontext dieser Studie gleichbedeutend zum Begriff IT-Audit verwendet werden. Die handelnde Person ist somit der IT-Revisor bzw.IT-Auditor. Als Verb wird in diesem Kontext „auditieren“ oder „prüfen“ verwendet.

[9] Zu den einzelnen Revisionsobjekten befinden sich Checklisten in Teil II dieses Leitfadens.

3.1 Methoden der IT-Revision

Eine IT-Revision kann in ihrem Ziel sehr unterschiedliche Ausprägungen haben. Die Möglichkeiten reichen von der Prüfung, ob ein gegebenes System die gestellten Anforderungen in Form von internen Regeln oder Richtlinien sowie geltenden Gesetzen und Vorschriften einhält, über die Prüfung, ob ein System die versprochenen Eigenschaften und Verhaltensweisen tatsächlich erfüllt, bis hin zur Verifikation, ob ein implementierter Algorithmus vollständig und richtig im Sinne der gestellten Anforderungen funktioniert.

Im Folgenden werden unterschiedliche Arten bzw. Ansätze zur Durchführung einer Revision beschrieben sowie herausgearbeitet, welche Methode diese Studie für die IT-Revision von Netzübergängen vorsieht.

Um Überschneidungen mit bereits bestehenden Studien des BSI zu vermeiden, erfolgt zunächst eine Abgrenzung zur BSI-Studie „Durchführungskonzept für Penetrationstests“ [BSI-PENTEST].

3.1.1 Abgrenzung zu Penetrationstests

Die Studie [BSI-PENTEST] geht von der Annahme aus, dass ein System Schwachstellen hat und diese durch entsprechende Werkzeuge entdeckt oder ausgenutzt werden können. Demzufolge wird dort eine Vorgehensweise zur Durchführung eines Penetrationstests nach dem folgendem Schema vorgestellt:

- Recherche nach Informationen über das Zielsystem
  Im Internet erreichbare Rechner müssen über eine offizielle IP-Adresse verfügen. Frei zugängliche Datenbanken liefern Informationen über IP-Adressblöcke, die einer Organisation zugewiesen sind.
- Scan der Zielsysteme auf angebotene Dienste
  Hierbei wird versucht, den oder die zu überprüfenden Rechner u. a. einem sog. Port-Scan zu unterziehen, wobei evtl. geöffnete Ports Rückschlüsse auf die zugeordneten Anwendungen zulassen.
- System- und Anwendungserkennung
  Über das sog. „Fingerprinting“ können Namen und Versionsnummern von Betriebssystemen und Anwendungen auf den Zielsystemen in Erfahrung gebracht werden.
- Recherche nach Schwachstellen
  Anhand der gewonnenen Informationen können zielgerichtet Informationen über Schwachstellen bestimmter Betriebssysteme und Anwendungen gesucht werden.
- Ausnutzen der Schwachstellen
  Gefundene Schwachstellen können dazu genutzt werden, unberechtigten Zugriff zum System zu erhalten bzw. weitere Angriffe vorzubereiten.

Ferner werden in der Studie verschiedene Typen von Penetrationstests klassifiziert, wie z. B. die Unterscheidung nach der **Informationsbasis** (wo grundsätzlich unterschieden wird zwischen sog. Black-Box-Testing ohne jegliches Insiderwissen und dem White-Box-Testing mit Insiderwissen), **Aggressivität** (passiv scannend/abwägend/vorsichtig/aggressiv), **Umfang** (vollständig/begrenzt/fokussiert) und weiteren Kriterien.

Es ist leicht einzusehen, dass hier das Auffinden von Schwachstellen im Vordergrund steht. Dies sagt aber zunächst noch nichts darüber aus, ob dadurch eventuelle Sicherheitsvorgaben verletzt werden oder sich aus einer bestimmten Schwachstelle auch ein konkretes Risiko ergibt.

Wie im folgenden Abschnitt gezeigt wird, verfolgt dieser Leitfaden den Ansatz, Prüfungen eines vorgegebenen Soll-Zustandes mit einem vorgefundenen Ist-Zustand durchzuführen. Penetrationstests stellen dabei eine Methode dar, die für das nachfolgend dargestellte „Substantive Audit“ eingesetzt werden kann.

3.1.2 Methoden für eine umfassende IT-Revision

Im Folgenden werden zwei Revisionsansätze beschrieben, die beide jeweils eine mögliche Form der Überprüfung darstellen. Im Sinne einer vollständigen Revision werden diese Ansätze aber eher als Module angesehen, die nur in ihrer Gesamtheit eine vollständige und umfassende Revision darstellen und ermöglichen.

„Compliance Audit“ (Ordnungsmäßigkeit)

Unter Compliance Audit wird eine Prüfung auf Übereinstimmung mit den geltenden internen Regelungen wie Sicherheitsleitlinie, Betriebshandbücher oder andere interne Vorgaben auf der einen Seite sowie mit den geltenden externen Vorgaben wie Gesetze, Vorschriften oder Richtlinien auf der anderen Seite verstanden.

Das bedeutet, dass zunächst alle geltenden und aktuellen internen und externen Vorgaben zu sammeln und auf konkrete Anforderungen in Bezug auf den Revisionsgegenstand auszuwerten sind. Dies können Anforderungen an die Konfiguration einzelner Systembestandteile, an die Architektur der Netze, bezüglich einzuhaltender Funktionstrennung einzelner administrativer oder operationeller Aufgaben oder auch Vorgaben bezüglich einzuhaltender Wartungs- und Administrationsprozesse sein.

Diese Vorgaben sind objektspezifisch vollständig zu identifizieren und innerhalb der Revision einzeln auf Übereinstimmung zu prüfen. Diese Überprüfung kann durch das Auswerten der Konfigurationsparameter eines Systems, durch Interviews der verantwortlichen Administratoren, durch Beobachten einzelner Handlungen verantwortlicher Personen oder durch persönliche Augenscheinnahme des Revisors geschehen.

Vorteile: Ein Compliance Audit verschafft einen Überblick über die Anforderungen, die an einen Revisionsgegenstand grundsätzlich gestellt werden, und prüft, ob diese Anforderungen auf Konfigurationsebene und auf Betriebsprozessebene eingehalten werden.

Nachteile: Korrekte Konfiguration und korrekt implementierte Betriebsprozesse lassen nur bedingt auf die korrekte Verhaltensweise der Komponenten an sich schließen. Ein Nachweis dessen kann mit einem Compliance Audit nicht geführt werden.

Bewertung: Ein Compliance Audit ist ein erster, wichtiger Schritt in einer Revision. Durch diese Art der Prüfung alleine ist aber keine belastbare Aussage möglich.

„Substantive Audit“ (Nachweis)

Ein Nachweistest weist die korrekte Funktion der Systembestandteile gemäß Anforderungen und Konfiguration nach. Das bedeutet für einen Netzübergang, dass gemäß Bestimmungen im Detail nachzuprüfen ist, ob tatsächlich bestimmte Kommunikationen unterbunden, andere zugelassen oder bestimmte Verbindungen verschlüsselt werden. Es wird überprüft, ob eine korrekte Authentisierung durchgeführt wird oder auch bestimmte Anwendungseigenschaften zugelassen oder abgewiesen werden. Wichtig ist ebenfalls die Überprüfung, ob Alarmierungen tatsächlich stattfinden.

Ein Nachweistest geht also einen Schritt weiter, als die Konfiguration zu prüfen. Das Verhalten der Komponenten sowie die Kommunikationseigenschaften eines Netzübergangs werden im Detail überprüft und verifiziert.

Dazu können auch ggf. spezielle Tools eingesetzt werden, die es erlauben, Netzverkehr zwischen einzelnen Komponenten im Detail auszuwerten oder auch automatisiert Konfigurationen einzelner Systeme zu prüfen und zu analysieren.

Eine derart toolgestützte Analyse ist in keinem Fall mit „Hacking“ gleichzusetzen, da es an dieser Stelle darum geht, Systemeigenschaften und -verhalten zu analysieren und zu bewerten, in der Regel jedoch nicht darum, gefundene Schwachstellen auszunutzen.

Vorteile: Das Compliance Audit wird durch ein Substantive Audit sinnvoll ergänzt, sodass insgesamt ein vollständigeres Bild entsteht und verlässlichere Aussagen über die korrekte Funktion der Systembestandteile getroffen werden können.

Nachteile: In bestimmten Fällen sind korrekte Nachweise nur äußerst schwierig zu führen. Hier entsteht möglicherweise hoher Aufwand mit fraglichem Ausgang.

Bewertung: Grundsätzlich eine wichtige Ergänzung zum Compliance Audit.

3.2 Prüfmodule für die IT-Revision

Um bei einer Revision einen vollständigen und umfassenden Überblick zu bekommen, ist es notwendig, nicht nur die Hardware oder die Konfiguration einzelner Elemente zu analysieren und zu bewerten, sondern auch Betriebsprozesse und Dokumentationen bei der Untersuchung zu berücksichtigen.

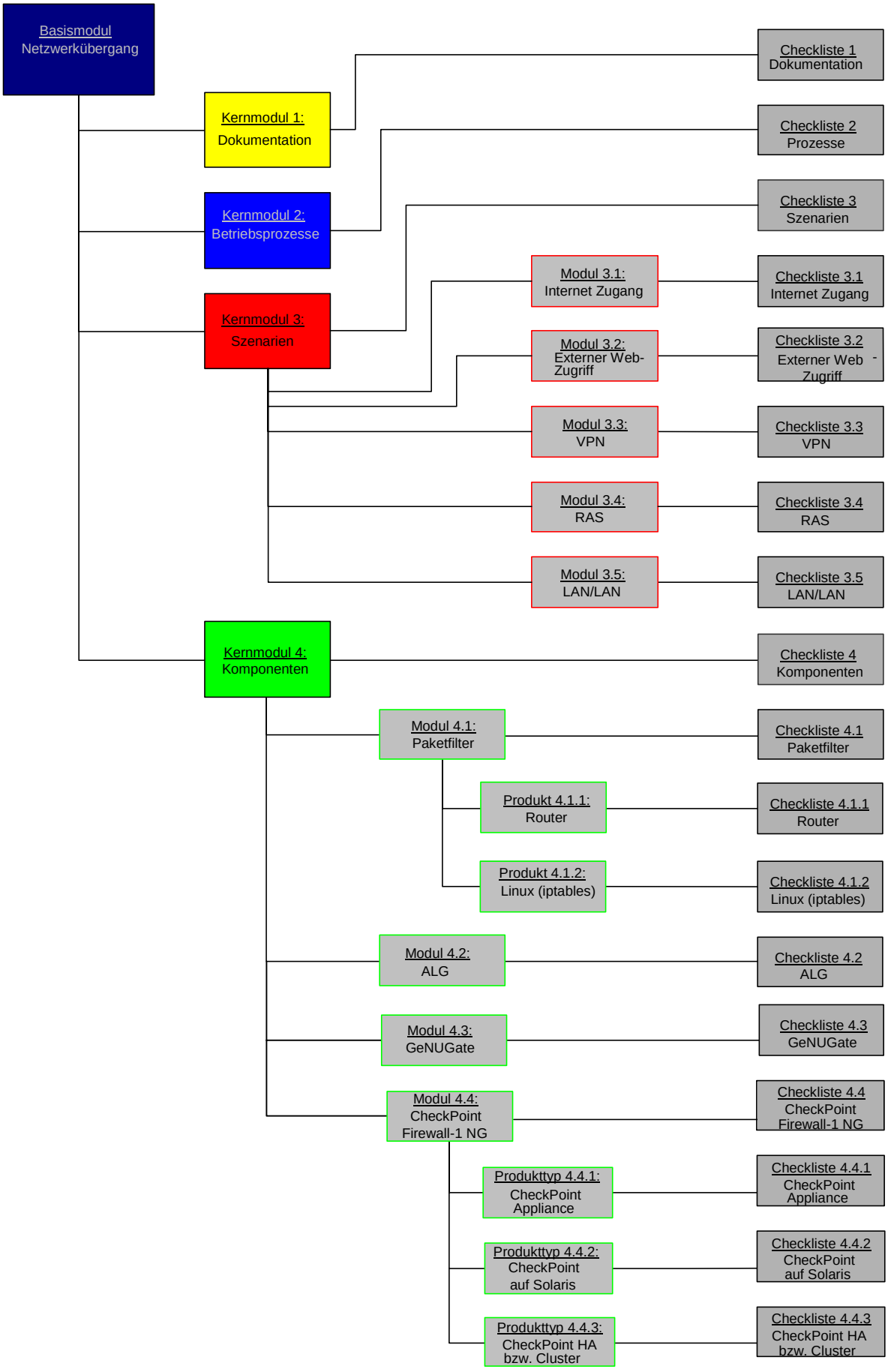


Abbildung 3: *Übersicht der Revisionsmodule*

Zur Sicherstellung der Vollständigkeit wird hier daher ein modularer Aufbau einer Revision vorgestellt. Ausgehend von dem Basismodul „Netzübergang“ zeigt die Abbildung 3 die einzelnen Module, die sich in vier Kernmodule aufteilen:

- Dokumentation,
- Betriebsprozesse,
- Szenarien und
- Komponenten.

Diese Kernmodule sind zum Teil noch einmal in verschiedene Module und Produkte unterteilt (s. Abb. 3), die es ermöglichen, einen konkreten Netzübergang nach technologischen, organisatorischen, personellen und infrastrukturellen Aspekten systematisch abzudecken. In dem so aufgespannten Baum finden sich am Ende eines jeden Astes Checklisten, auf die im Teil II „Revisionshilfsmittel“ detailliert eingegangen wird.

Zu beachten ist dabei, dass die in Abbildung 3 dargestellten Prüfmodule keine in sich abgeschlossene Zusammenstellung repräsentieren, sondern jederzeit weitere Module hinzugefügt werden können.

Für die konkrete Revision eines Netzübergangs sind aus jeder der vier Kernmodule die relevanten Einzelmodule mit den zugehörigen Checklisten auszuwählen.

Nachfolgend werden die o. g. Kernmodule näher erläutert.

Dokumentation

Neben den konkreten Betriebsprozessen ist eine vollständige Dokumentation notwendig, in der alle wesentlichen Aspekte festgelegt wurden. Folgende Aspekte sollten dokumentiert sein:

- Verantwortlichkeiten,
- Sicherheitsleitlinie, Sicherheitskonzept,
- Notfallvorsorge-Konzept,
- alle Betriebsprozesse (s. u.),
- Konfiguration,
- Software-Versionen und Patch-Level,
- Architektur- und Systemdokumentation,
- zugelassene Kommunikationen,
- berechtigte Personen sowie
- Fehlerhandbuch.

Betriebsprozesse

Damit Netzübergänge ihre Aufgabe zuverlässig und konstant erfüllen können, ist eine Reihe von „geordneten Tätigkeiten“ notwendig. Diese sollten in Form von Betriebsprozessen durchgeführt werden. Dazu gehören u. a. Administration und Wartung, Patches und Upgrades, Regeländerungen und Sicherung der Daten.

Szenarien

Bei Netzübergängen ist ausschlaggebend, welche Arten von Netzen sie miteinander verbinden sollen und welcher Zweck damit verbunden ist. Die zu beachtenden Sicherheitsanforderungen ergeben sich aus dem Sicherheitskonzept (vgl. Kap. 2) und können je nach Art des Kommunikationsbedarfs unterschiedliche Ausprägungen haben.

Nachfolgend werden einige Beispiele von typischen Netzübergängen beschrieben.

- **Internet-Zugang:**
  Dies ist der einfachste Fall einer Absicherung eines vertrauenswürdigen (internen) Netzes gegen ein nicht vertrauenswürdiges, externes Netz (Internet).

  Die Architektur eines Internet-Zugangs wird in Abbildung 4 gezeigt. Man sieht dort als „typische" Architektur eine einfache Anbindung ohne Extranet[10]/DMZ (Demilitarisierte Zone), wobei als Kontrollelemente eine Kombination der drei Komponenten Paketfilter, Application-Level-Gateway (ALG) und Paketfilter zur Anwendung kommt (vgl. [BSI-SICH-GW]).

  Voraussetzung dafür ist, dass weder eigene Web-Dienste innerhalb der Internet-Anbindung angeboten werden noch E-Mail aus Fremdnetzen direkt in das interne Netz zugestellt wird, so dass keine eingehenden Verbindungen erlaubt werden müssen.

  Dabei ist darauf zu achten, dass diese Kombination mit Komponenten unterschiedlicher Konzeption und Technologie realisiert werden sollte:

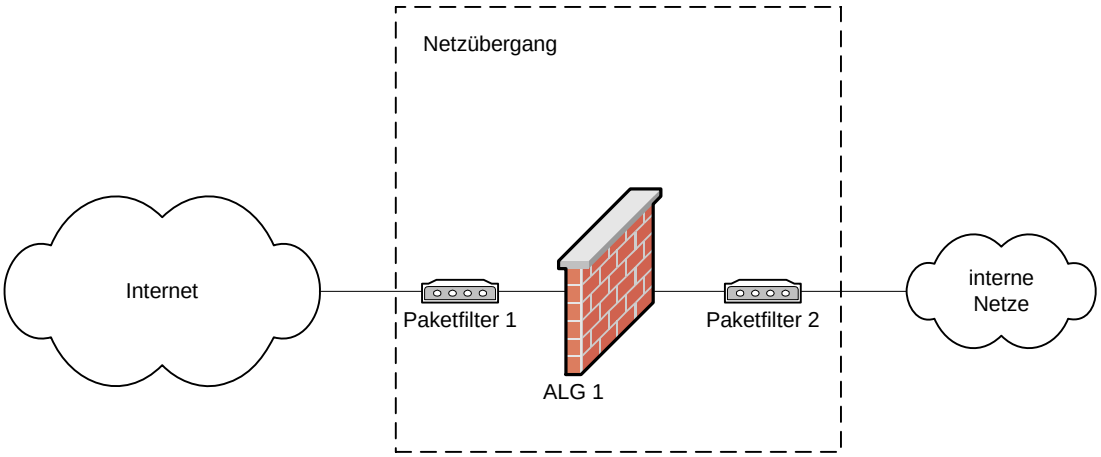


Abbildung 4: *Architektur Internet-Zugang*

[10] Unter „Extranet" versteht man den Anschluss eines weiteren Netzes an das eigene Intranet unter Verwendung der gleichen Techniken wie beim Internet (u. a. TCP/IP, UDP). Dieses Extranet hat einen höheren Schutzbedarf als das Internet, aber in der Regel einen niedrigeren Schutzbedarf als das eigene Intranet. Es befindet sich meistens unter fremder Kontrolle.

- **Externer Web-Zugriff**
  Dieses Szenario stellt eine komplexe Struktur mit einem mehrstufigen Sicherheitsgateway dar, um Web-, Applikations- und Datenbank-Server in verschiedenen DMZ zu plazieren und sie somit aus Sicherheitsgründen stärker voneinander zu trennen. Eine solche Struktur findet man typischerweise in eGoverment/eBusiness-Anwendungen. Vorausgesetzt wird dabei, dass in Erweiterung der o. a. Infrastruktur der Zugriff durch Externe aus dem Internet heraus auf eigene Systeme erfolgen soll, üblicherweise über eine Web-Schnittstelle (Portal-Technologie). Das Web-Portal könnte über eine Skript-Schnittstelle eine Middleware ansteuern, die wiederum die Kopplung zu internen (Datenbank-)Systemen bildet und ggf. selbst Abfragen bei Fremdsystemen über das Internet ansteuert (z. B. für die Validierung von Kreditkarten).

  Als „typische“ Infrastruktur für den externen Web-Zugriff könnte man eine Erweiterung der o. a. Internet-Anbindung mit zwei gestaffelten Extranet/DMZ entwerfen, wobei als Kontrollelement zwischen den beiden DMZ ein ALG dient (s. Abb. 5). Zusätzlich wird die zweite DMZ gegenüber den internen Netzen durch einen Paketfilter gesichert[11] (vgl. [BSI-SICH-GW]):

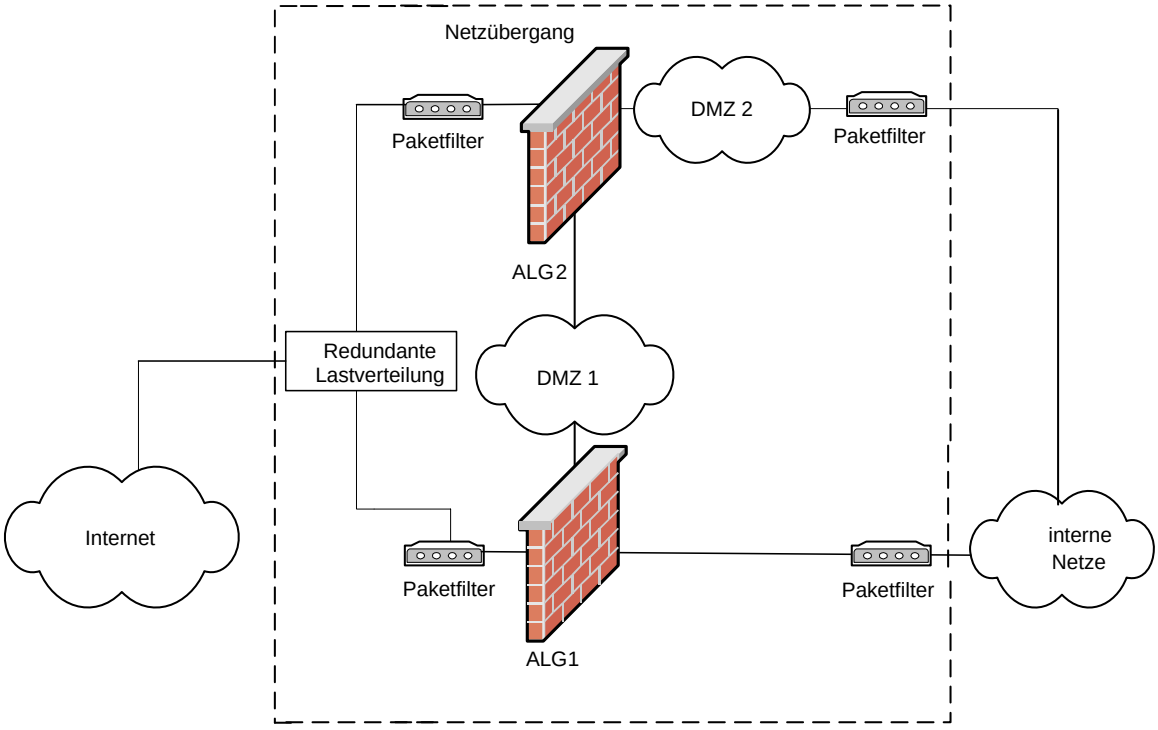


Abbildung 5: *Architektur Externer Web-Zugriff*

[11] Der Internet-Zugang für die Mitarbeiter soll dabei weiterhin durch die bestehende Kombination von Paketfilter/Application-Level-Gateway/Paketfilter realisiert werden, während der eingehende Datenverkehr durch die beiden zusätzlichen DMZ kanalisiert wird.

- **VPN (Virtuel Private Network) Zugang:**
  Ein VPN ist ein Netz, das physisch innerhalb eines anderen Netzes (meist des Internets) betrieben wird, jedoch logisch von diesem Netz getrennt wird. VPNs können unter Zuhilfenahme kryptographischer Verfahren die Integrität und Vertraulichkeit von Daten schützen und die Kommunikationspartner sicher authentisieren, auch dann, wenn mehrere Netze oder Rechner über gemietete Leitungen oder öffentliche Netze miteinander verbunden sind.

  Die Abbildung 7 zeigt die beiden prinzipiellen Möglichkeiten einer VPN-Verbindung. Der „VPN Tunnel I“ verbindet zwei vertrauenswürdige Netze über ein unsicheres drittes Netz.

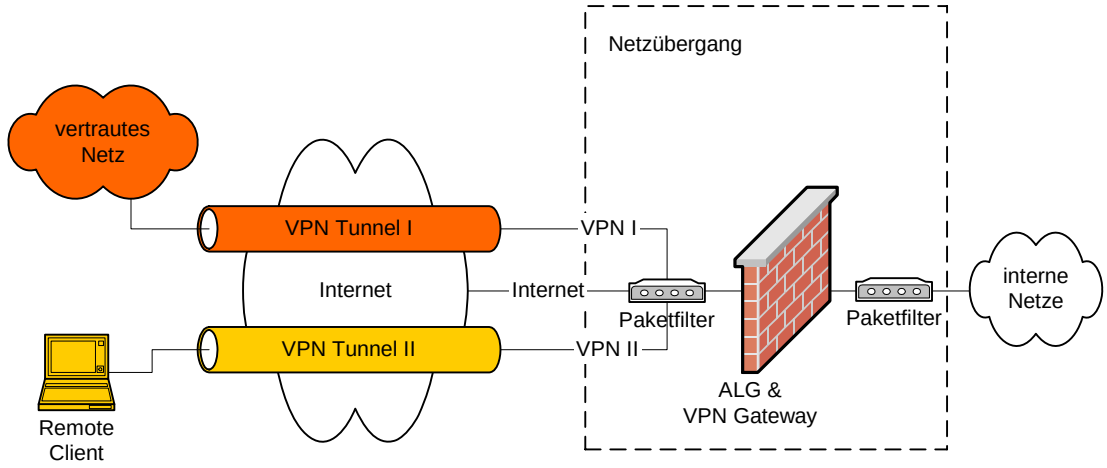


Abbildung 6: *Architektur VPN-Zugang*

Beim „VPN-Tunnel II“ wird ein einzelnes System mit einem vertrauenswürdigen Teilnetz verbunden. Dabei übernimmt üblicherweise eine Software-Applikation die VPN-Gateway Funktionalität auf dem Remote-Client.

Prinzipiell gelten für einen VPN-Zugang ähnliche Überlegungen wie sie für den RAS-Zugang (s. u.) beschrieben werden: Entweder werden die über ein VPN angebundenen Systeme als vollwertige, interne Systeme betrachtet und bedürfen keiner weiteren Sonderbehandlung oder die angebundenen Systeme werden nicht als eigentlich interne Systeme betrachtet, wie es z. B. bei einem Fernwartungszugriff durch Dritte der Fall ist. In diesem Fall kann man die gleiche Netzkopplung wie zwischen einem Extranet/DMZ unter fremder Kontrolle und dem internen Netz unterstellen und müsste folglich die Kommunikationsbeziehungen dementsprechend absichern.

Hinweis: Bei VS-Netzen und bei Netzen mit datenschutzrelevanten Daten (z. B. von Patienten) sowie firmenvertraulichen Daten wird die Fernwartung durch Dritte vom BSI generell nicht empfohlen.

Weiterhin sind zu beachten:

- VSA für Verschlusssachen,
- Geheimschutzhandbuch - Handbuch für den Geheimschutz in der Wirtschaft,
- Bundesdatenschutzgesetz.

- **RAS (Remote Access Service) Zugang:**
  Dies ist ein spezieller Einwahlzugang über Telefonie, um Zugriffe auf bestimmte Systeme bereitzustellen (Fernwartungsszenario) oder mobilen Mitarbeitern und Mitarbeitern an Heimarbeitsplätzen den mehr oder weniger unbeschränkten Zugriff auf interne Systeme zu ermöglichen.

  Man sollte einen solchen RAS-Zugang durch einen Paketfilter (s. Abb. 7) kontrollieren:

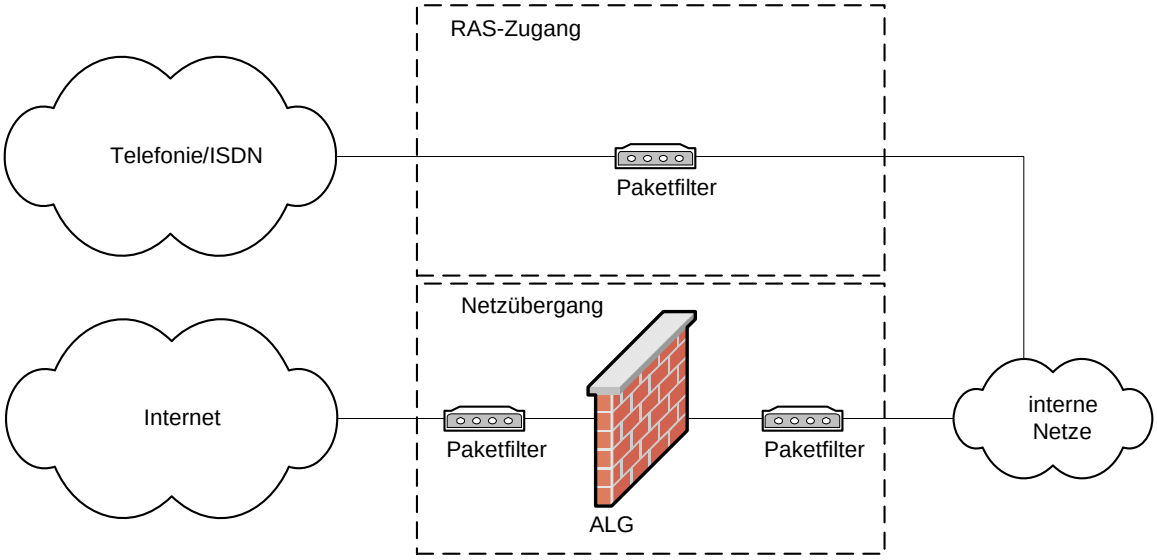


Abbildung 7: *Architektur RAS-Zugang und normaler Zugang*

Wenn das Sicherheitskonzept nach dem im Kapitel 2 beschriebenen Verfahren erstellt wird, müssen auch hier zunächst einmal Kommunikationsanforderungen und -beziehungen definiert werden.

Man kann sich auf den Standpunkt stellen, dass ein mobiler PC bei der (ggf. besonders stark abgesicherten) Einwahl in den RAS-Zugang wie ein interner PC am Büroarbeitsplatz behandelt wird. Dies ist nur dann zu empfehlen, wenn durch eine erfolgreiche Einwahl sämtliche anderen Netzschnittstellen des entfernten PC abgeschaltet werden und die gesamte Datenkommunikation ausschließlich über die Einwahlschnittstelle erfolgt. Dies setzt die vollständige Kontrolle über den entfernten PC voraus. Der PC sollte auch nur für diesen Zweck genutzt werden.

In einem Fernwartungsszenario wird man typischerweise nicht von den o. a. Überlegungen ausgehen können. In diesem Fall existiert in der Regel eine Netzkopplung zwischen einem Extranet/DMZ unter fremder Kontrolle und dem internen Netz und es müssten die Kommunikationsbeziehungen entsprechend abgesichert werden.

Hinweis: Bei VS-Netzen und bei Netzen mit datenschutzrelevanten Daten (z. B. von Patienten) sowie firmenvertraulichen Daten wird die Fernwartung durch Dritte vom BSI generell nicht empfohlen.

Weiterhin sind zu beachten:

- VSA für Verschlusssachen,
- Geheimschutzhandbuch - Handbuch für den Geheimschutz in der Wirtschaft,
- Bundesdatenschutzgesetz.

- **LAN/LAN-Kopplung:**
  Die LAN/LAN-Kopplung stellt eine interne Trennung zwischen zwei prinzipiell vertrauenswürdigen Netzen dar. Hierbei kann es sich um die Verbindung zweier Standorte handeln. Denkbar wäre auch, einen sensiblen Bereich (z. B. Finanzbuchhaltung oder Entwicklungsabteilung) gegen den Zugriff nicht berechtigter Personen abzusichern oder einen Bereich mit Publikumsverkehr (Bankschalter) gegen den Rest des internen Netzes abzuschotten.

  Eine LAN/LAN-Kopplung könnte, wie in Abbildung 8 gezeigt, durch ein Sicherheitsgateway realisiert werden. Dieses muss entsprechend dem Schutzbedarf der Teilnetze eingerichtet werden.

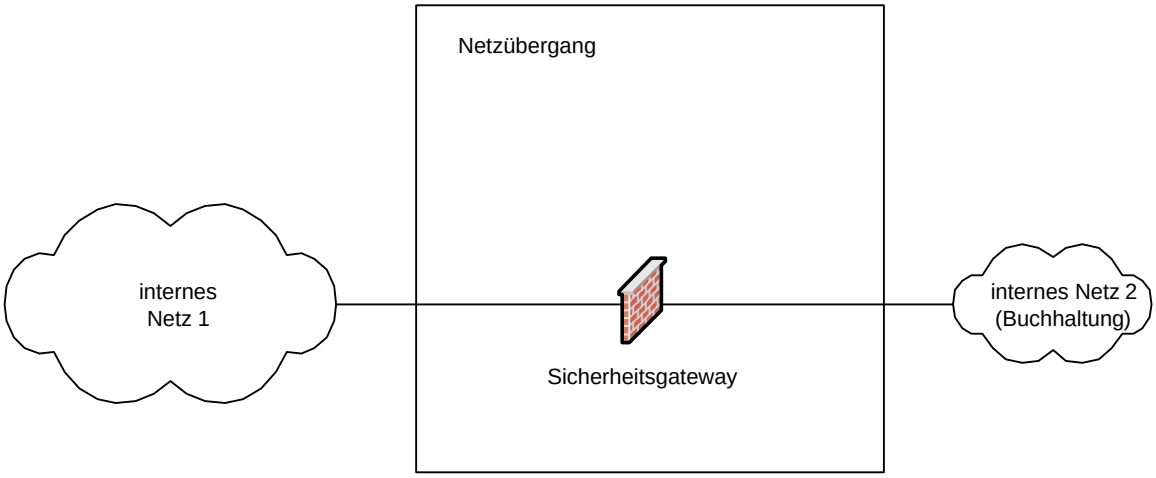


Abbildung 8: *Architektur LAN/LAN*

Wenn das Sicherheitskonzept nach dem im Kapitel 2 beschriebenen Verfahren erstellt wird, müssen zunächst einmal Kommunikationsanforderungen und -beziehungen definiert werden. Dies ist deshalb notwendig, weil zwischen internen Teilnetzen prinzipiell beliebig komplexe Kommunikationsbeziehungen und -anforderungen bestehen können; im Gegensatz zu einem „einfachen“ Internetzugang, der für gewöhnlich in die eine Richtung alles sperren und in die andere Richtung ein begrenztes Kommunikationsportfolio (z. B. E-Mail und HTTP) ermöglichen soll.

So könnte ein intern besonders schützenswertes Netz (Buchhaltung) zwar Kommunikationsbeziehungen in ein anderes internes Netz (Netz 1) aufbauen, aber Kommunikationsbeziehungen von Netz 1 zur Buchhaltung sind nicht zulässig.

Die oben genannten Szenarien können als generische Beispiele von typischen Netzübergängen verstanden werden, wobei die Übergangsformen zwischen diesen typischen Szenarien fließend sein können, wie das folgende Beispiel nahelegt:

Im Szenario Internet-Zugang geht es beispielsweise darum, ein internes vertrauenswürdiges Netz an das Internet anzubinden. Im Wesentlichen werden dabei Internet-Dienste für Systeme im internen Netz zugänglich gemacht, typischerweise die Nutzung eines Web-Browsers, Mail abrufen und versenden oder Dateien transferieren. Maßgeblich für dieses Szenario ist die grundsätzliche Einschränkung, dass Datenverbindungen immer von eigenen Systemen in das Internet initiiert werden. Jeder aktive Verbindungsaufbau von Internet-Systemen zu eigenen Systemen ist somit nicht zulässig und wird unterbunden. Alle Datenverbindungen werden also ausschließlich von eigenen Systemen aufgebaut.

Als Variante oder Erweiterung dieses Grundszenarios Internet-Zugang könnten beispielsweise die folgenden Erweiterungen gelten:

- Eingehende Mail wird nicht von internen Systemen abgerufen, sondern von externen Systemen einem internen System in das vertrauenswürdige Netz zugestellt: In diesem Fall muss die Zustellung eingeschränkt vom Internet aus über einen Proxy in das vertrauenswürdige Netz (DMZ) möglich sein.
- Es werden Informationen auf öffentlich zugänglichen Servern innerhalb des vertrauenswürdigen Netzes bereitgestellt. In diesem Fall müssen spezielle Datenverbindungen (HTTP-Protokoll sowie ggf. File-Transfer, FTP-Protokoll) eingeschränkt vom Internet aus in die DMZ möglich sein.

Bestehende (komplexere) Architekturen können auf die generischen Modelle durch Separation abgebildet werden, um Hinweise für die Revision zu erhalten. Wenn beispielsweise ein Internet-Zugang einer Institution gleichzeitig als VPN-Zugang dient, wird man die Revision der VPN-Funktionen mit den entsprechenden Hilfsmitteln abdecken, während die Internet-Zugangsfunktionen mit den Revisionskriterien des Internet-Zuganges abgedeckt werden können.

Die Häufigkeit der Revision von Netzübergängen richtet sich am ehesten nach folgenden Kriterien:

- Sicherheitsgefälle:
  Je größer das Sicherheitsgefälle zwischen zwei verbundenen Teilnetzen, desto größer das Gefährdungspotential.
- Änderungsfrequenz:
  Mit der Zahl der Konfigurationsänderungen steigt auch die Wahrscheinlichkeit von Administrations- und Konzeptionsfehlern.

Allgemein lässt sich sagen: Bei Netzübergängen mit hohem Schutzbedarf wird man häufiger eine Revision durchführen als bei Netzübergängen, die einen niedrigen Schutzbedarf haben.

Komponenten

Dieses Kernmodul 4 (s. Abb. 3) beinhaltet alle denkbaren Komponenten eines Netzübergangs, die für eine mehrstufige Architektur notwendig und sinnvoll sind. Dazu gehören prinzipiell: Paketfilter und Application-Level-Gateways (ALG). Speziell werden die Produkte GeNUGate und CheckPoint betrachtet.

3.3 Grundlegende Schritte und Rollen der IT-Revision

Voraussetzung für die Durchführung einer erfolgreichen Revision ist ein strukturiertes Vorgehen. Die dazu notwendigen Ablaufschritte und die Organisation des Revisionsprozesses werden in den folgenden Abschnitten detailliert erörtert. Hier wird zunächst eine Übersicht geboten, welche Aspekte bei einer Revision zu beachten sind.

Initiierung

Zu Beginn einer Revision stehen die Initiierung der Prüfung und die damit verbundenen Abläufe. Auslöser einer IT-Revision kann ein Ereignis sein, etwa ein sicherheitsrelevanter Vorfall, z. B. Unregelmäßigkeiten im internen Netz oder auch konkrete Ereignisse wie beispielsweise ein Virenbefall. Andere IT-Revisionen werden regelmäßig initiiert, etwa weil Sicherheitsvorgaben für kritische IT-Objekte eine zyklische Prüfung erfordern.

Identifizierung des IT-Revisionsobjekts, Beauftragung und Vorbereitung

Ist die Revisionsanforderung gestellt, so gilt es, das Revisionsobjekt zu identifizieren und die Prüfungsinhalte und den Prüfrahmen (Beteiligte, Zeitablauf, Termine) in einem vorläufigen Prüfplan festzulegen. Dazu gehört auch eine Festlegung der Revisionsziele, also des Prüfmaßes.

Steht der vorläufige Prüfrahmen fest, kann eine Beauftragung der Revision an einen externen oder internen Revisor erfolgen. Dieser muss den vorläufigen Revisionsplan ggf. konkretisieren und modifizieren. Der überarbeitete Revisionsplan wird zum Abschluss der Vorbereitungsphase verabschiedet und bildet die Grundlage sowohl für die folgende Prüfung als auch für die Bewertung der aufgefundenen Mängel.

Durchführung und Abschluss

Im Rahmen der Prüfungsphase wird der Revisionsplan umgesetzt. Dabei wird der Ist-Zustand der vorher festgelegten Objekte gegen den Soll-Zustand (Revisionsziele) geprüft, die Ergebnisse werden protokolliert und Abweichungen von den Revisionszielen vermerkt. Als Prüfobjekte können Betriebsprozesse, Dokumente, Konfigurationen, Architekturen und technische Komponenten dienen. Ggf. muss der vorher festgelegte Revisionsplan in dieser Phase noch angepasst werden, wenn beispielsweise im Verlaufe der Prüfung neue Prüfaspekte evident werden.

Die Revision schließt mit einem Bericht ab, in dem Mängel aufgezeigt und bewertet werden. Innerhalb des Berichtes sollten Hinweise zur Behebung der entdeckten Schwachstellen nicht fehlen. Auch sollte den für die entdeckten Diskrepanzen Verantwortlichen die Gelegenheit gegeben werden, innerhalb des Prüfungsberichtes Stellung zu beziehen. Werden jedoch im Verlaufe der Revision erhebliche Mängel festgestellt, so müssen diese so schnell wie möglich abgestellt werden.

Die hier skizzierte Vorgehensweise wird im folgenden Abschnitt detailliert als Prozess dargestellt. In diesem Prozess werden die relevanten Rollen und ihre wesentlichen Aufgaben innerhalb der IT-Revision wie folgt verwendet:

- Oberste Organisationsleitung (Geschäftsführung oder Dienststellenleiter):
  - Gesamtverantwortung für die Revision.
- Interne Revision[12]:
  - Veranlassung und Begleitung der Revision,
  - Erstellung des vorläufigen Prüfplanes.
- Objektverantwortlicher (Objekt Owner): Verantwortlicher eines Systems oder Verbundes.
  - Gesamtaufsicht über das System,
  - Initiierung der Revision,
  - Beauftragung des Revisors,
  - Abnahme der Prüf- und Zeitpläne.
- Objekt Administrator: zuständig für Administration und Wartung der Systeme
  - Verantwortung für die Umsetzung der Anforderungen,
  - Hilfestellung bei der Analyse des Objektes und seines Schutzbedarfes,
  - Begleitung bei der Erstellung der Zeitpläne.

---

[12] Die interne Revision ist eine direkt der obersten Unternehmens- oder Behördenleitung unterstellte unabhängig handelnde Stelle für organisatorisch interne Beratungen und Prüfungen.

- Beauftragter Revisor:
  - Erstellung des endgültigen Prüfplanes,
  - Durchführung der Revision,
  - Bewertung der Ergebnisse,
  - Erstellung der Revisionsdokumentation,
  - Präsentation der Ergebnisse.

3.4 Detaillierter IT-Revisionsprozess

Im Folgenden wird der Revisionsprozess erläutert, beginnend bei der Initiierung und endend bei der Ablage der erzielten Ergebnisse sowie der ggf. durchgeführten Realisierung empfohlener Maßnahmen. Dabei werden sowohl die einzelnen Prozessschritte als auch die dabei entstehenden oder verarbeiteten Informationen aufgezeigt und beschrieben.

Jeder Prozessschritt wird einzeln beschrieben. Neben der Beschreibung des Prozessschrittes wird der notwendige Input sowie der Output als Resultat erläutert. Die handelnden Personen bzw. Rollen werden ebenfalls genannt.

Neben den einzelnen Prozessschritten gibt es zusätzlich eine kurze und einführende Gesamtbeschreibung der Prozesse an sich. Dazu wird auch der Initiator für jeden Prozess beschrieben sowie das Ziel des Prozesses verdeutlicht und die verantwortlichen Personen bzw. Rollen werden genannt.

Teilprozesse werden wiederum in einzelne Prozesse unterteilt und gesondert in ihren Einzelprozessen beschrieben.

3.4.1 Revisionsprozess

Der Revisionsprozess beschreibt den gesamten Ablauf einer Revision (s. Abb. 9), beginnend mit der Initiierung und endend mit der Ablage der erzielten Ergebnisse sowie einer Bearbeitung der dokumentierten Empfehlungen. Eine Revision kann entweder durch ein Ereignis ausgelöst werden, nach dem eine Revision des Netzübergangs erforderlich erscheint, oder aber durch Anforderungen, basierend auf den Vorgaben einer Sicherheitsleitlinie. Ziel der Revision ist die Überprüfung, ob der Netzübergang gemäß den Vorgaben betrieben wird und die Funktionalität gemäß den Anforderungen gegeben ist. Verantwortlich für den gesamten Revisionsprozess ist die oberste Führung der Organisation (Geschäftsleitung, Dienststellenleiter).

Im Folgenden werden die Teilschritte des Revisionsprozesses beschrieben. Teilprozesse werden wiederum in einzelne Prozesse unterteilt und gesondert erläutert.

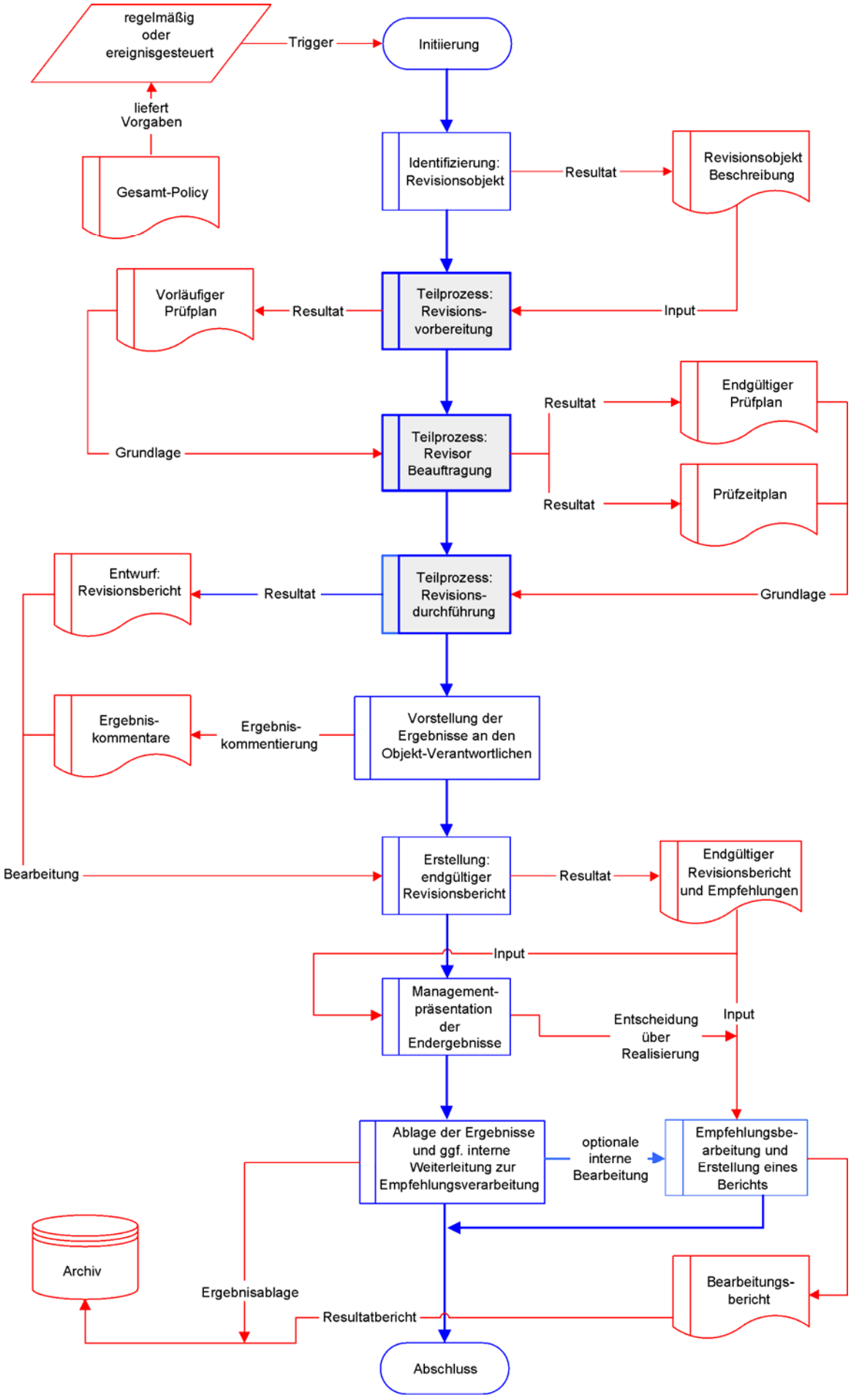

regelmäßig oder ereignisgesteuert
Trigger
Initiierung
liefert Vorgaben
Gesamt-Policy
Identifizierung: Revisionsobjekt
Resultat
Revisionsobjekt Beschreibung
Vorläufiger Prüfplan
Resultat
Teilprozess: Revisions-vorbereitung
Input
Resultat
Endgültiger Prüfplan
Grundlage
Teilprozess: Revisor Beauftragung
Resultat
Prüfzeitplan
Entwurf: Revisionsbericht
Resultat
Teilprozess: Revisions-durchführung
Grundlage
Ergebnis-kommentare
Ergebnis-kommentierung
Vorstellung der Ergebnisse an den Objekt-Verantwortlichen
Bearbeitung
Erstellung: endgültiger Revisionsbericht
Resultat
Endgültiger Revisionsbericht und Empfehlungen
Input
Management-präsentation der Endergebnisse
Entscheidung über Realisierung
Input
Ablage der Ergebnisse und ggf. interne Weiterleitung zur Empfehlungsverarbeitung
optionale interne Bearbeitung
Empfehlungsbe-arbeitung und Erstellung eines Berichts
Archiv
Ergebnisablage
Bearbeitungs-bericht
Resultatbericht
Abschluss

Abbildung 9: *Grafische Übersicht über den Revisionsprozess. Er besteht aus mehreren Einzelprozessen sowie Gruppen von Einzelprozessen, den so genannten Teilprozessen. Diese Teilprozesse werden später noch einmal in gesonderten Grafiken in ihre Einzelprozesse zerlegt und dargestellt.*

Die Teilschritte des Revisionsprozesses lassen sich wie folgt beschreiben:

Initiierung:

Beschreibung: Die Initiierung ist der Beginn der Revision eines Netzübergangs. Der Anlass dafür kann einer der folgenden Aspekte sein:

- Ein Ereignis: Ein nichtalltägliches Ereignis wird registriert, das darauf schließen lässt, dass der Netzübergang nicht vollständig den dokumentierten Anforderungen genügt oder aber außerhalb etablierter Schemata liegt und somit als Sicherheitsrisiko eingestuft wird.
- Ein Plan: Die maßgebliche Sicherheitsleitlinie sieht regelmäßige Revisionen des Netzübergangs vor.
- Eine Modifikation des Netzübergangs: Der bestehende Netzübergang wurde technologisch (Hardware, Software, Architektur) verändert (verkleinert, vergrößert).

Die interne Revision sowie die beteiligten Administratoren entscheiden über die Durchführung der Revision.

Input: Informationen oder Kriterien, die eine Revision rechtfertigen oder notwendig erscheinen lassen. Dazu gehören Informationen über ein konkretes, registriertes Ereignis oder aber Anforderungen, die auf einer Sicherheitsleitlinie basieren und eine Revision fordern.

Output: Resultat dieser Initiierung ist zunächst die Entscheidung, eine Revision durchzuführen, und als Folge dessen die Anweisung zur Durchführung.

Handelnde:
- Administratoren des Netzübergangs
- Interne Revision

Identifizierung Revisionsobjekt:

Beschreibung: Basierend auf der Art des Anlasses wird das Revisionsobjekt festgelegt. Dies kann eine einzelne Hardware-Komponente, eine Software-Komponente, ein Betriebsprozess, Teile der Dokumentation oder aber der gesamte Netzübergang mit allen dazugehörenden Komponenten, der zugrunde liegenden Architektur (Struktur), Betriebsprozessen und Dokumenten sein.

Input: Die Art des Anlasses liefert wesentliche Informationen, um das Revisionsobjekt festzulegen.

Output: Das Revisionsobjekt wird festgelegt und eine Beschreibung erstellt.

Handelnde:
- Administratoren des Netzübergangs
- Interne Revision

Teilprozess Revisionsvorbereitung:

Beschreibung: In der Revisionsvorbereitung wird das Revisionsobjekt detailliert analysiert und ein vorläufiger Prüfplan festgelegt. Dies ist ein eigenständiger Prozess, der im Abschnitt 3.4.1.1 näher erläutert wird.

Input: Das gewählte Revisionsobjekt sowie dessen Beschreibung bilden den notwendigen Input.

Output: Das Resultat dieses Teilprozesses ist der vorläufige Prüfplan.

Handelnde:
- Objektverantwortliche

Teilprozess Revisor Beauftragung:

Beschreibung: Auf der Grundlage des vorläufigen Prüfplanes wird ein Revisor bestimmt, der optimal die gestellte Aufgabe erfüllen kann.

Der ausgewählte Revisor entwickelt dann auf der Grundlage des vorläufigen Prüfplanes einen endgültigen Prüfplan sowie einen Zeitplan für die Revision.

Detailliert wird dieser Teilprozess im Abschnitt 3.4.1.2 beschrieben.

Input: Der vorläufige Prüfplan ist der wesentliche Bestandteil der Beauftragung.

Output: Das Resultat des Prozesses ist der Abschluss aller Vorarbeiten zur Revision. Dazu gehören im Einzelnen:

- Revisor ist ausgewählt und beauftragt,
- abgestimmter Prüfplan und
- abgestimmter Zeitplan für die Revision liegen vor.

Handelnde:
- Objektverantwortliche

Teilprozess Revisionsdurchführung:

Beschreibung: Die Revisionsdurchführung besteht zum einen aus der Ausführung des festgelegten und abgenommenen Prüfplanes und zum anderen aus der ausführlichen Dokumentation der erzielten Ergebnisse.

Der Teilprozess Revisionsdurchführung wird detailliert im Abschnitt 3.4.1.3 beschrieben.

Input: Der endgültige Prüfplan und der verabschiedete Zeitplan bilden die Grundlage dieses Teilprozesses.

Output: Der vorläufige Ergebnisbericht ist das Resultat dieses Teilprozesses.

Handelnde:
- Beauftragter Revisor

Vorstellung der Ergebnisse an den Objektverantwortlichen:

Beschreibung: Die erzielten Ergebnisse werden auf der Basis des vorläufigen Ergebnisberichts dem Objektverantwortlichen vorgestellt.

Dieser hat dann die Möglichkeit, die vorläufigen Ergebnisse zu kommentieren und zu bewerten.

Zur Erstellung des Ergebnisberichts kann die Dokumentationsvorlage im Anhang genutzt werden.

Input: Die vorläufigen Ergebnisse bilden die Grundlage dieses Schrittes.

Output: Die Bewertungen und die Kommentare des Objektverantwortlichen.

Handelnde:
- Revisor
- Objektverantwortlicher (Objekt Owner)
- Objekt Administratoren

Erstellung endgültiger Revisionsbericht:

Beschreibung: Auf der Grundlage des vorläufigen Ergebnisberichts sowie der abgegebenen Kommentare und Bewertungen des Objektverantwortlichen erstellt der Revisor den endgültigen Revisionsbericht.

Der Bericht enthält neben den dokumentierten Ergebnissen auch Empfehlungen zur Behebung aufgedeckter Schwachstellen.

Input: Der vorläufige Ergebnisbericht sowie die abgegebenen Bewertungen und Kommentare des Verantwortlichen für das Revisionsobjekt.

Output: Endgültiger Revisionsbericht.

Handelnde: Revisor

Managementpräsentation der Endergebnisse:

Beschreibung: Die erzielten Ergebnisse werden einem festzulegenden Führungskreis vorgestellt.

Input: Endgültiger Revisionsbericht.

Output: Das Resultat der Präsentation ist die Entscheidung, ob und in welchem Rahmen und Umfang die abgegebenen Empfehlungen zu realisieren sind.

Handelnde:

- Revisor
- Oberste Führung der Organisation (Geschäftsleitung, Dienststellenleiter)

Ablage der Ergebnisse und ggf. interne Weiterleitung zur Empfehlungsverarbeitung:

Beschreibung: Das erzielte Ergebnis wird archiviert. Ggf. werden die beschlossenen Maßnahmen zur Realisierung weitergeleitet.

Input: Endgültiger Revisionsbericht.

Output: Resultat ist die Archivierung des Revisionsberichtes.

Handelnde: Objektverantwortlicher

Optional: Empfehlungsverarbeitung und Erstellung eines Berichts:

Beschreibung: Die abgegebenen Empfehlungen werden im gewünschten Maß realisiert. Über die dabei erzielten Resultate wird ein Bericht verfasst, der ebenfalls – zusammen mit dem Revisionsbericht – archiviert wird.

Input: Die abgegebenen Empfehlungen des Revisionsberichts.

Output: Der Bericht über die Realisierung der empfohlenen und beschlossenen Maßnahmen.

Handelnde: Objekt Administratoren

Abschluss:

Beschreibung:	Der Revisionsprozess ist beendet: Das Revisionsobjekt wurde gemäß den Vorgaben einer Revision unterzogen. Die Resultate wurden dokumentiert und den verantwortlichen Personen vorgestellt. Empfehlungen wurden ggf. zur Umsetzung freigegeben und realisiert. Die vollständige Dokumentation der durchgeführten Revision wird archiviert.
Input:	Information über den Abschluss der Revision sowie Ablage der Ergebnisse und ggf. Realisierung der Maßnahmen.
Output:	-
Handelnde:	• Oberste Führung der Organisation (Geschäftsleitung, Dienststellenleiter) • Interne Revision

3.4.1.1 Teilprozess: Revisionsvorbereitung

Die Revisionsvorbereitung (s. Abb. 10) dient dazu, das Revisionsobjekt im Detail zu analysieren und einen vorläufigen Prüfplan zu erstellen, der im weiteren Verlauf der Revision verfeinert und konkretisiert wird. Verantwortlich für diesen Prozess ist der Objektverantwortliche.

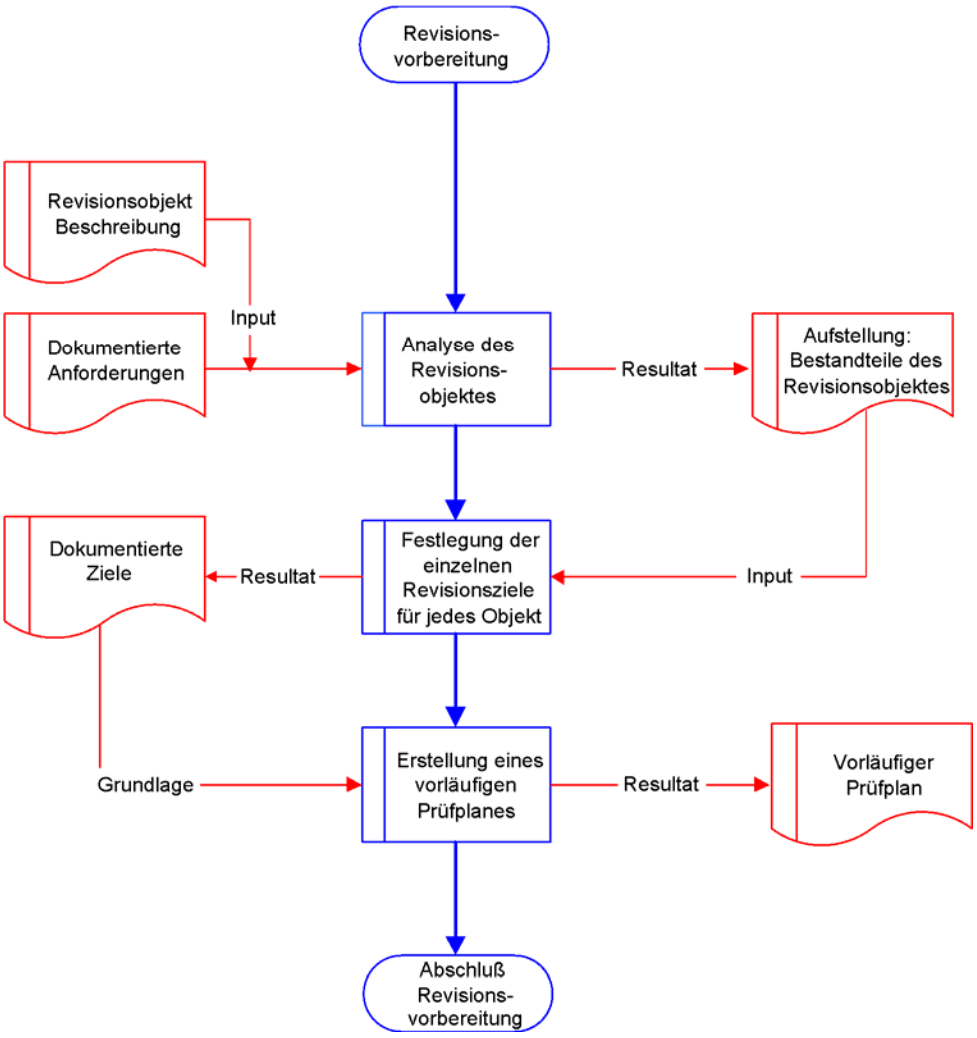


Abbildung 10: *Teilprozess: Revisionsvorbereitung*

Der in Abbildung 10 dargestellte Teilprozess „Revisionsvorbereitung“ gliedert sich wie folgt:

Analyse des Revisionsobjektes:

Beschreibung: Die Analyse des Revisionsobjektes wird auf der Grundlage des maßgeblichen Schutzbedarfs durchgeführt. Das Resultat der Analyse ist eine detaillierte Aufstellung aller zu prüfenden Bestandteile des Revisionsobjektes.

Input:
- Beschreibung des Revisionsobjektes
- Schutzbedarfsfeststellung für das Revisionsobjekt

Output: Die Analyse liefert eine genaue Beschreibung aller zu untersuchenden Bestandteile des Revisionsobjektes.

Handelnde:
- Objekt Administrator
- Objektverantwortlicher

Festlegung der einzelnen Revisionsziele für jedes Objekt:

Beschreibung: Die Festlegung der Ziele bedeutet, dass hier der Soll-Zustand für jeden Bestandteil des Revisionsobjektes festgelegt wird. Diese Festlegung stellt im weiteren Verlauf die Grundlage der Revision dar.

Input: Die genaue Beschreibung aller Bestandteile des Revisionsobjektes.

Output: Die genaue Dokumentation der konkreten Revisionsziele (der Soll-Zustand aller Bestandteile).

Handelnde:
- Objektverantwortlicher
- Objekt Administrator

Erstellung eines vorläufigen Prüfplanes:

Beschreibung: Der dokumentierte Sollzustand dient als Grundlage, um einen ersten, vorläufigen Prüfplan zu erstellen. Dieser wird später, wenn ein Revisor ausgewählt ist, verfeinert und konkretisiert.

Der vorläufige Prüfplan kann auf der Grundlage der im Anhang dargestellten Checklisten erstellt bzw. zusammengestellt werden.

Input: Dokumentation des Soll-Zustandes.

Output: Vorläufiger Prüfplan.

Handelnde: Interne Revision

3.4.1.2 Teilprozess: Revisor Beauftragung

Auf der Grundlage des vorläufigen Prüfplanes wird ein Revisor beauftragt. Dieser konkretisiert und verfeinert dann den Prüfplan und stimmt ihn mit dem Objektverantwortlichen ab (s. Abb. 11).

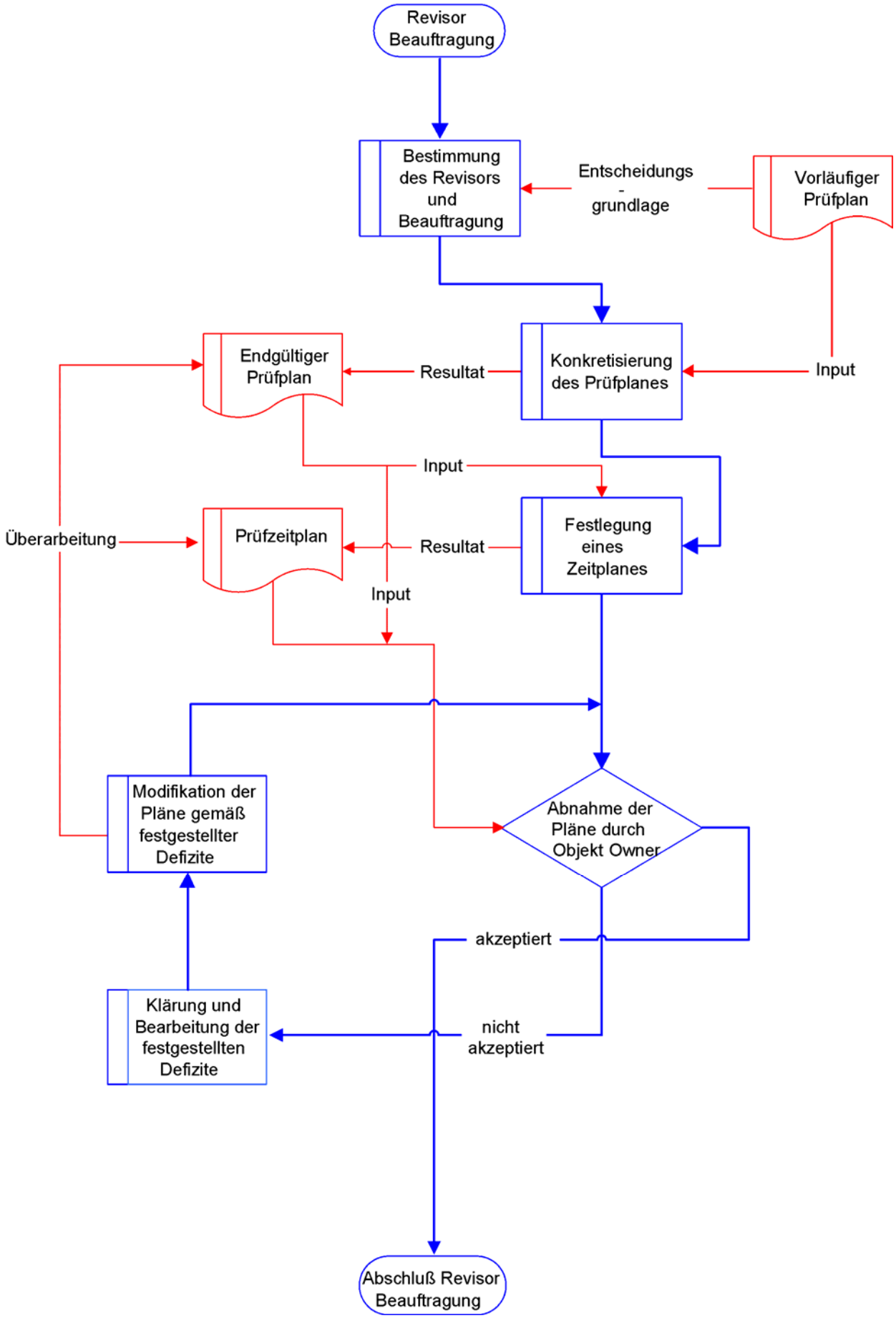


Abbildung 11: *Teilprozess: Revisor Beauftragung*

Der in Abbildung 11 dargestellte Teilprozess „Revisor Beauftragung“ besteht aus den folgenden Ablaufschritten:

Bestimmung des Revisors:

Beschreibung: Auf der Basis des vorläufigen Prüfplans wird ein Revisor ausgewählt. Auf diese Weise wird sichergestellt, dass der Revisor die geforderten Fähigkeiten bereitstellen kann.

Die Beauftragung zur Durchführung der Revision kann an einen internen oder an einen externen Revisor erfolgen. Für den letzteren Fall wäre eine Ausschreibung, Auswertung und Beauftragung – inklusive vertraglicher Verhandlungen und eines verbindlichen Abkommens notwendig. Dieser Prozess wird in diesem Leitfaden nicht näher konkretisiert.

Input: Vorläufiger Prüfplan.

Output: Das Resultat ist die Beauftragung eines internen oder externen Revisors.

Handelnde: Objektverantwortlicher

Konkretisierung des Prüfplanes:

Beschreibung: Der beauftragte Revisor entwickelt auf der Basis des vorläufigen Planes den endgültigen Prüfplan.

Input: Der vorläufige Prüfplan bildet die Grundlage zur Konkretisierung des Prüfplanes.

Output: Vorschlag für den endgültigen Prüfplan.

Handelnde: Beauftragter Revisor

Festlegung eines Zeitplanes:

Beschreibung: Auf der Grundlage des Vorschlags zum endgültigen Prüfplan entwickelt der Revisor einen Zeitplan zur Durchführung der Revision in allen Einzelheiten.

Die Festlegung des Zeitplanes und damit des gesamten Durchführungsrahmens der Revision kann mit Hilfe der Formblätter dokumentiert werden.

Input: Der Vorschlag zum endgültigen Prüfplan bildet die Grundlage des Zeitplanes.

Output: Vorschlag zur zeitlichen Durchführung der Revision.

Handelnde:

- Beauftragter Revisor
- Objekt Administrator

Entscheidung: Abnahme der Prüfpläne durch den Objektverantwortlichen:

Beschreibung: Die durch den Revisor entwickelten Pläne müssen durch den Objektverantwortlichen abgenommen werden. Möglichkeiten zur Entscheidung sind:

Akzeptiert: Die Beauftragung ist abgeschlossen und die Pläne abgenommen.

Nicht akzeptiert: Die nicht akzeptablen Aspekte werden dokumentiert und an den Revisor zur Bearbeitung zurückgegeben.

Input: Vorschlag zum endgültigen Prüfplan und Zeitplan.

Output: Entweder eine dokumentierte Abnahme der vorgeschlagenen Prüf- und Zeitpläne oder dokumentierte Änderungsvorschläge.

Handelnde: Objektverantwortlicher

Klärung und Bearbeitung der festgestellten Defizite:

Beschreibung: Der Objektverantwortliche gibt die nicht akzeptierten Aspekte an den Revisor weiter, damit dieser seine Pläne entsprechend modifizieren kann.

Input: Begründung für die Ablehnung der Pläne in Teilen oder auch vollständig.

Output: Änderungsvorschläge für die einzelnen Pläne.

Handelnde:
- Objektverantwortlicher
- Beauftragter Revisor

Modifikation der Pläne gemäß festgestellter Defizite:

Beschreibung: Die festgestellten Defizite werden durch den Revisor bearbeitet und in den Plänen entsprechend berücksichtigt.

Die modifizierten Pläne werden dem Objektverantwortlichen im Anschluss erneut zur Abnahme vorgelegt.

Input: Änderungsvorschläge für die einzelnen Pläne.

Output: Modifizierte Prüf- und Zeitpläne.

Handelnde: Beauftragter Revisor

3.4.1.3 Teilprozess: Revisionsdurchführung

Die Revisionsdurchführung startet mit der Abarbeitung des festgelegten und verabschiedeten Prüfplans auf der Grundlage des verabschiedeten Zeitplans. Parallel zur Abarbeitung der einzelnen Prüfungen werden die Resultate protokolliert. Ergänzend gibt es die Möglichkeit, falls während der Revision weitere relevante Prüfobjekte identifiziert werden, diese – nach Absprache – in den Prüfplan mit aufzunehmen und entsprechend zu prüfen. Verantwortlich für die Durchführung der Revision ist der beauftragte Revisor.

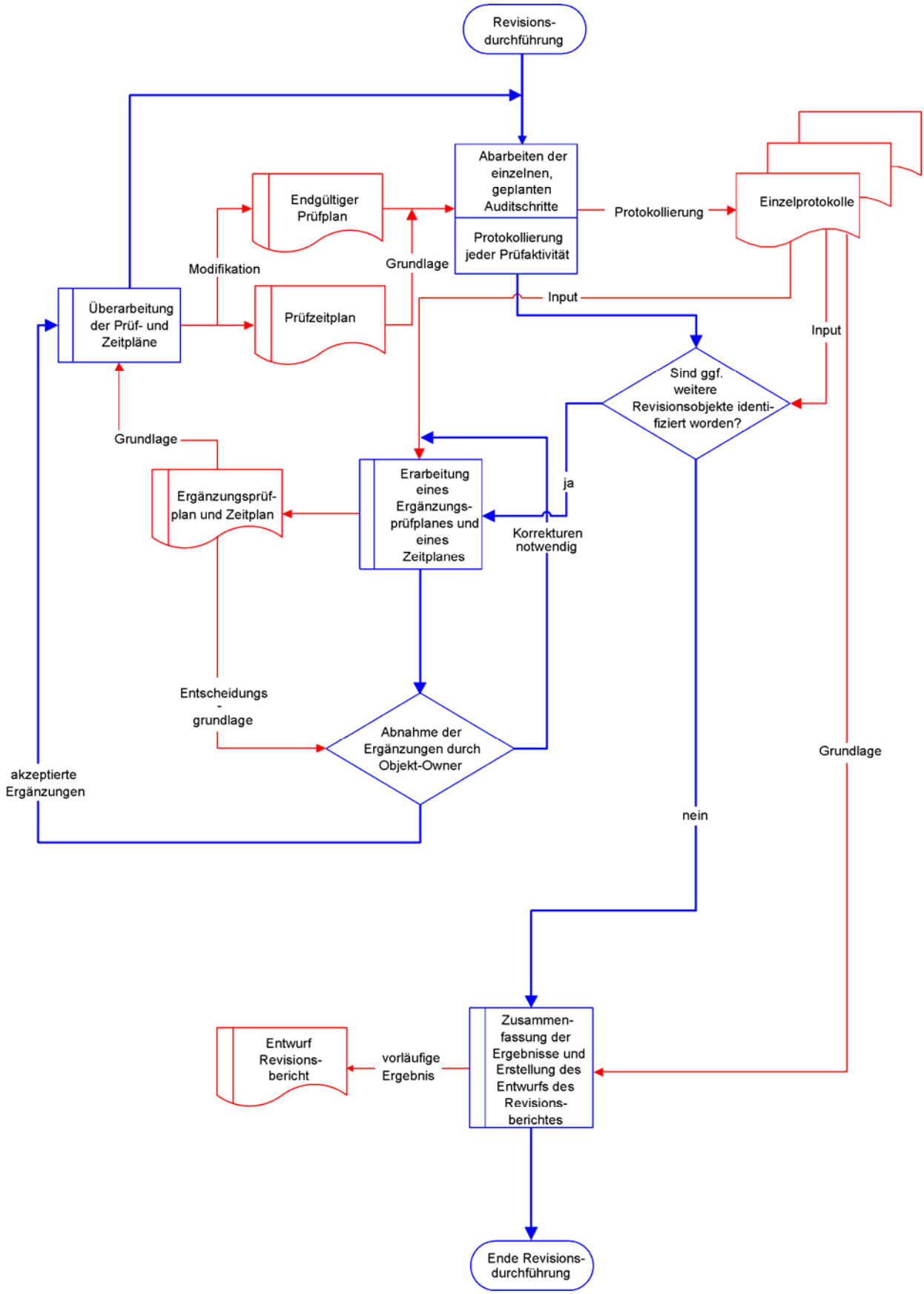


Abbildung 12: *Teilprozess: Revisionsdurchführung*

Folgende Teilschritte in Abbildung 12 bilden den Ablauf des Teilprozesses „Revisionsdurchführung“:

Abarbeiten der einzelnen geplanten Revisionsschritte:

Beschreibung: Der Revisor prüft die festgelegten einzelnen Aspekte des Prüfplanes gemäß dem vorgegebenen Zeitplan.

Input: Grundlage der Prüfungen sind die verabschiedeten Prüfpläne sowie der festgelegte Zeitplan.

Output: Prüfungsresultate

Handelnde: Beauftragter Revisor

Protokollierung jeder Aktivität:

Beschreibung: Jedes Resultat wird einzeln protokolliert und dient als Grundlage der späteren Dokumentation der Revision.

Input: Einzeln erzielte Ergebnisse.

Output: Protokolle der einzelnen Prüfungen.

Handelnde: Beauftragter Revisor

Entscheidung: Sind ggf. weitere Revisionsobjekte identifiziert worden?

Beschreibung: Während der Revision ergeben sich möglicherweise Prüfaspekte oder Objekte, die zum früheren Zeitpunkt der Verabschiedung des Prüfplanes nicht bekannt waren oder auch übersehen worden sind.

An dieser Stelle gibt es die Möglichkeit, den Revisionsplan zu ergänzen, damit die entdeckten zusätzlichen Objekte bei der Revision berücksichtigt werden können.

Die Entscheidung bietet zwei Möglichkeiten:

Keine weiteren Prüfobjekte identifiziert: Die Prüfung ist abgeschlossen.

Weitere Prüfobjekte wurden identifiziert: Ein Ergänzungsprüfplan ist zu erstellen.

Eine weitere Möglichkeit ist denkbar: Es wurden weitere Objekte identifiziert, aber eine Prüfung als nicht notwendig erachtet. In diesem Fall ist die Entscheidung zu dokumentieren und wie im Fall „keine weiteren Prüfobjekte identifiziert“ fortzufahren.

Input: Erstellte Einzelprotokolle sowie Informationen des beauftragten Revisors.

Output: Entscheidung sowie deren Dokumentation.

Handelnde:

- Objektverantwortlicher
- Beauftragter Revisor

Erarbeitung eines Ergänzungsprüfplanes und eines Zeitplanes:

Beschreibung: Es wurden während der Revision weitere relevante Revisionsobjekte identifiziert und entschieden, diese einer Prüfung zu unterziehen. Dazu ist ein ergänzender Prüfplan bzw. eine Ergänzung für den abgearbeiteten Prüfplan zu erstellen.

Input: Erzielte Einzelprotokolle sowie die Entscheidung zur erweiterten Prüfung.

Output: Ergänzungsvorschläge zum Prüfplan und zum Zeitplan.

Handelnde: Beauftragter Revisor

Entscheidung: Abnahme und Ergänzung durch den Objektverantwortlichen:

Beschreibung: Die vorgeschlagenen Ergänzungen müssen von dem Objektverantwortlichen akzeptiert und abgenommen werden.

Ergänzungspläne akzeptieren: Der Prüfplan sowie der Zeitplan werden entsprechend den akzeptierten Ergänzungen erweitert und zur ergänzenden Revision freigegeben.

Ergänzungspläne nicht akzeptieren: Korrekturen der Ergänzungen werden erarbeitet, um erneut eine Entscheidung über die Abnahme herbeizuführen.

Input: Ergänzungsvorschläge zu den Prüf- und Zeitplänen.

Output: Ggf. Korrekturvorschläge zu den Ergänzungen oder die Abnahme.

Handelnde: Objektverantwortlicher

Überarbeitung der Prüf- und Zeitpläne:

Beschreibung: Die Prüf- und Zeitpläne werden entsprechend den akzeptierten Ergänzungen erweitert, um als Grundlage für die erweiterte Prüfung zu dienen.

Input: Abgenommene Erweiterungen.

Output: Überarbeitete Prüf- und Zeitpläne.

Handelnde: Beauftragter Revisor

Zusammenfassung der Ergebnisse und Erstellung eines Entwurfs des Revisionsberichts:

Beschreibung: Die einzelnen Protokolle aus den ausgeführten Prüfungen werden zu einem vorläufigen Ergebnisbericht zusammengefasst. Dieser Bericht enthält auch ggf. konkrete Empfehlungen zur Beseitigung von Schwachstellen bzw. zur Verbesserung identifizierter Mängel.

Input: Einzelprotokolle der Prüfungen.

Output: Vollständiger und vorläufiger Ergebnisbericht.

Handelnde: Beauftragter Revisor

3.5 Zusammenfassung

In diesem Kapitel wurden unterschiedliche Methoden der IT-Revision vorgestellt (Compliance Audit und Substantive Audit) und gegen den bekannten Penetrationstest abgegrenzt. Die vorgestellten Methoden können im Teil II „Revisionshilfsmittel“ an geeigneter Stelle verwendet werden.

Es wurde ein modulares Prüfkonzept vorgestellt und seine Kernmodule wurden näher erläutert. Die Checklisten des vorgestellten Prüfbaumes finden sich ebenfalls im Teil II.

Der wesentliche Teil dieses Kapitels beschreibt die Abläufe und Rollen einer IT-Revision in Form von Prozessdiagrammen. Diese Abläufe werden durch die Hilfsmittel des Teils II an den geeigneten Stellen unterstützt.

Anhang

Anlage 1 Ergänzende Verzeichnisse

Anlage 1.1 Abkürzungsverzeichnis

AAA	**A**uthentication, **A**uthorization, **A**ccounting (z. B. Directory, RADIUS, TACACS, tokenbasierende Authentisierungssysteme, Accounting-Daten)
ACK	Acknowledge
AktG	Aktiengesetz
ALG	Application-Level-Gateways
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BEW	Beweissicherung
BSI	Bundesamt für Sicherheit in der Informationstechnik
CEO	Chief Executive Officer
CFO	Chief Financial Officer
Corba	Common Object Request Broker Architecture
DFK	Datenflusskontrolle
DMZ	Demilitarisierte Zone
DNS	Domain Name Service
DV	Datenverarbeitung
EDI	Electronic Data Interchange
EG	Europäische Gemeinschaft
E-Mail	Electronic Mail
FTP	File Transfer Protocol
GoB	Grundsätze ordnungsgemäßer Buchführung
GoBS	Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme
GoDV	Grundsätze für eine ordnungsmäßige Datenverarbeitung
GSHB	Grundschutzhandbuch
HA	High Availability
HGB	Handelsgesetzbuch
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol

IDA	Identifikation und Authentisierung
IIOP	Internet Inter Object Request Broker Protokoll
IP	Internet Protocol
IPv6	Internet Protocol Version 6
IT	Informationstechnik
KBSt	Koordinierungs- und Beratungsstelle der Bundesregierung
KEY	Schlüsselmanagement
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KRY	Kryptographische Übertragungssicherung
KWG	Kreditwesengesetz
LAN	Local Area Network
LDSG	Landesdatenschutzgesetz
MDStV	Staatsvertrag für Mediendienste
NIS	Network Information System
OSPF	Open Shortest Path First
PC	Personal Computer
PersVG	Personalvertretungsgesetz
POP3	Post Office Protocol 3
RAS	Remote Access Service
RPC	Remote Procedure Call
SEC	Securities and Exchange Commission
setuid	set user id
SGB	Sozialgesetzbuch
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOA	Sarbanes-Oxley Act
SRVwV	Allgemeine Verwaltungsvorschrift über das Rechnungswesen in der Sozialversicherung
SVRV	Sozialversicherungs-Rechnungsverordnung
SYN	Synchronize
SYSLOG	System logging
TCP	Transmission Control Protocol
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TDSV	Telekommunikations-Datenschutzverordnung
TELNET	Terminal Network
TKG	Telekommunikationsgesetz

TKÜV	Telekommunikationsüberwachungsverordnung
UDP	User Datagram Protocol
UNIX	Uniplexed Information and Computing System
VPN	Virtuelles Privates Netz
VSA	VS-Anweisung - Allgemeine Verwaltungsvorschrift zum materiellen und organisatorischen Schutz von Verschlusssachen

Anlage 1.2 Glossar

Application-Level Gateway (ALG) Die Funktionen eines Sicherheitsgateways auf Anwendungsebene werden von den so genannten Application-Level Gateways (ALG) übernommen. Implizit nehmen ALGs auch Funktionen auf den Schichten 2 bis 3 des TCP/IP-Referenzmodells wahr. ALGs, auch Sicherheits-Proxies genannt, unterbrechen den direkten Datenstrom zwischen Quelle und Ziel. Bei einer Kommunikationsbeziehung zwischen Client und Server über einen Proxy hinweg nimmt der Proxy die Anfragen des Clients entgegen und leitet sie an den Server weiter. Bei einem Verbindungsaufbau in umgekehrter Richtung, also vom Server zum Client, verfährt der Proxy analog. Sämtliche Kommunikationsbeziehungen zwischen den beiden Rechnern verlaufen in diesem Fall also mittelbar über den Proxy. Diese Kommunikationsform ermöglicht es einem Proxy beispielsweise, die übertragenen Daten inhaltlich zu kontrollieren oder bestimmte Protokollbefehle zu filtern.

Demilitarisierte Zone (DMZ) Eine DMZ ist ein Zwischennetz, das an Netzübergängen gebildet wird, aber weder zu dem einen noch zu dem anderen Netz gehört. Sie stellt ein eigenes Netz dar, das nicht so stark gesichert ist wie das eigentlich zu schützende Netz. DMZ werden bei einfachen Sicherheitsgateways üblicherweise an einer dritten Schnittstelle des Paketfilters erzeugt. Besteht das Sicherheitsgateway aus Paketfilter – Application-Level-Gateway – Paketfilter, dient in der Regel eine weitere Schnittstelle des Application-Level-Gateways (ALG) als DMZ-Schnittstelle. Verfügen Paketfilter oder ALG über mehr als drei Schnittstellen, können weitere DMZ gebildet werden.

Dienst Unter dem Begriff „Dienst“ wird eine Anwendung verstanden, die in der Regel auf höherwertigen Protokollen (TCP, UDP) basiert. Einfache Dienste verwenden dabei in der Regel genau ein Anwendungsprotokoll (z. B. HTTP, POP3, SMTP). Komplexere Applikationen (z. B. Reuters, Bloomberg, Xetra) können mehrere Anwendungsprotokolle/Dienste verwenden.

Interne Revision Die interne Revision ist eine direkt der obersten Unternehmens- oder Behördenleitung unterstellte unabhängig handelnde Stelle für organisatorisch interne Beratungen und Prüfungen.

Proxy Ein Proxy ist eine Art Stellvertreter in Netzen. Er nimmt Daten von einer Seite an und leitet sie an eine andere Stelle im Netz weiter. Mittels eines Proxys lassen sich Datenströme filtern und gezielt weiterleiten.

Prüfbericht Der Prüfbericht dokumentiert das gesamte Vorgehen zur Durchführung einer Revision. Im Teil II ist dazu ein Dokumentationsrahmen angefügt.

Prüfmodul Ein „Modul“ bezeichnet eine sinnvolle und in sich vollständige Prüfeinheit einer Revision.
In diesem Leitfaden werden vier Kernmodule unterschieden:
- Betriebsprozesse,
- Dokumentation,
- Szenarien und
- Komponenten.

Teile dieser Kernmodule sind in weitere sinnvolle Einzelmodule aufgespalten, sodass eine Revision einerseits alle vier Kernmodule enthalten sollte, um vollständig zu sein, andererseits aber untergeordnete Module ausgewählt werden können, um speziellen Typen und Topologien gerecht zu werden.

Prüfplan Der Prüfplan dokumentiert alle zu prüfenden Kriterien. Als Grundlage für einen konkreten Prüfplan können die Checklisten aus dem Teil II verwendet werden.

Restrisiko Risiko, das grundsätzlich bleibt, auch wenn Maßnahmen zum Schutz des IT-Einsatzes ergriffen worden sind.

Revisionsobjekt Der Begriff „Revisionsobjekt“ bezeichnet abstrakt den Revisionsgegenstand sowie alle dazugehörigen und untergeordneten Teilaspekte.

Router Verbindet unterschiedliche – räumlich getrennte – Netzwerke. Entweder über ISDN-Verbindungen oder öffentlich zugängliche Netzwerke (Internet).

Schutzbedarf Der Schutzbedarf beschreibt, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist.

Sicherheitsgateway Ein Sicherheitsgateway (oft auch Firewall genannt) ist ein System aus soft- und hardwaretechnischen Komponenten zur Gewährleistung einer sicheren Kopplung von IP-Netzen durch Einschränkung der technisch möglichen auf die in einer IT-Sicherheitsleitlinie ordnungsgemäß definierte Kommunikation.
Sicherheit bei der Netzkopplung bedeutet hierbei vor allem die ausschließliche Zulassung erwünschter Zugriffe oder Datenströme zwischen verschiedenen Netzen und die Kontrolle der übertragenen Daten.
Die Verwendung des Begriffs Sicherheitsgateway anstatt des üblicherweise verwendeten Begriffs „Firewall“ soll verdeutlichen, dass zur Absicherung von Netzübergängen heute nicht mehr ein einzelnes Gerät verwendet wird, sondern eine Menge von Rechnern, die unterschiedliche Aufgaben übernehmen, z. B. Paketfilterung, Schutz vor Viren oder die Überwachung des Netzverkehrs.
(Definition aus [BSI-SICH-GW])

Sicherheitskonzept In einem Sicherheitskonzept werden die konzeptionellen Sicherheitsanforderungen systematisch festgelegt und das Vorgehen zu ihrer Umsetzung in Maßnahmen beschrieben.

Sicherheitsleitlinie Die Sicherheitsleitlinie definiert das angestrebte Sicherheitsniveau, mit dem Aufgaben durch die Organisation erfüllt werden.

Trojaner (Trojanisches Pferd) Programm, welches sich als nützliches Werkzeug tarnt, jedoch schädlichen Programmcode einschleust und im Verborgenen unerwünschte Aktionen ausführt.

Anlage 1.3 Verzeichnis der Grafiken

Anlage 1.4 Literatur- und Quellenverzeichnis

[BSI-EGOV-HB] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): E-Government-Handbuch. http://www.bsi.de/fachthem/egov/3.htm, Bonn 2006

[BSI-GSHB04] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): IT-Grundschutzhandbuch. Stand: 2004. http://www.bsi.bund.de/gshb/deutsch/index.htm, Bonn 2004

[BSI-PENTEST] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Durchführungskonzept für Penetrationstests. http://www.bsi.de/literat/studien/pentest/index.htm, Bonn 2003

[BSI-SICH-GW] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Konzeption von Sicherheitsgateways. http://www.bsi.de/fachthem/sinet/loesungen_netze/konzsichgw.htm, Bonn 2005

Anlage 1.5 Internet-Linksammlung

Gesetzgebende Einrichtungen

BMI	http://www.bmi.bund.de/
BMJ	http://www.bmj.bund.de/

Technische Informationen

Checkpoint	http://www.checkpoint.de/
Cisco Systems, Inc.	http://www.cisco.com/
GeNUA mbH	http://www.genua.de/
Linux iptables	http://www.netfilter.org/
Red Hat Inc.	http://www.redhat.com/
SANS Top 20 Risiken	http://www.sans.org/top20/
SUSE LINUX AG	http://www.suse.de/

Organisationen, Verbände und sonstige Informationen

Baseler Ausschuss für Bankenaufsicht	http://www.bis.org/bcbs/
BSI	http://www.bsi.bund.de/
Bundesbeauftragten für den Datenschutz	http://www.datenschutz.bund.de/
Deutsche Gesetzestexte	http://bundesrecht.juris.de/bundesrecht/GESAMT_index.html
Dienstleistungsportal des Bundes	http://www.bund.de/
KBSt	http://www.kbst.bund.de/
Sarbanes-Oxley Act	http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf
Weitere Datenschutzadressen	http://www.datenschutz.bund.de/anschriften/index.html

Revision

Auditors Sharing Audit Programs	http://www.auditnet.org/asapind.htm
Information Systems Audit and Control Association	http://www.isaca.de/
IT-Revision und IT-Sicherheit	http://www.it-audit.de/
Linux Audit	http://www.isaca.de/LinuxAuditAid/indexD.html
Revision und Revisoren im Internet	http://www.revision-online.com/html/ron_t_www.html