Bundesamt
für Sicherheit in der
Informationstechnik

Umsetzungshinweise zum Baustein: ORP.4. Identitäts- und Berechtigungsmanagement

1. Einleitung

Benutzer oder auch IT-Komponenten, die auf die Ressourcen einer Institution zugreifen, müssen zweifelsfrei identifiziert und authentisiert werden. Die Verwaltung der dafür notwendigen Informationen wird als Identitätsmanagement bezeichnet.

Beim Berechtigungsmanagement geht es darum, ob und wie Benutzer oder IT-Komponenten auf Informationen oder Dienste zugreifen und diese benutzen dürfen. Außerdem steht im Fokus, mit welchen Prozessen die dafür notwendigen Rechte vergeben, entzogen und kontrolliert werden können.

Die Übergänge zwischen beiden Begriffen sind fließend, daher wird in diesem Umsetzungshinweis der Begriff Identitäts- und Berechtigungsmanagement (engl.: Identity and Access Management) verwendet.

Generell wird im IT-Grundschutz zwischen den Begriffen "Zugang", "Zugriff" und "Zutritt" unterschieden. Mit "Zugang" wird die Nutzung von IT-Systemen, System-Komponenten und Netzen bezeichnet. Zugangsberechtigungen erlauben somit einer Person, bestimmte Ressourcen wie IT-Systeme bzw. System-Komponenten und Netze zu nutzen.

"Zugriff" bezeichnet die Nutzung von Informationen bzw. Daten. Über Zugriffsberechtigungen wird geregelt, welche Personen im Rahmen ihrer Funktionen oder welche IT-Anwendungen bevollmächtigt sind, Informationen, Daten oder auch IT-Anwendungen zu nutzen oder Transaktionen auszuführen.

Mit "Zutritt" wird das Betreten von abgegrenzten Bereichen wie z. B. Räumen oder geschützten Arealen in einem Gelände bezeichnet. Zutrittsberechtigungen erlauben somit Personen, bestimmte Umgebungen zu betreten, beispielsweise ein Gelände, ein Gebäude oder definierte Räume eines Gebäudes.

Zur besseren Verständlichkeit wird in diesem Umsetzungshinweis der Begriff "Benutzerkennung" bzw. "Kennung" synonym für "Benutzerkonto", "Login" und "Account" verwendet. In diesem Umsetzungshinweis wird der Begriff "Passwort" als allgemeine Bezeichnung für "Passphrase", "PIN" oder "Kennwort" verwendet.

2. Maßnahmen

Im Folgenden sind spezifische Maßnahmen für die Anforderungen des Bausteins ORP.4 *Identitäts- und Berechtigungsmanagement* aufgeführt.

Alle Maßnahmen (gekennzeichnet mit M) sind aufsteigend nummeriert und korrespondieren mit den entsprechenden Anforderungen (gekennzeichnet mit A).

2.1 Maßnahmen zum Baustein ORP.4 Identitäts- und Berechtigungsmanagement

ORP.4.M1 Regelung für die Einrichtung und Löschung von Benutzern und Benutzergruppen (B)

Regelungen, die festlegen, wie Benutzer und Benutzergruppen eingerichtet werden, sind die Voraussetzung für eine angemessene Vergabe von Zugriffsrechten und stellen einen geordneten und überwachbaren Betriebsablauf sicher.

Es sollte ein Formblatt existieren, um von jedem Benutzer bzw. für jede Benutzergruppe zunächst die erforderlichen Daten abzufragen:

- Name, Vorname,
- Vorschlag für die Benutzer- bzw. Gruppenkennung, wenn diese nicht durch Konventionen vorgegeben sind,
- Organisationseinheit,
- Erreichbarkeit (z. B. Telefon, Raum),
- falls erforderlich: Projekt,
- falls erforderlich: Angaben über die geplante Tätigkeit im System und die dazu benötigten Rechte sowie die Dauer der Tätigkeit,
- falls erforderlich: Restriktionen auf Zeiten, Endgeräte, Plattenvolumen, Zugriffsberechtigungen (für bestimmte Verzeichnisse, Remote-Zugriffe etc.), eingeschränkte Benutzerumgebung sowie
- falls erforderlich: Zustimmung von Vorgesetzten.

Jede Benutzerkennung muss eindeutig einem registrierten Benutzer zugeordnet werden können. Sollten Zugriffsberechtigungen vergeben werden, die über den üblichen Standard hinausgehen, muss dies begründet werden. Das kann auch in elektronischer Form erfolgen, z. B. durch ein spezielles Login, dessen Name und Passwort den einzurichtenden Benutzern bekanntgegeben wird. Dort wird ein entsprechendes Programm durchlaufen, das mit einem Logout endet. Die erfassten Daten sollten anschließend überprüft werden, z. B. durch den Vorgesetzten. Ein Passwort, das einem Benutzer für die erstmalige Systemnutzung mitgeteilt wird, muss danach gewechselt werden. Dies sollte vom System initiiert werden.

Es sollte eine begrenzte Anzahl von Rechteprofilen festgelegt werden. Ein neuer Benutzer wird dann einem solchen Profil zugeordnet und erhält damit genau die für seine Tätigkeit erforderlichen Rechte. Dabei sind die systemspezifischen Möglichkeiten bei der Einrichtung von Benutzern und Gruppen zu beachten. Es ist sinnvoll, Namenskonventionen für die Benutzer- und Gruppennamen festzulegen (z. B. mit Benutzer-ID, Kürzel der Organisationseinheit, lfd. Nummer usw.).

Die Zugriffsberechtigung für Dateien ist auf Benutzer bzw. Gruppen mit berechtigtem Interesse zu beschränken. Wenn mehrere Personen auf eine Datei zugreifen müssen, sollte für diese eine Gruppe eingerichtet werden. Jedem Benutzer muss eine eigene Benutzerkennung zugeordnet sein, es dürfen nicht mehrere Benutzer unter derselben Kennung arbeiten. Bei Kennungen gegenüber Betriebssystemen ist für jeden Benutzer ein eindeutiges Heimatverzeichnis anzulegen.

Für die Einrichtungsarbeiten im System sollte eine administrative Rolle geschaffen werden. Die Einrichtung sollte mithilfe eines speziellen Logins erfolgen, unter dem ein entsprechendes Programm oder Skript gestartet wird. Die zuständigen Administratoren können Benutzer bzw. Benutzergruppen somit nur auf definierte Weise einrichten. Es ist nicht erforderlich, ihnen Rechte für andere Administrationsaufgaben zu geben.

ORP.4.M2 Einrichtung, Änderung und Entzug von Berechtigungen (B)

In einer Institution müssen viele verschiedene Berechtigungen pro Benutzer vergeben und verwaltet werden (siehe ORP.4.M5 *Vergabe von Zutrittsberechtigungen,* ORP.4.M6 *Vergabe von Zugangsberechtigungen,* ORP.4.M7 *Vergabe von Zugriffsrechten*). Es sollte für die jeweilige Anwendung bzw. für das jeweilige System ein Rollenmodell entwickelt werden, mit dem aufgabenspezifische Berechtigungen zugewiesen und verwaltet werden können.

Benutzerkennungen und Berechtigungen unterliegen einem Lebenszyklus, sie werden angelegt, geändert und gelöscht. Berechtigungen sollten zentral verwaltet werden. Hilfreich sind dabei angemessene Benutzer- und Rechtemanagement-Werkzeuge, um den Administrations- und Pflegeaufwand zu reduzieren.

Einrichtung und Änderungen von Berechtigungen

Bei der Einrichtung von Benutzerkennungen und Berechtigungen sind häufig viele Genehmigungsschritte erforderlich, die zusammengetragen und verfolgt werden müssen. Daher ist es empfehlenswert, dafür ein standardisiertes und möglichst automatisiertes Antrags- und Vergabeverfahren zu nutzen.

Beim Identitäts- und Berechtigungsmanagement können folgende generische Rollen betrachtet werden:

- Benutzer: Dies ist die Einzelperson, die auf die Informationen, Anwendungen oder IT-Systeme unter der Benutzerkennung zugreift. Mit Ausnahme von Gruppenkennungen ist der Benutzer normalerweise identisch mit dem Besitzer.
- Genehmigende: Dies sind die Personen, die die Vergabe von Zugangs-, Zugriffs- oder Zutrittsrechten genehmigen, typischerweise die Fachverantwortlichen. Ein Genehmigender sollte keine Rechte für sich selbst genehmigen dürfen.
- Fachverantwortliche: Die Fachverantwortlichen sind die Eigentümer von Informationen, Anwendungen, Fachverfahren, Geschäftsprozessen oder Systemen. Sie haben das letzte Wort zu allen Fragen im Zusammenhang mit Inhalten und Verwendung sowie zu Anforderungen an die jeweiligen Informationen, zu Anwendungen oder Systemen.
- IT-Betrieb: Die Mitarbeiter des IT-Betriebs haben die Aufgabe, die genehmigten Berechtigungen technisch einzurichten.

Generell sollten Benutzerkennungen und Berechtigungen immer nur so vergeben werden, wie es für die Aufgabenwahrnehmung notwendig ist (Prinzip *Need-to-know*). Berechtigungen sollten außerdem immer restriktiv vergeben werden (Prinzip der geringsten Berechtigungen, engl. *Least Privileges*).

Bevor neue Benutzerkennungen eingerichtet oder Berechtigungen vergeben werden, ist zu beachten:

- Es muss ein Antrag gestellt werden, aus dem die Rolle, Funktionsbreite und auch zeitliche Begrenzungen der Aufgaben des Antragstellers erkennbar sind. Es empfiehlt sich, die Form der Anträge vorzugeben, damit alle erforderlichen Informationen erfasst werden (siehe ORP.4.M1 *Regelung für die Einrichtung von Benutzern und Benutzergruppen*). Hierfür können Formblätter, Webformulare oder E-Mails verwendet werden. Anträge sollten einfach zu stellen und zu bearbeiten sein, aber auch alle erforderlichen Informationen enthalten.
- Der Antrag muss durch die zuständige Rolle genehmigt werden. Privilegierte Benutzerkennungen müssen zusätzlich vom Fachverantwortlichen der jeweiligen Ressource genehmigt werden.
- Alle vergebenen, geänderten und gelöschten Berechtigungen müssen dokumentiert und gespeichert werden.
- Jede Benutzerkennung muss eindeutig einem registrierten Benutzer zugeordnet werden können. Ebenso muss für jede Gruppenkennung eindeutig nachweisbar sein, welche Personen dieser Gruppe zugehören.

Für jede Gruppenkennung muss eine einzelne Person bzw. ein Rolleninhaber als Verantwortlicher für die Nutzung der Kennung benannt sein.

- Bevor einer Person eine Benutzerkennung oder ein Authentisierungsmittel, wie ein Passwort, zugeteilt wird, muss diese dazu verpflichtet werden, alle Sicherheitsvorgaben und -regelungen einzuhalten.
- Passwörter für Erst-Anmeldungen müssen bei der ersten Anmeldung des Benutzers geändert werden (siehe ORP.4.M8 *Regelung des Passwortgebrauchs*).
- Es muss sichergestellt sein, dass nur die berechtigten Benutzer die Zurücksetzung eines Passwortes oder die Anpassung eines Authentisierungsmittels anfordern können.
- Es sollte möglichst vermieden werden, Gruppenkennungen einzurichten, wenn dies die Zuordnung zu den handelnden Personen erschwert. Dies gilt vor allem für administrative Kennungen und sicherheitsrelevante Bereiche.

Wird ein Zugriff auf Daten benötigt, ohne dass der Besitzer der Kennung zugestimmt hat, muss dieser Zugriff sowohl von einem autorisierten Genehmigenden als auch vom Informationssicherheitsbeauftragten (ISB) genehmigt werden. Ein solcher Zugriff ist zu dokumentieren und dem Besitzer mitzuteilen.

Entzug von Berechtigungen

Wenn Mitarbeiter die Institution verlassen oder die Funktion in der Institution wechseln, müssen die nicht mehr benötigten Benutzerkennungen und Berechtigungen innerhalb einer definierten Zeit gesperrt und nach einer definierten Wartezeit vollständig gelöscht werden. Dabei kann es sinnvoll sein, zwar die Berechtigungen zu löschen, aber in den Unterlagen zu dokumentieren, von wann bis wann die Benutzerkennung welche Berechtigungen hatte, um auch Aktionen nach dem Weggang von Mitarbeitern nachvollziehbar zu halten. Wichtig ist, dass die Berechtigungen durchgängig aktuell gehalten werden.

Zum Entzug bzw. zur Sperrung von Benutzerkennungen und Authentisierungsmitteln gehört beispielsweise, dass Benutzerkennungen deaktiviert, Passwörter geändert und Mitarbeiterausweise eingezogen werden. Außerdem muss die Benutzerkennung in Rollenzuweisungen und Gruppen entfernt werden. Voraussetzung dafür ist, dass die für das Berechtigungsmanagement zuständige Stelle zeitnah informiert wird, wenn Mitarbeiter ausscheiden. Gegebenenfalls ist ein entsprechender Punkt in eine einschlägige Checkliste der Personalabteilung aufzunehmen.

Es wird empfohlen, Benutzerkennungen zunächst lediglich zu deaktivieren (beispielsweise für einen Monat), damit sie im Fehlerfall leicht wieder eingerichtet werden können. Alle Benutzerkennungen und die damit verbundenen Daten müssen jedoch mittelfristig, z. B. innerhalb von drei Monaten nach Weggang des Mitarbeiters von den Produktivsystemen entfernt werden. Um die dort gespeicherten Informationen und die Nachvollziehbarkeit von Tätigkeiten für einen längeren Zeitraum sicherzustellen, sollten die Daten in einen anderen Bereich, z. B. ein Archivsystem kopiert werden.

ORP.4.M3 Dokumentation der Benutzerkennungen und Rechteprofile (B)

Zugelassene Benutzer, angelegte Benutzergruppen und Rechteprofile müssen dokumentiert werden. Dabei gibt es verschiedene Dokumentationsmöglichkeiten, wie beispielsweise über

- vorgegebene Administrationsdateien des Systems,
- individuelle Dateien, die vom zuständigen Administrator verwaltet werden oder
- Listen und Aufstellungen in Papierform.

Es sollte eine geeignete Form ausgewählt werden, möglichst einheitlich für die gesamte Institution.

Dokumentiert werden sollten insbesondere folgende Angaben zur Rechtevergabe an Benutzer und Benutzergruppen:

Zugelassene Benutzer:

- zugeordnetes Rechteprofil (auch mögliche Abweichungen vom verwendeten Standard-Rechteprofil),
- Begründung für die Wahl des Rechteprofils (und der Abweichungen),

- Zuordnung des Benutzers zu einer Organisationseinheit, einer Raum- und Telefonnummer,
- Zeitpunkt und Grund der Einrichtung sowie
- Befristung der Einrichtung.

Zugelassene Gruppen:

- zugehörige Benutzer,
- Zeitpunkt und Grund der Einrichtung sowie
- Befristung der Einrichtung.

Die Dokumentation der zugelassenen Benutzer und Rechteprofile sollte regelmäßig (mindestens alle 6 Monate) daraufhin überprüft werden, ob sie den tatsächlichen Stand der Rechtevergabe widerspiegelt und ob die Rechtevergabe noch den Sicherheitsanforderungen und den aktuellen Aufgaben der Benutzer entspricht. Nach System- oder Anwendungsupdates sollte die Dokumentation ebenfalls überprüft werden. Die vollständige Dokumentation ist Voraussetzung für Kontrollen der vergebenen Benutzerrechte.

Die Dokumentation muss so gespeichert bzw. aufbewahrt werden, dass sie vor unberechtigtem Zugriff geschützt ist und so, dass auch bei einem größeren Sicherheitsvorfall oder IT-Ausfall darauf zugegriffen werden kann. Falls die Dokumentation in elektronischer Form erfolgt, muss sie in das Datensicherungsverfahren einbezogen werden.

ORP.4.M4 Aufgabenverteilung und Funktionstrennung (B)

Die im Baustein ORP.1 *Organisation* in Anforderung ORP.1.A4 *Funktionstrennung zwischen unvereinbaren Aufgaben* definierten unvereinbare Aufgaben und unvereinbare Funktionen müssen durch das Identitäts- und Berechtigungsmanagement umgesetzt werden.

Nachdem die einzuhaltenden Funktionstrennungen festgelegt wurden, können die Funktionen den jeweiligen Personen zugeordnet werden. Vertreterregelungen sind dabei ebenfalls zu berücksichtigen und zu dokumentieren.

Die hier getroffenen Festlegungen sind zu dokumentieren und, falls sich Änderungen ergeben, zu aktualisieren. Sollte es vorkommen, dass eine Person miteinander unvereinbare Funktionen wahrnehmen muss, so ist das in der Dokumentation über die Funktionsverteilung besonders hervorzuheben.

ORP.4.M5 Vergabe von Zutrittsberechtigungen (B)

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

Anschließend ist festzulegen, welche Person welches Zutrittsrecht benötigt, um ihre Aufgaben auszuüben. Dabei ist die vorher erarbeitete Funktionstrennung zu beachten. Unnötige Zutrittsrechte sind zu vermeiden.

Um die Zahl zutrittsberechtigter Personen zu einem Raum möglichst gering zu halten, sollte der Grundsatz der Funktionstrennung berücksichtigt werden. So verhindert z. B. eine getrennte Lagerung von IT-Ersatzteilen und Datenträgern, dass ein Wartungstechniker unerlaubt auf die Datenträger zugreifen kann.

Alle vergebenen und wieder entzogenen Zutrittsberechtigungen sind zu dokumentieren. Wenn Zutrittsberechtigungen entzogen werden, muss gewährleistet sein, dass die Zutrittsmittel wieder zurückgenommen werden. Zusätzlich ist zu dokumentieren, ob es Konflikte bei der Vergabe der Zutrittsberechtigungen an Personen gab. Gründe für Konflikte können vorliegen, wenn Personen Funktionen wahrnehmen, die bezüglich der Zutrittsberechtigungen der Funktionstrennung entgegenstehen, oder aufgrund räumlicher Notwendigkeiten.

Zur Überwachung der Zutrittsberechtigung können sowohl Personen wie Pförtner oder ein Schließdienst als auch technische Einrichtungen, z. B. Ausweisleser, biometrische Verfahren wie Iris- oder Fingerabdruck-Scanner sowie Sicherheitstürschlösser eingesetzt werden. Nicht autorisiertes Personal, z. B. Besucher oder

Reinigungs- und Wartungspersonal, dürfen nur zusammen mit zutrittsberechtigten Mitarbeitern schutzbedürftige Räume betreten.

Ebenfalls muss geregelt werden, wie Zutrittsberechtigungen an Fremdpersonal und Besucher vergeben und wieder entzogen werden.

ORP.4.M6 Vergabe von Zugangsberechtigungen (B)

Zugangsberechtigungen erlauben der betreffenden Person oder einem autorisierten Vertreter, bestimmte IT-Systeme bzw. System-Komponenten und Datennetze zu nutzen. Zugangsberechtigungen sollten möglichst restriktiv vergeben werden. Diese sind für jede nutzungsberechtigte Person aufgrund ihrer Funktion unter Beachtung der Funktionstrennung im Einzelnen festzulegen. Entsprechend der Funktion ist zu definieren, wie die nutzungsberechtigten Personen auf die IT-Systeme zugreifen können, also wie etwa der Systemverwalter Zugang zum Betriebssystem oder ein Anwender Zugang zu einer IT-Anwendung erhält. Ergänzend hierzu muss sichergestellt sein, dass personelle und aufgabenbezogene Änderungen unverzüglich berücksichtigt werden.

Auf IT-Systeme oder IT-Anwendungen darf erst nach einer Identifikation des Nutzungsberechtigten, z. B. durch Name, Benutzerkennung oder Chipkarte, und Authentisierung, z. B. durch ein Passwort oder über ein Authentisierungstoken, zugegriffen werden können. Dies sollte protokolliert werden.

Es ist zu dokumentieren, wann und wie Zugangsmittel, wie Benutzerkennungen oder Chipkarten, ausgegeben und entzogen werden. Regelungen, wie mit Zugangs- und Authentisierungsmitteln, z. B. Chipkarten oder Passwörtern, umgegangen werden darf, müssen ebenfalls getroffen werden (siehe auch ORP.4.M8 *Regelung des Passwortgebrauchs*). Alle Zugangsberechtigten müssen auf den korrekten Umgang mit den Zugangsmitteln hingewiesen werden.

Zugangsberechtigungen sollten bei längeren Abwesenheiten von berechtigten Personen vorübergehend gesperrt werden, etwa bei Krankheit oder Urlaub. Dies sollte zumindest bei Personen mit weitreichenden Berechtigungen wie Administratoren erfolgen.

Es sollte sporadisch kontrolliert werden, ob die Festlegungen eingehalten werden.

ORP.4.M7 Vergabe von Zugriffsrechten (B)

Über Zugriffsrechte wird geregelt, welche Person im Rahmen ihrer Funktion bevollmächtigt wird, IT-Anwendungen oder Daten zu nutzen. Die Zugriffsrechte auf IT-Anwendungen, Teilanwendungen oder Daten sind von der Funktion abhängig, die die Person wahrnimmt. Bei erhöhtem Schutzbedarf sollte sichergestellt werden, dass angemessene Identifikations- und Authentisierungsmechanismen eingesetzt werden. Dabei sollten immer nur so viele Zugriffsrechte vergeben werden, wie es für die Aufgabenwahrnehmung notwendig ist (Need-to-know-Prinzip). Die Zugriffsrechte müssen durch die Rechteverwaltung des IT-Systems vergeben werden.

Viele IT-Systeme lassen es zu, dass verschiedene Rechte als Gruppenrechte bzw. als Rechteprofil definiert werden (z. B. Gruppe *Datenerfassung*). Diese Definition entspricht der technischen Umsetzung der Rechte, die einer Funktion zugeordnet werden. Für die Administration der Rechte eines IT-Systems ist es vorteilhaft, solche Gruppen oder Profile zu erstellen, damit die Rechte einfacher zugeteilt und aktualisiert werden können.

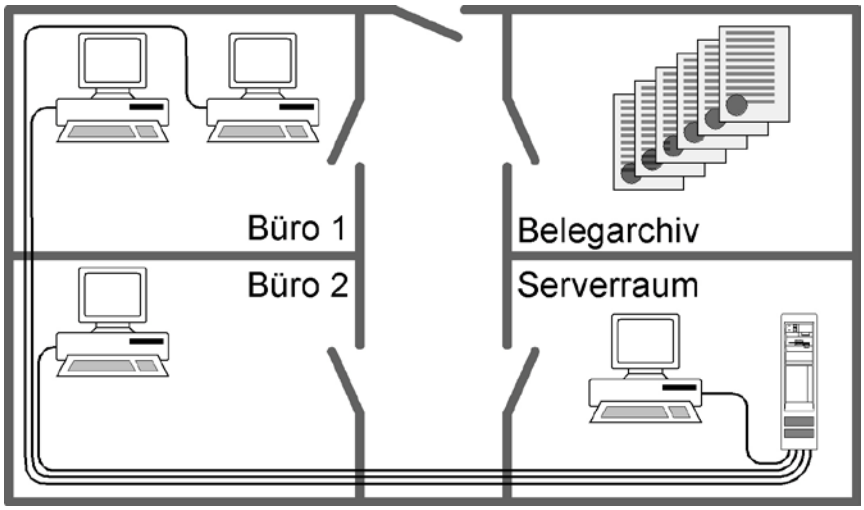
Die Festlegung und Veränderung von Zugriffsrechten ist vom jeweils Verantwortlichen zu veranlassen und zu dokumentieren. Aus der Dokumentation muss hervorgehen,

- welche Funktion unter Beachtung der Funktionstrennung mit welchen Zugriffsrechten ausgestattet wird,
- welche Gruppen bzw. Profile eingerichtet werden,
- welche Person welche Funktion wahrnimmt,
- welche Zugriffsrechte eine Person im Rahmen welcher Rolle erhält (hierbei sollten auch die Zugriffsrechte von Vertretern erfasst werden),

- welche Konflikte bei der Vergabe von Zugriffsrechten aufgetreten sind (diese Konflikte können z. B. daraus resultieren, dass eine Person unvereinbare Funktionen wahrnimmt oder daraus, dass abhängig vom IT-System bestimmte Zugriffsrechte nicht getrennt werden können),
- welche Personen in einem Notfall welche Zugriffsrechte erhalten, z. B. der Krisenstab.

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

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



Schritt 1: Aufgabenverteilung und Funktionstrennung

Folgende Funktionen sind für das betrachtete Reisekosten-Abrechnungssystem notwendig:

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

Folgende Funktionen sind aufgrund der Sachzwänge nicht miteinander vereinbar:

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

Diese Funktionen werden durch folgende Personen wahrgenommen:

Nr.	Funktion/Person	Hr. Mayer	Fr. Schmidt	Hr. Müller	Fr. Fleiß
1.	LAN-Administration	x			
2.	Revision		x		
3.	Datenerfassung			x	
4.	Sachbearbeitung rechn.			x	

Nr.	Funktion/Person	Hr. Mayer	Fr. Schmidt	Hr. Müller	Fr. Fleiß
5.	Sachbearbeitung sachl.			x	
6.	Anordnungsbefugnis				x

Schritt 2: Vergabe von Zutrittsrechten

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

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

Nr.	Funktion/Raum	Serverraum	Belegarchiv	Büro 1	Büro 2
1.	LAN-Administration	x			
2.	Revision	x	x	x	x
3.	Datenerfassung			x	
4.	Sachbearbeitung rechn.		x	x	
5.	Sachbearbeitung sachl.		x	x	
6.	Anordnungsbefugnis		x	x	x

Schritt 3: Vergabe von Zugangsberechtigungen

Aufgrund der Funktionen ergeben sich folgende Zugangsberechtigungen:

Nr.	Funktion/Anwendung	Betriebssystem Server	Anwendung Protokollauswertung	Anwendung Datenerfassung	Anwendung Belegbearbeitung
1.	LAN-Administration	x			
2.	Revision	x	x		x
3.	Datenerfassung			x	
4.	Sachbearbeitung rechn.				x
5.	Sachbearbeitung sachl.				x
6.	Anordnungsbefugnis				x

Schritt 4: Vergabe von Zugangsberechtigungen

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

A = Recht zur Ausführung der Anwendung/Software

L = Leserecht auf Daten

S = Schreibrecht, d. h. Erzeugen von Daten

M = Recht zum Modifizieren von Daten

Ö = Recht zum Löschen von Daten

U = Recht zum Unterschreiben von Zahlungsanweisungen

Nr.	Funktion/Anwendung	Betriebssystem Server	Anwendung Protokollauswertung	Anwendung Datenerfassung	Anwendung Belegbearbeitung
1.	LAN-Administration	A, L, S, M, Ö			
2.	Revision	A, L	A, L, Ö		A, L
3.	Datenerfassung			A, S	
4.	Sachbearbeitung rechn.				A, L, M
5.	Sachbearbeitung sachl.				A, L, M
6.	Anordnungsbefugnis				A, L, U

Schritt 5: Vergabe von Zugriffsrechten

Eine solche Dokumentation erleichtert die Rechteverteilung. Angenommen, Frau Schmidt wechselt den Arbeitgeber und ihre Stelle müsste neu besetzt werden. Anhand der obigen Tabellen lässt sich einfach feststellen, welche der ehemaligen Rechte Frau Schmidts zu löschen und für die neue Kraft einzurichten sind. Wenn die neue Kraft aber z. B. zusätzlich vertretungsweise die Funktion "Sachbearbeitung mit Anordnungsbefugnis" übernehmen soll, wird bei der Rechteverteilung deutlich, dass die neue Kraft im Vertretungsfall unbemerkt Manipulationen vornehmen könnte.

ORP.4.M8 Regelung des Passwortgebrauchs (B)

Grundsätzlich ist zu überlegen, ob überhaupt Passwörter als alleiniges Authentisierungsverfahren eingesetzt werden sollten oder ob anstelle von Passwörtern andere Authentisierungsverfahren bzw. zusätzliche Authentisierungsmerkmale verwendet werden können, wie Zertifikate oder eine Mehr-Faktor-Authentisierung.

Um Passwörter zu erstellen und handzuhaben, muss es feste Regelungen geben. Die Benutzer von IT-Systemen sind diesbezüglich zu unterweisen. So muss vorgebeugt werden, schwache Passwörter zu verwenden und falsch mit ihnen umzugehen. Folgende Regeln zum Passwortgebrauch müssen beachtet werden:

- Passwörter müssen geheim gehalten werden und nur dem Benutzer persönlich bekannt sein.
- Passwörter dürfen allenfalls für die Hinterlegung schriftlich fixiert werden. Hierbei ist zwischen der physischen Hinterlegung, z. B. auf Papier, und der digitalen, z. B. in einem Passwort-Manager, zu unterscheiden.
- Bei der physischen Hinterlegung muss das Passwort in einem versiegelten Umschlag sicher aufbewahrt werden.
- Passwörter dürfen nicht auf programmierbaren Funktionstasten von Tastaturen oder Mäusen gespeichert werden.
- Da Menschen sich lange und komplizierte Passwörter in der Regel schlecht merken können und zudem für jede Anwendung ein anderes Passwort zu verwenden ist, sollte die Nutzung eines Passwort-Managers geprüft werden. Sicherheitsmaßnahmen für diese sind unten beschrieben.
- Ein Passwort muss gewechselt werden, wenn es unautorisierten Personen bekannt geworden ist oder der Verdacht dazu besteht.

- Die Wiederverwendung bereits eingesetzter Passwörter sollte unterbunden werden. Gegebenenfalls können Regelungen erlassen werden, dass Passworte nach einer angemessenen Zeitspanne wiederverwendet werden dürfen.
- Passwörter dürfen nur unbeobachtet eingegeben werden.
- Voreingestellte Passwörter und Kennungen, z. B. des Herstellers bei Auslieferung von IT-Systemen, müssen durch individuelle Passwörter und, wenn möglich, Kennungen ersetzt werden.

Passwort-Manager

Wenn der Passwort-Manager kompromittiert wurde, sind alle darin enthaltenen Passwörter betroffen. Bevor ein Passwort-Manager eingesetzt wird, ist daher der Schutzbedarf der Passwörter zu bestimmen, die damit gespeichert werden sollen. Nicht alle Passwort-Manager eignen sich dafür, hochschutzbedürftige Passwörter zu speichern. Wenn ein Tool benutzt werden soll, um Passwörter zu speichern, sind die im Folgenden beschriebenen Anforderungen an solche Werkzeuge zu beachten:

- Ein Passwort-Manager sollte komfortabel nutzbar sein. Die Länge und der Zeichenzusammensetzung der sicher hinterlegten Passwörter sollte nicht eingeschränkt sein. Es sollte möglich sein, lange und komplexe Master-Passwörter zu benutzen, dies sollte möglichst auch technisch gefordert werden.
- Ein Passwort-Manager darf auf keinen Fall die Möglichkeit bieten, dass Benutzer auf die Passwörter zugreifen können, ohne ein Master-Passwort einzugeben oder dass das Master-Passwort vom Tool gespeichert und automatisch eingetragen werden kann.
- Nach einem vorgegebenen Inaktivitäts-Zeitraum sollte das Tool den angemeldeten Benutzer automatisch abmelden.
- Passwörter dürfen nur verschlüsselt gespeichert werden. Dafür muss der Passwort-Manager ein anerkanntes Verschlüsselungsverfahren mit ausreichender Schlüssellänge verwenden. Wenn verschiedene Verschlüsselungsverfahren ausgewählt werden können, muss ein geeignetes gewählt werden.
- Bei Einsatz eines Passwort-Managers sollten regelmäßig Schwachstellenmeldungen, z. B. des CERT-Bund, überprüft werden, um sicherzustellen, dass keine Sicherheitslücken bekannt geworden sind.
- Da der Zugriff auf Passwort-Manager sehr gut abgesichert sein muss, kann es sinnvoll sein, Produkte mit spezieller Sicherheitshardware einzusetzen. Dies können z. B. Passwort-Tools auf USB-Token oder Chipkarte sein.
- Als Schutz vor Keyloggern kann es auch sinnvoll sein, einen Passwort-Manager einzusetzen, bei dem die Passwörter über eine mausgesteuerte Bildschirm-Tastatur eingegeben werden. Diese sollte einerseits sowohl Zahlen, als auch Buchstaben und Sonderzeichen anbieten, damit möglichst vielfältige Passwörter ausgewählt werden können. Andererseits sollten die Zeichen dynamisch in der Bildschirmtastatur angezeigt werden, also die Zeichen nach jeder Eingabe an einer anderen Stelle angeordnet sein. Dies macht zwar für die Benutzer die Eingabe langsamer, erschwert aber, dass Schadsoftware anhand der Zeichenposition auf dem Bildschirm das Passwort mitlesen kann.
- Passwort-Manager sollten möglichst nur auf vertrauenswürdigen IT-Systemen benutzt werden, also solchen IT-Systemen, die unter der eigenen Aufsicht bzw. unter der Kontrolle der eigenen Institution stehen. Dies können beispielsweise Mobiltelefone oder spezielle Authentisierungsserver sein.
- Bei Passwort-Managern mit Funktionen oder Plug-ins, mit denen Passwörter über Onlinedienste Dritter synchronisiert oder anderweitig an Dritte übertragen werden, müssen diese Funktionen und Plug-ins deaktiviert werden.

ORP.4.M9 Identifikation und Authentisierung (B)

Der Zugriff zu allen IT-Systemen und Diensten muss durch eine angemessene Identifikation und Authentisierung der zugreifenden Benutzer, Dienste oder IT-Systeme abgesichert sein. Dazu ist im Rahmen eines Authentisierungskonzeptes zu definieren, welche Funktions- und Sicherheitsanforderungen an die

Authentisierung gestellt werden (siehe ORP.4.M12 *Entwicklung eines Authentisierungskonzeptes für IT-Systeme und Anwendungen*).

Die Identifikation und Authentisierung muss vor jeder Interaktion zwischen IT-System, IT-Anwendung, Dienst und Benutzer erfolgen. Weitere Interaktionen dürfen nur nach der erfolgreichen Identifikation und Authentisierung möglich sein. Die Authentisierungsinformationen müssen so gespeichert sein, dass nur autorisierte Benutzer darauf zugreifen können bzw. diese prüfen oder ändern können. Bei jeder Interaktion muss das IT-System, die IT-Anwendung und der Dienst die Identität des Benutzers feststellen können.

Bevor Nutzerdaten übertragen werden, muss der Kommunikationspartner, d. h. das IT-System, der Prozess oder der Benutzer, eindeutig identifiziert und authentisiert sein. Erst nach der erfolgreichen Identifikation und Authentisierung dürfen die Nutzdaten übertragen werden. Beim Empfang von Daten muss deren Absender eindeutig identifiziert und authentisiert werden können. Alle Authentisierungsdaten müssen vor unbefugtem Zugriff und vor Fälschung geschützt sein.

Hinweise für die geeignete Auswahl von Authentisierungsmechanismen sind in ORP.4.M13 *Geeignete Auswahl von Authentisierungsmechanismen* zu finden.

ORP.4.M10 Schutz von Benutzerkennungen mit weitreichenden Berechtigungen (S)

Benutzerkonten mit weitreichenden Berechtigungen sollten mit starker Authentisierung mit mindestens zwei Authentisierungsmerkmalen geschützt werden. Hierbei werden zwei Authentisierungstechniken kombiniert, wie Passwort plus Transaktionsnummer (Einmalpasswort) oder plus Chipkarte. Daher wird dies auch häufig als Mehr-Faktor-Authentisierung bezeichnet.

ORP.4.M11 Zurücksetzen von Passwörtern (S)

Solange Benutzer sich mit Passwörtern authentisieren müssen, wird es vorkommen, dass sie ihre Passwörter vergessen. Einerseits soll Benutzern in so einer Situation schnell geholfen werden, damit sie wieder arbeiten können. Andererseits muss verhindert werden, dass sich Unberechtigte durch unzureichende Berechtigungsprüfungen Zugriff auf IT-Systeme verschaffen können. Daher muss jede Institution für das Zurücksetzen von Passwörtern geeignete Vorgehensweisen auswählen.

Wichtig ist dabei, dass für das Zurücksetzen von Passwörtern flexible Richtlinien definiert werden. Ein starres Vorgehen ist in den meisten Fällen in der heutigen mobilen Arbeitswelt nicht praktikabel. Einerseits sollte das Vorgehen dem Schutzbedarf des jeweiligen Passwortes entsprechen. Andererseits sollten aber auch die Zugriffsanforderungen der Benutzer berücksichtigt werden.

Welche Vorgehensweise jeweils angemessen ist, hängt von vielen Faktoren ab, beispielsweise von der Größe der Institution oder der Anzahl der Mitarbeiter. Auch der Einsatzort der Beschäftigten spielt eine Rolle: Sind diese immer vor Ort oder oft beim Kunden? Wie sind diese dann erreichbar? Das sind Fragen, die unter anderem beantwortet werden müssen. Nicht zuletzt ist der Schutzbedarf der durch das Passwort geschützten Informationen und Geschäftsprozesse zu berücksichtigen. Dazu ist zu klären, ob der Zugriff nur auf lokale IT-Systeme, auf ein LAN, auf interne Netze von außerhalb oder auf ein Internet-Postfach oder Ähnliches erfolgt.

Hinweis: Das übliche Authentisierungsverfahren mithilfe von Benutzername und Passwort ist in der Regel für den normalen Schutzbedarf geeignet. Für einen höheren Schutzbedarf sollten stärkere Authentisierungsverfahren eingesetzt werden, beispielsweise durch die Kombination mit Chipkarte, USB-Token oder Einmalpasswort-Verfahren.

Im Folgenden werden die Vor- und Nachteile einiger Varianten zur Passwort-Rücksetzung dargestellt, aus denen die für den jeweiligen Anwendungsfall angemessenen Verfahren ausgewählt werden können.

Schriftlich per Post oder Fax

Dabei wird für das Zurücksetzen eines Passworts ein Formular verwendet, das der Benutzer ausfüllen und unterschreiben muss. Dieses Formular wird dann per Post oder Fax an den IT-Betrieb geschickt. Dieses Verfahren ist gründlich, vor allem, wenn die Formulare archiviert werden. Der Nachteil ist, dass es je nach Größe der Institution einige Zeit dauern kann, bis das Formular per (Haus-)Post beim IT-Betrieb ankommt. Um zu verhindern, dass sich ein Unberechtigter im Namen eines berechtigten Benutzers ein Passwort

zurücksetzen lässt, sollten bei dieser Variante Vergleichsunterschriften vorliegen. Der Bearbeiter im IT-Betrieb muss dann die Unterschrift auf dem Formular mit der hinterlegten Unterschrift vergleichen.

Die Antwort mit dem neuen Passwort könnte der Bearbeiter ebenfalls per Post, etwa in einem versiegelten Umschlag, oder per Fax übersenden. Bei einem Fax kann meist nicht sichergestellt werden, dass wirklich nur der Benutzer das Passwort erhält.

Telefonisch ohne Zusatzmerkmale

Die einfachste Variante ist, Passwörter per Telefon zurückzusetzen. Allerdings ist es dabei aufwendig, den Benutzer zu verifizieren. Der IT-Betrieb muss in der Lage sein, anhand der Stimme den Benutzer zu identifizieren. In kleineren Institutionen, in denen sich die Beschäftigten alle persönlich kennen, ist diese Lösung möglich.

Eine Überprüfung der Telefonnummer ist hingegen nicht ausreichend, denn diese könnte gefälscht sein. Ein Angreifer könnte auch die Abwesenheit eines Mitarbeiters nutzen, um aus dessen Büro heraus beim IT-Betrieb anzurufen. Da genau dieses Szenario im Fokus von Social-Engineering-Angriffen steht, sollte auf diese Variante möglichst verzichtet werden.

Telefonisch plus Wissensfrage

Um einen Passwort-Wechsel per Telefon vorzunehmen, kann der IT-Betrieb auch zusätzliche Wissensmerkmale abfragen, die vorher hinterlegt wurden. Das können beispielsweise das Geburtsdatum oder die Personalnummer des Mitarbeiters sein. Es kann sich auch um Merkwörter handeln, die sich der Benutzer zwar leicht merken kann, die aber schwer zu erraten sind. Hierfür empfiehlt es sich, nicht nur einen Begriff zu hinterlegen, sondern mehrere, und eventuell zu jedem Begriff auch eine passende Frage zu formulieren. Beispielsweise könnte beim IT-Betrieb dann eine Frage wie: "Wie hieß das Haustier, das Sie mit 10 Jahren hatten?" mit der passenden Antwort hinterlegt sein.

Es sollten hierbei möglichst keine einfachen Wissensfragen wie "Wie ist der Vorname ihres Vaters?" verwendet werden, da diese Antworten leicht herauszufinden sind.

Identitätsüberprüfung mittels schon abgespeicherter Informationen

Bei einer Anfrage per Telefon kann zur Identitätsüberprüfung auch auf andere, bei der Registrierung des Benutzers schon abgespeicherte, Informationen zurückgegriffen werden. Das könnte beispielsweise eine Mitarbeiterkennziffer oder das Geburtsdatum sein. Ein Nachteil ist, dass die meisten solcher typischerweise vorab erfassten Informationen vielerorts bekannt sind und meist auch schnell über das Internet recherchiert werden können.

Persönliche Vorsprache

Dabei muss sich der Benutzer direkt an eine bestimmte Person wenden und den Passwort-Wechsel veranlassen. Diese Person kann, je nach Größe der Institution, entweder ein Vorgesetzter, ein Fachverantwortlicher oder ein Mitarbeiter des IT-Betriebs sein. Diese Person sollte auf jeden Fall dazu berechtigt sein, die (Neu-)Vergabe von Zugriffsrechten zu genehmigen und deren Einrichtung zu beauftragen oder selbst durchzuführen.

Beauftragung einer vertrauenswürdigen Person

Bei dieser Variante könnte beispielsweise ein Kollege beauftragt werden, eine signierte E-Mail an den IT-Betrieb zu senden, in der er um die Zurücksetzung des Passwortes bittet. Durch die kryptografische Signatur kann überprüft werden, wer die Anfrage gestellt hat. Hat er hierfür keinen Auftrag erhalten, könnte ein Angriff nachträglich nachgewiesen werden.

Das neue Passwort könnte in einer verschlüsselten E-Mail der beauftragten Person übermittelt werden, das er dem betroffenen Benutzer mitteilt. Zusätzlich sollte der Benutzer über die Zurücksetzung informiert werden, damit ein möglicher Angriff entdeckt werden kann.

Dieser Ansatz hat allerdings die Nachteile, dass ein Angriff im Allgemeinen erst nachträglich festgestellt und dass ein Dritter das Rücksetzungspasswort erfahren würde.

Zurücksetzen auf Einmal-Passwörter

Generell sollte der IT-Betrieb bei der Rücksetzung von Passwörtern nur Einmal-Passwörter vergeben, sodass die Benutzer diese unmittelbar nach der erfolgreichen Anmeldung auf ein nur ihnen bekanntes Passwort ändern müssen. Dabei sollte der IT-Betrieb darauf achten, kein einheitliches Passwort zur Rücksetzung zu verwenden, da dieses schnell bekannt werden würde. Das Passwort sollte außerdem so komplex sein, dass es nicht leicht zu erraten ist.

Außerdem sollte der IT-Betrieb verifizieren, ob das Passwort wirklich zurückgesetzt werden muss.

Mitteilung des Rücksetzungspasswortes

Um dem betroffenen Mitarbeiter das neue Passwort mitzuteilen, können ebenfalls verschiedene Wege gewählt werden, beispielsweise:

- Der IT-Betrieb teilt dem Mitarbeiter das neue Passwort durch einen zweiten vordefinierten Weg mit, z. B. per Hauspost oder Rückruf auf eine vorher registrierte Telefonnummer (von dieser darf nicht die Anfrage zur Rücksetzung stammen).
- Das Passwort kann einem Vorgesetzten, einem Sekretariat oder einer anderen vertrauenswürdigen Stelle mitgeteilt werden, die den Mitarbeiter kennt und diesen informiert.
- Das Passwort wird an eine vorab registrierte Post- oder E-Mail-Adresse gesendet.
- Das Passwort wird per Kurier versendet, der den Ausweis des Empfängers überprüft.

Schulung der Mitarbeiter im IT-Betrieb

Wichtig ist, dass die Mitarbeiter im IT-Betrieb zum Berechtigungsmanagement ausreichend geschult werden. Sie sollten sowohl typische Social-Engineering-Methoden kennen, um einen unberechtigten Zugang zu Informationen oder IT-Systemen abwehren zu können, als auch den Umgang mit Problemfällen und flexiblen Lösungsmöglichkeiten gelernt haben. Die Erfahrung zeigt, dass eine starre Vorgehensweise leichter zu hintergehen ist, vor allem, wenn sie einem Angreifer bekannt ist. Wenn beispielsweise festgelegt wurde, dass bei einer Passwort-Rücksetzung immer der Vorgesetzte zu informieren ist, dieser aber gerade nicht da ist, ist es besser, einen geeigneten Vertreter zu suchen, als zu lange zu warten.

Wenn der Schutzbedarf des jeweiligen Passworts zu hoch ist und der Mitarbeiter des IT-Betriebs aufgrund fehlender sicherer Möglichkeiten die Verantwortung nicht übernehmen möchte, muss es für diese Situation eine Eskalationsstrategie geben.

Information der Mitarbeiter

Alle Benutzer sollten darüber informiert sein, was sie tun müssen, wenn sie ein Passwort vergessen haben. Außerdem sollten alle Benutzer aufmerksam werden, wenn sie bei einem Anmeldeversuch feststellen, dass sie sich nicht mit ihrem korrekten Passwort anmelden können. Neben Vergesslichkeit könnte dies auch ein Zeichen dafür sein, dass sich ein Angreifer unbefugten Zugriff verschafft hat. Im Zweifelsfall sollte so ein Vorfall dem Sicherheitsmanagement gemeldet werden.

ORP.4.M12 Entwicklung eines Authentisierungskonzeptes für IT-Systeme und Anwendungen (S)

Es ist sinnvoll, ein Authentisierungskonzept zu erstellen, das für jedes IT-System bzw. jede Anwendung die Funktions- und Sicherheitsanforderungen an die Authentisierung definiert.

Wenn Institutionen neue IT-Systeme oder Anwendungen einführen wollen, muss vorher geklärt werden, wie sich Benutzer vor dem Zugriff auf das IT-System oder die mit der Anwendung verarbeiteten Daten authentisieren.

Im Authentisierungskonzept ist zu klären, ob das IT-System bzw. die Anwendung überhaupt über Authentisierungsmechanismen verfügen soll. Bei Bürokommunikationssoftware ist dies z. B. unüblich, da die Berechtigung auf der Ebene der verarbeiteten Dokumente geregelt wird. Ist eine Authentisierung jedoch vorgesehen, ist zu klären, ob das IT-System oder die Anwendung über eine eigenständige Benutzerverwaltung verfügt oder ob die Authentisierung über einen zentralen Verzeichnisdienst erfolgen soll (siehe APP.2.1 *Allgemeiner Verzeichnisdienst*). Kann ein Verzeichnisdienst genutzt werden, sollte geklärt werden, ob ein Single-Sign-On (SSO) vorgesehen ist.

Grundsätzlich sollte die Anbindung einer selbst entwickelten Authentisierung an einen Verzeichnisdienst oder SSO-Dienst angestrebt werden. Ist dies nicht möglich, sollte in jedem Fall sichergestellt werden, dass Authentisierungsinformationen verdeckt eingegeben werden können. Authentisierungsinformationen dürfen nicht unverschlüsselt auf Datenträgern, wie Festplatten, gespeichert oder über Kommunikationsnetze übertragen werden (siehe ORP.4.M8 *Regelung des Passwortgebrauchs*).

Weitere, im Konzept behandelte Aspekte können sein:

- Vorgaben für ein Log-in-Banner: Es ist beispielsweise sinnvoll, bei einer Anmeldung sowohl Nutzungshinweise als auch den letzten Anmeldezeitpunkt anzuzeigen. Andererseits sollten Log-in-Banner nicht zu viele Informationen enthalten, vor allem keine, die Angreifern Ansatzpunkte liefern könnten, wie z. B. Netzadressen oder Art und Version der eingesetzten Software.
- Behandlung paralleler Sitzungen eines Benutzers in der Anwendung: Wenn sie erlaubt sind, sollte die maximale Anzahl definiert werden.
- Absicherung der Authentisierungsinformationen: Es ist festzulegen, wie die Authentisierungsinformationen kryptografisch abgesichert übermittelt und gespeichert werden können.
- Untätigkeit des Benutzers: Es sollte eine zeitgesteuerte Zwangstrennung sowie eine geeignete Information, etwa ein Hinweisfenster, bei vollzogener automatischer Trennung und Abmeldung erfolgen.

Außerdem sollte die vorgesehene Art und Stärke der Authentisierungsmechanismen beschrieben werden. Hierbei sind insbesondere folgende Kriterien zu berücksichtigen:

- Art und Kombination der eingesetzten Techniken bzw. Faktoren zur Authentisierung (Wissen, Besitz, biometrische Merkmale) sowie
- Stärke der eingesetzten Faktoren (beim Faktor Wissen siehe auch ORP.4.M8 *Regelung des Passwortgebrauchs*).

ORP.4.M13 Geeignete Auswahl von Authentisierungsmechanismen (S)

Die Identifikations- und Authentisierungsmechanismen von IT-Systemen bzw. IT-Anwendungen müssen so gestaltet sein, dass Benutzer eindeutig identifiziert und authentisiert werden (siehe ORP.4.M9 *Identifikation und Authentisierung*).

Es gibt verschiedene Techniken, um die Authentizität eines Benutzers nachzuweisen. Die bekanntesten sind:

- PINs (Persönliche Identifikationsnummern),
- Passwörter,
- Token, z. B. Zugangskarten sowie
- biometrische Verfahren.

Für sicherheitskritische Anwendungsbereiche sollte eine Mehr-Faktor-Authentisierung benutzt werden, z. B. Passwort plus Transaktionsnummer (Einmalpasswort) oder plus Chipkarte. Beide eingesetzten Authentisierungstechniken müssen sich auf dem aktuellen Stand der Technik befinden.

Im Folgenden werden verschiedene Kriterien aufgezeigt, die beachtet werden sollten, wenn Identifikations- und Authentisierungsmechanismen ausgewählt werden. Nicht alle marktgängigen Systeme erfüllen alle Kriterien, diese sollten aber bei der Auswahl entsprechend berücksichtigt werden. Viele IT-Produkte beinhalten bereits neben ihrer eigentlichen Funktionalität Authentisierungsmechanismen, beispielsweise Betriebssysteme. Hier ist zu überprüfen, ob diese den Ansprüchen genügen oder ob sie um zusätzliche Funktionen erweitert werden müssen. Auch dazu eignen sich die folgenden Kriterien.

Administration der Authentisierungsdaten

Authentisierungsdaten für Benutzern dürfen nur von autorisierten Administratoren angelegt oder geändert werden. Werden Passwörter verwendet, sollten nur autorisierte Benutzer ihre eigenen Authentisierungsdaten innerhalb festgesetzter Grenzen verändern können. Das IT-System sollte über einen

geschützten Mechanismus verfügen, damit Benutzer ihre Passwörter selbstständig verändern können. Dabei sollte es möglich sein, eine Mindestlebensdauer für Passwörter vorzugeben.

Nachdem sich Benutzer erfolgreich angemeldet haben, sollte ihnen Datum und Zeit des letzten erfolgreichen Zugriffs angezeigt werden.

Schutz der Authentisierungsdaten vor Veränderung

Das IT-System bzw. IT-Anwendung muss die Authentisierungsdaten bei der Verarbeitung jederzeit davor schützen, dass sie ausgespäht, verändert oder zerstört werden. Das kann beispielsweise geschehen, indem die Passwortdateien verschlüsselt und die eingegebenen Passwörter nicht angezeigt werden. Die Authentisierungsdaten sind getrennt von Applikationsdaten zu speichern.

Systemunterstützung

Werden institutionsweite Authentisierungsverfahren eingesetzt, sollten diese nur auf Servern betrieben werden, deren Betriebssystem einen adäquaten Schutz vor Manipulationen bietet. Werden Authentisierungsverfahren ausgewählt, ist darauf zu achten, dass diese möglichst plattformübergreifend eingesetzt werden können.

Fehlerbehandlung bei der Authentisierung

Das IT-System bzw. die IT-Anwendung sollte nach jedem erfolglosen Authentisierungsversuch weitere Anmeldeversuche zunehmend verzögern (Time Delay). Die Gesamtdauer eines Anmeldeversuchs sollte begrenzt werden können. Das IT-System bzw. die IT-Anwendung sollte Anmeldevorgänge nach einer vorgegebenen Anzahl erfolgloser Authentisierungsversuche beenden können. Nach Überschreitung der vorgegebenen Anzahl erfolgloser Authentisierungsversuche muss das IT-System bzw. die IT-Anwendung in der Lage sein, den Benutzer-Account bzw. das Terminal zu sperren bzw. die Verbindung zu unterbrechen.

Administration der Benutzerdaten

Das IT-System bzw. die IT-Anwendung sollte die Möglichkeit bieten, den Benutzern verschiedene Voreinstellungen zuweisen zu können. Diese sollten angezeigt und verändert werden können. Die Möglichkeit, Benutzerdaten zu verändern, muss auf den autorisierten Administrator beschränkt sein. Wenn die Administration der Benutzerdaten über eine Kommunikationsverbindung erfolgen soll, muss diese ausreichend kryptografisch gesichert sein.

Definition der Benutzereinträge

Das IT-System bzw. die IT-Anwendung muss es ermöglichen, dass die Sicherheitsrichtlinie umgesetzt werden kann, indem für jeden Benutzer die entsprechenden Sicherheitseinstellungen gewählt werden können.

Ein Authentisierungsverfahren sollte auch erweiterbar sein, z. B. um starke Authentisierungstechniken, wie Token oder Chipkarten zu unterstützen (siehe auch ORP.4.M21 *Mehr-Faktor-Authentifizierung*).

Umfang der Benutzerdaten

Neben Benutzernamen und Rechteprofil sollten noch weitere Informationen über jeden Benutzer hinterlegt werden (siehe auch ORP.4.M1 *Regelung für die Einrichtung von Benutzern und Benutzergruppen*):

- Es sollte mindestens Vorname und Nachname eines Benutzers in der Benutzerverwaltung aufgenommen werden. Zusätzlich ist auch die Telefon- und Raumnummer hilfreich.
- Um mit dem Benutzer in Kontakt zu treten, sollten zusätzlich auch Informationen wie E-Mail-Adresse, Telefonnummer und geografischer Standort (Adresse, Raumnummer) erfasst werden.
- Zusätzlich sollte erfasst werden, wie lange die Benutzerkennung gültig sein soll. Ist die Benutzerkennung abgelaufen, sollte sie gesperrt werden.

Passwortgüte

Wenn Passwörter eingesetzt werden, um sich an IT-Systemen bzw. IT-Anwendung zu authentisieren, sollte das IT-System bzw. die IT-Anwendung Mechanismen bieten, die Bedingungen aus ORP.4.M8 *Regelung des Passwortgebrauchs* erfüllen.

Biometrie

Unter Biometrie im hier verwendeten Sinn ist das automatisierte Erkennen von Personen anhand ihrer körperlichen Merkmale zu verstehen. Um biometrische Verfahren für die Authentisierung einsetzen zu können, werden eventuell zusätzliche Peripherie-Geräte benötigt, die die Benutzer auf Grundlage besonderer Merkmale eindeutig authentisieren können. Eine oder mehrere der folgenden biometrischen Merkmale können beispielsweise für eine Authentisierung verwendet werden:

- Iris,
- Fingerabdruck,
- Gesichtsproportionen,
- Stimme und Sprachverhalten,
- Handschrift sowie
- Tippverhalten.

Neben einer Vielzahl von biometrischen Merkmalen und darauf basierenden biometrischen Verfahren bestehen darüber hinaus auch große Unterschiede zwischen den verfügbaren konkreten biometrischen Systemen und Produkten. Die Leistungsfähigkeit von biometrischen Verifikationssystemen ist sehr unterschiedlich. In sicherheitskritischen Bereichen muss darauf geachtet werden, dass das biometrische System eine akzeptable Erkennungsleistung und eine hohe Sicherheit bietet. Es darf nicht möglich sein, dass es mithilfe von Nachbildungen wie z. B. einer Gesichtsmaske, einer Wachsnachbildung des Fingers oder Kontaktlinsen mit Irismuster überlistet werden kann.

Authentisierung mit Token

Eine weitere Alternative bieten Authentisierungstoken, also externe Datenträger, die als Speicherplatz für die Authentisierungsdaten dienen, wie z. B. kryptografische Schlüssel. Typische Beispiele für Authentisierungstoken sind Chipkarten, USB-Sticks oder Geräte, die Einmalpasswörter erzeugen.

Anforderungen an Authentisierungsmechanismen für Benutzer

Das IT-System bzw. die IT-Anwendung muss vor jeder anderen Benutzertransaktion die Benutzeridentität überprüfen. Es sollte darüber hinaus erkennen und verhindern können, dass Authentisierungsdaten der Benutzer oder gefälschte bzw. kopierte Authentisierungsdaten von Benutzern wieder eingespielt werden. Das IT-System bzw. die IT-Anwendung darf die Authentisierungsdaten erst dann überprüfen, wenn sie vollständig eingegeben wurden.

Es sollte für jeden Benutzer individuell einstellbar sein, wann und von wo er auf das IT-System bzw. die IT-Anwendung zugreifen darf.

Protokollierung der Authentisierungsmechanismen

Authentisierungsvorgänge sind in einem sinnvollen Umfang zu protokollieren. Die Protokolldateien sollten in regelmäßigen Abständen von den Administratoren überprüft werden. Das IT-System bzw. die IT-Anwendung muss die folgenden Ereignisse protokollieren können:

- Ein- und Ausschalten der Protokollierung,
- jeden Versuch, auf Mechanismen zum Management von Authentisierungsdaten zuzugreifen,
- erfolgreiche Versuche, auf Authentisierungsdaten zuzugreifen,
- jeden Versuch, unautorisiert auf Authentisierungsdaten von Benutzern zuzugreifen,
- jeden Versuch, auf Funktionen zur Administration von Benutzereinträgen zuzugreifen,
- Änderungen an Benutzereinträgen,
- jeden durchgeführten Test auf Passwort-Güte,
- jede Benutzung von Authentisierungsmechanismen,

- jede Konfiguration der Abbildung von Authentisierungsmechanismen zu spezifischen Authentisierungsereignissen sowie
- die Installation von Authentisierungsmechanismen.

Jeder Protokolleintrag sollte Datum, Uhrzeit, Art des Ereignisses, Bezeichnung des Subjektes sowie Erfolg bzw. Misserfolg der Aktion enthalten.

ORP.4.M14 Kontrolle der Wirksamkeit der Benutzertrennung am IT-System bzw. an der Anwendung (S)

In angemessenen Zeitabständen ist zu überprüfen, ob sich die Benutzer von IT-Systemen bzw. Anwendungen regelmäßig abmelden, nachdem sie eine Aufgabe erfüllt haben, oder ob mehrere Benutzer unter einer Kennung arbeiten. Dazu sollten Protokolle ausgewertet oder Stichproben gemacht werden.

Sollte festgestellt werden, dass tatsächlich mehrere Benutzer unter einer Kennung arbeiten, sind sie darauf hinzuweisen, dass sie zum Abmelden verpflichtet sind, wenn sie ihre Aufgabe beendet haben. Gleichzeitig sollte der Sinn dieser Maßnahme erläutert werden, die im Interesse des einzelnen Benutzers liegt.

Stellt sich heraus, dass die An- und Abmeldevorgänge zu zeitintensiv sind und trotz Aufforderung nicht akzeptiert werden, sollten alternative Maßnahmen diskutiert werden, wie zum Beispiel:

- Das IT-System bzw. Anwendung kann für bestimmte Zeitintervalle einem Benutzer zugeordnet werden, sodass in dieser Zeit andere Benutzer das IT-System nicht nutzen dürfen. Das setzt voraus, dass der Arbeitsprozess dementsprechend zeitlich variabel ist.
- Es können zusätzliche IT-Systeme bzw. Anwendungen angeschafft werden, mit denen die Arbeit an nur einem IT-System bzw. nur einer Anwendung vermieden werden kann.
- Statt zeitaufwendigen mehrstufigen Authentisierungsverfahren könnten automatisierte Authentisierungsverfahren, wie beispielsweise über RFID-basierte Token oder biometrische Verfahren, eingesetzt werden.
- Es sollten unterschiedliche Zugriffsrechte für die Daten eingeräumt werden.

ORP.4.M15 Vorgehensweise und Konzeption der Prozesse beim Identitäts- und Berechtigungsmanagement (S)

Es sollte ein übergreifendes Konzept für das Identitäts- und Berechtigungsmanagement für die gesamte Institution geben. Daraus sollten für einzelne Bereiche oder Systeme angepasste Regelungen abgeleitet werden können. Das Konzept sollte die einzelnen Aufgaben und Prozessschritte für das Identitäts- und Berechtigungsmanagement beschreiben, die dann auf die einzelnen Bereiche angepasst werden müssen. Dazu gehören:

- Erstellen eines Überblicks über Gruppen und Arten von Identitäten und Berechtigungen, die typischerweise in den verschiedenen Bereichen einer Institution verwaltet werden,
- Vorgaben zur Verwaltung von Identitäten, Benutzerkennungen und Berechtigungen,
- Vorgaben zum Umgang mit den Benutzerkennungen, Berechtigungen und Authentisierungsmitteln durch die Benutzer,
- Vorgaben zum Umgang mit Kennungen von Administratoren, Notfallbenutzern und anderen privilegierten Benutzern sowie Vorgaben für den zeitlich eingeschränkten Zugriff auf erweiterte Berechtigungen,
- Festlegen von Berechtigungsstrukturen, Dokumentation und Genehmigungsverfahren für die Vergabe von Berechtigungen,
- Festlegen und Einhalten von Administrationsprozessen,
- Vorgaben zur Erstellung und restriktiven Zuweisung von Berechtigungen auf den Zielsystemen,
- regelmäßige Überprüfung der Berechtigungen darauf, ob

- alle Personen und Prozesse die notwendigen Berechtigungen haben, also weder zu viele noch zu wenige (nach dem Need-to-Know- und Least-Privilege-Prinzip),
- alle Berechtigungen aktuell sind, es also z. B. keine Benutzerkennungen gibt, die nicht mehr aktiv sind, aber nicht gelöscht wurden sowie
- es Berechtigungen gibt, die den Benutzern unter Umgehung des Identitäts- und Berechtigungsmanagements direkt auf den Zielsystemen zugewiesen wurden.

Grundsätzlich ist für jeden Bereich zunächst zu klären, welchen Schutzbedarf die zu schützenden Informationen und Geschäftsprozesse haben, welche Gefährdungen relevant sind und welche Sicherheitsmaßnahmen bereits vorhanden sind. Außerdem muss geregelt werden, wer die Informationen und Geschäftsprozesse wie nutzen darf.

Richtlinien erstellen

Es sollte Richtlinien für das Identitäts- und Berechtigungsmanagement geben, in denen spezifisch für den betreffenden Bereich und die Zielgruppe, wie z. B. Administratoren, Benutzer oder Fachverantwortliche, die einzelnen Aufgaben und Prozessschritte beschrieben werden. Dazu gehören die folgenden Punkte:

- Wer ist zuständig für die Verwaltung von Identitäten, Benutzerkennungen und Berechtigungen?
- Wer darf Berechtigungen genehmigen?
- Was müssen die Benutzer über den korrekten Umgang mit den Benutzerkennungen, Berechtigungen und Authentisierungsmitteln wissen?

Außerdem sollte es Vorgaben für die Art und Ausgestaltung der jeweiligen Authentisierung geben, z. B. über die Art der Authentisierung, über Besitz, Wissen oder biometrische Verfahren sowie die Mindestanforderungen an Passwörter (siehe ORP.4.M16 *Richtlinie für die Zugriffs- bzw. Zugangskontrolle* und ORP.4.M8 *Regelung des Passwortgebrauchs*).

Zu regeln ist auch, welche Personen auf welche Weise Zugriff auf welche Informationen erhalten, also z. B. ob nur aus dem Intranet oder auch von unterwegs zugegriffen werden darf, und welche IT-Systeme dabei für Zugriffe zugelassen sind.

Dabei müssen die spezifischen Rahmenbedingungen berücksichtigt werden, wie z. B. vorhandene Sicherheitsrichtlinien und gesetzliche Vorgaben. Bereits vorhandene Berechtigungskonzepte müssen konsolidiert und in einem übergreifenden Konzept zusammengeführt werden. Dabei dürfen auch verteilte Anwendungen nicht vergessen werden. Daher ist es meistens sinnvoll, Programme zur Benutzer- und Rechte-Verwaltung einzusetzen.

Funktionen trennen

Ein Identitäts- und Berechtigungsmanagement muss den Ansatz verfolgen, Aufgaben und Funktionen und somit auch Berechtigungen geeignet zu trennen und entsprechend gesetzlicher oder organisatorischer Vorgaben auf verschiedene Mitarbeiter zu verteilen (siehe ORP.4.M4 *Aufgabenverteilung und Funktionstrennung*).

Rollen trennen

Personen können verschiedene Rollen wahrnehmen. Dabei müssen diese Rollen aber organisatorisch und technisch klar voneinander getrennt werden, insbesondere bei unterschiedlichen Sicherheitsanforderungen. Es sollte verhindert werden, dass sich mehrere sicherheitskritische Rollen auf eine Person konzentrieren.

Berechtigungen anlegen, ändern und löschen

Im Mittelpunkt des Identitäts- und Berechtigungsmanagement steht, wie Berechtigungen angelegt, geändert und gelöscht werden (siehe ORP.4.M2 *Regelung für Einrichtung, Änderung und Entzug von Berechtigungen*).

Mit Passwörtern umgehen

Es muss geregelt werden, wie Authentisierungsmechanismen anzuwenden sind. Außerdem müssen die Benutzer darin eingewiesen werden (siehe ORP.4.M8 *Regelung zum Passwortgebrauch*, ORP4.M9 *Identifikation und Authentisierung*, ORP4.M13 *Geeignete Auswahl von Authentisierungsmechanismen*).

In jeder Institution muss es eine geeignete Vorgehensweise für den Umgang mit Identitäten und Berechtigungen geben. Es wird daher empfohlen, die Aufgaben aus den generischen Prozessen der Maßnahme ORP.4.M15 *Vorgehensweise und Konzeption der Prozesse beim Identitäts- und Berechtigungsmanagement* in der Institution einzurichten.

Prozesse beim Identitäts- und Berechtigungsmanagement

Ein Identitäts- und Berechtigungsmanagement besteht meist aus folgenden generischen Prozessen:

- Richtlinien verwalten,
- Identitätsprofile verwalten,
- Benutzerkennungen verwalten,
- Berechtigungsprofile verwalten sowie
- Rollen verwalten.

Richtlinien verwalten

Im Rahmen des Prozesses "Richtlinien verwalten" werden Richtlinien für die Beantragung, Veränderung und den Entzug von Rollen und (Einzel-)Berechtigungen sowie die Verwaltung von Identitäten und Benutzerkonten innerhalb von IT-Systemen erstellt, überprüft und fortgeschrieben.

In der Richtlinie zum Identitäts- und Berechtigungsmanagement werden die Vorgehensweisen zu den folgenden Prozessen beschrieben. Außerdem wird definiert, wie diese zusammenspielen sollten:

- Identitätsprofile verwalten,
- Benutzerkennungen verwalten,
- Berechtigungsprofile verwalten sowie
- Rollen verwalten.

Die Richtlinien sollten bei wesentlichen Änderungen oder in bestimmten zeitlichen Abständen einem Review unterzogen werden.

Identitätsprofile verwalten

Im Prozess "Identitätsprofile verwalten" werden Identitätsprofile erfasst, verändert und gelöscht. Identitätsprofile sind beispielsweise Stammdaten von Mitarbeitern einer Institution. Typische Eigenschaften, die verarbeitet werden, sind

- Name,
- Organisationseinheit und
- Aufgabenbeschreibung.

Die Verarbeitung der Informationen im Prozess "Identitätsprofile verwalten" wird in Form von Anträgen (siehe ORP.4.M1 *Regelung für die Einrichtung von Benutzern und Benutzergruppen*) initiiert. Die Anträge enthalten alle wichtigen Informationen zu einem Mitarbeiter und die entsprechende Aufgabenbeschreibung. Die Anträge werden zum Beispiel erstellt, wenn ein Mitarbeiter neu eingestellt wird oder sich Aufgabenbeschreibungen von Beschäftigten ändern. Die Änderungen werden in einem Identitätsprofil dokumentiert.

Das Ergebnis des Prozesses "Identitätsprofile verwalten" ist ein Identitätsprofil mit Stammdaten und einer konkreten Aufgabenbeschreibung. Es muss geregelt sein, wer die Berechtigungsvergabe initiiert. Der Vorgang muss dokumentiert werden.

Identitätsprofile können beispielsweise von folgenden Abteilungen einer Institution angelegt oder geändert werden:

- Personalabteilung, Verwaltung, Fachabteilung (z. B. bei Neueinstellungen, Personalabgängen, Aufgabenänderungen),

- Einkauf, Beschaffung (z. B. für externe Mitarbeiter),
- Vertrieb, Support (z. B. für neue Kunden oder wenn sich bei Kunden etwas ändert).

Der Prozess "Richtlinie verwalten" regelt die Rahmenbedingungen für das Einrichten und Verändern von Identitäten. Die Informationen der erstellten bzw. überarbeiteten Identitätsprofile werden im Anschluss dem Prozess "Benutzerkennungen verwalten" zum weiteren Verarbeiten übertragen.

Benutzerkennungen verwalten

Der Prozess "Benutzerkennungen verwalten" beschreibt den operativen Anteil der Prozesse innerhalb des Identitäts- und Berechtigungsmanagements. Er umfasst das Anlegen, Löschen und Ändern von Benutzerkennungen, Initialpasswörtern und Berechtigungen. Typische Vorgänge sind z. B.:

- Anlegen neuer Mitarbeiter,
- Anlegen neuer Benutzerkennungen,
- Weggang von Mitarbeitern,
- Veränderung von Aufgaben,
- Kennungen bei längeren Abwesenheiten sperren sowie
- Benutzerkennungen löschen.

Im Rahmen des Vorgangs "*Anlegen neuer Mitarbeiter*" muss eine Benutzerkennung erstellt, ein Initialpasswort vergeben sowie die Organisationseinheit zugeordnet und es müssen Mitarbeiterstammdaten erfasst sowie Rollen und Berechtigungen zugewiesen werden. Eine Neuanlage erfolgt auch, um zusätzliche Benutzerkennungen zu schaffen.

Der Vorgang "Weggang von Mitarbeitern" umfasst das vollständige Löschen aller Rollenzuordnungen und Berechtigungen für den jeweiligen Mitarbeiter sowie, falls erforderlich, die Rückgabe von Authentisierungstoken.

Der Vorgang "Veränderung von Aufgaben" umfasst den Wechsel einer Organisationseinheit, den Ein- und Austritt in Projekte und andere Aufgabenänderungen mit dem jeweiligen Datum. Es kann erforderlich sein, dass einige Berechtigungen vor oder nach der erfolgten Aufgabenänderung zugewiesen werden.

Der Vorgang "Kennungen bei längeren Abwesenheiten sperren" erfolgt bei längerer Abwesenheit von Mitarbeitern, z. B. bei Erziehungsurlaub oder Krankheit. Die Berechtigungen bleiben während des Zeitraums erhalten.

Der Vorgang "Benutzerkennung löschen" enthält das vollständige Löschen der Benutzerkennung einschließlich aller Stammdaten und Berechtigungen.

Jede Benutzerkennung muss eindeutig einem Mitarbeiter als Besitzer zugeordnet sein. Bei Gruppen- und Systemkennungen muss mindestens eine Person als verantwortlich benannt werden.

Mitarbeiter können mehrere Benutzerkennungen haben. Es ist zu klären, ob

- die Benutzerkennungen getrennt geführt werden,
- die Benutzerkennungen getrennt geführt, aber verkettet werden, oder
- die Benutzerkennungen zusammengeführt werden sollen.

Auf jeden Fall ist es zweckmäßig, automatisch zu prüfen, ob es Doppeleinträge gibt. Denn solche Einträge führen zu Intransparenz im Identitäts- und Berechtigungsmanagement.

Der Prozess "Benutzerkennungen verwalten" ordnet die Berechtigungen zu einer Aufgabe innerhalb der IT-Systeme zu. Der Prozess "Richtlinien verwalten" gibt die Rahmenbedingungen vor, wie Berechtigungen in den IT-Systemen zugeordnet werden. Zum Abschluss des Prozesses "Benutzerkennungen verwalten" liegt eine eingerichtete oder veränderte Benutzerkennung inklusive der entsprechenden Berechtigungen vor.

Berechtigungsprofil verwalten

Der Prozess "Berechtigungsprofil verwalten" beschreibt das Verfahren für einen Abgleich zwischen der Aufgabenbeschreibung, die im Prozess "Identitätsprofile verwalten" verfasst wurde, und den dazugehörigen Rollen und Einzelberechtigungen für einen Mitarbeiter.

Für den Abgleich benötigt der Prozess "Berechtigungsprofil verwalten" diverse Informationen über die Identitätsprofile aus verschiedenen Quellen, z. B. die Stammdaten der Mitarbeiter aus der Personalverwaltung oder die Fachaufgaben aus den Fachabteilungen. Dazu gehören auch vergleichbare Informationen zu externen Mitarbeitern sowie zu technischen Berechtigungen von IT-Systemen.

In einem Mitarbeiter-Berechtigungsprofil werden alle Rollen und Einzelberechtigungen verwaltet, die diesem Mitarbeiter zugeordnet sind. Untersucht werden muss, ob Aufgaben und die dazugehörigen Berechtigungen miteinander vereinbar sind oder unter Umständen neu verteilt werden müssen (siehe ORP.4.M4 *Aufgabenverteilung und Funktionstrennung*).

Rollen verwalten

Im Prozess "Rollen verwalten" werden Berechtigungen für einzelne Rollen angelegt. In Rollen werden Aufgaben, Verantwortlichkeiten und damit zusammenhängende Berechtigungen gebündelt, um die Benutzerverwaltung zu erleichtern. Eine Rolle kann somit für mehrere Mitarbeiter mit den gleichen Aufgaben verwendet werden. Dazu werden der Rolle die Zugangsberechtigungen zugeordnet, die für die Aufgabenerfüllung notwendig ist. Rollen sollten modular und in sich geschlossen definiert werden, sodass sie beliebig kombinierbar sind. Der Rollenzuschnitt muss auf Ebene der Fachverantwortlichen abgestimmt werden.

Der Prozess "Rollen verwalten" besteht aus zwei Ebenen: Die Ebene der Fachverantwortlichen definiert die Rollen. Die administrative Ebene legt Berechtigungsprofile für diese Rollen an, ändert und löscht sie.

Der Prozess "Richtlinien verwalten" gibt Regeln vor, wie Rollen gebildet werden. Zwischen dem Prozess "Identitätsprofile verwalten" und dem Prozess "Rollen verwalten" erfolgt der Vergleich der Aufgabenprofile von Mitarbeitern und den tatsächlich zugeordneten Rollen über einen Soll-Ist-Abgleich. Im Prozess "Benutzer verwalten" wird die Zuordnung von Rollen zu Mitarbeitern angelegt, gelöscht oder geändert. Im Prozess "Rollen verwalten" werden Einzelberechtigungen zu einem Berechtigungsprofil für ein Benutzerkonto in der Kontenverwaltung zusammengefasst.

Die dargestellten generischen Prozesse für das Identitäts- und Berechtigungsmanagement können durch weitere unterstützende Prozesse verfeinert und erweitert werden.

ORP.4.M16 Richtlinien für die Zugriffs- und Zugangskontrolle (S)

Um IT-Systeme bzw. Systemkomponenten und Datennetze nutzen zu können, muss die Zugriffs- bzw. Zugangskontrolle geregelt sein. Dazu sollte neben den an den einzelnen IT-Komponenten einzurichtenden Zugriffs- bzw. Zugangskontrollen eine übergreifende Richtlinie existieren, in der die Grundsatzfragen geregelt sind. Die Regelungen zur Zugriffs- bzw. Zugangskontrolle müssen den Schutzbedarf der Institution widerspiegeln. Insbesondere ist hier darauf zu achten, dass einschlägige Gesetze, Vorschriften und Regelungen eingehalten werden, wie z. B. Datenschutz- und Urheberrechtsgesetze bzw. Lizenzregelungen.

Es empfiehlt sich, dabei Standard-Rechteprofile für nutzungsberechtigte Personen aufgrund ihrer Funktionen und Aufgaben festzulegen (siehe auch ORP.4.M5 *Vergabe von Zutrittsberechtigungen*, ORP.4.M6 *Vergabe von Zugangsberechtigungen*, ORP.4.M7 *Vergabe von Zugriffsrechten*). Die Benutzerrechte für Zugriffe auf Dateien und Programme müssen abhängig von der jeweiligen Rolle, dem *Need-to-Know*-Prinzip und der Sensitivität der Daten definiert sein. Falls Rechte vergeben werden, die über den Standard hinausgehen, sollte dies begründet werden.

Die Richtlinien für die Zugriffs- bzw. Zugangskontrolle sollten allen Verantwortlichen für IT-Anwendungen vorliegen. Darauf aufbauend können dann Zugriffsregelungen für die einzelnen IT-Systeme abgeleitet und eingerichtet werden.

Für jedes einzelne IT-System und jede IT-Anwendung sollten schriftliche Zugriffsregelungen vorhanden sein. Das gilt auch für die Dokumentation der Einrichtung von Benutzern und der Rechtevergabe (siehe ORP.4.M1 *Regelung für die Einrichtung von Benutzern und Benutzergruppen*). Dabei müssen die system- bzw. anwendungsspezifischen Besonderheiten und Sicherheitsanforderungen berücksichtigt werden. Die IT-

Verantwortlichen müssen dafür sorgen, dass die system- bzw. anwendungsspezifischen Vorgaben erstellt und aktualisiert werden.

Werden an Mitarbeiter besonders weitgehende Rechte vergeben, z. B. an Administratoren, so sollte dies möglichst restriktiv erfolgen. Dabei sollte zum einem der Kreis der privilegierten Benutzer möglichst eingeschränkt werden und zum anderen sollten nur die für die jeweilige Aufgabe benötigten Rechte vergeben werden. Für alle Aufgaben, die ohne erweiterte Rechte durchgeführt werden können, sollten auch privilegierte Benutzer unter Accounts mit Standard-Rechten arbeiten.

Der Zugriff auf alle IT-Systeme oder Dienste muss durch Identifikation und Authentisierung des zugreifenden Benutzers oder IT-Systems abgesichert werden. Beim Zugriff aus externen Netzen sollten starke Authentisierungsverfahren eingesetzt werden, z. B. solche, die auf dem Einsatz von Einmalpasswörtern oder von Chipkarten basieren.

Beim Anmeldevorgang sollten keine Informationen über das IT-System oder den Fortschritt der Anmeldeprozedur angezeigt werden, bis dieser erfolgreich abgeschlossen ist. Es sollte darauf hingewiesen werden, dass der Zugriff nur autorisierten Benutzern gestattet ist. Die Authentisierungsdaten dürfen erst dann überprüft werden, wenn sie vollständig eingegeben wurden.

Weitere Anforderungen an die Authentisierungsmechanismen finden sich in ORP.4.M13 *Geeignete Auswahl von Authentisierungsmechanismen*.

ORP.4.M17 Geeignete Auswahl von Identitäts- und Berechtigungsmanagement-Systemen (S)

Bei der Auswahl geeigneter Lösungen für das Identitäts- und Berechtigungsmanagement spielen nicht nur technische Fragen eine Rolle. In der Praxis hat sich gezeigt, dass dabei auch organisatorische Aspekte wesentliche Erfolgsfaktoren sind. Ein Identitäts- und Berechtigungsmanagement-System muss in erster Linie auf die Institution und deren jeweilige Geschäftsprozesse, Organisationsstrukturen und Abläufe sowie deren Schutzbedarf passen und erst in zweiter Linie in die vorhandene Infrastruktur eingebunden werden. Es muss die in der Institution vorhandenen Vorgaben zum Umgang mit Identitäten und Berechtigungen abbilden können. Dazu gehören beispielsweise die Anforderungen aus ORP.4.M16 *Richtlinien für die Zugriffs- und Zugangskontrolle*.

Identitäts- und Berechtigungsmanagement-Systeme sind komplexe Systeme, deren Einführung sehr viel Wissen über Technik, Geschäftsprozesse und Berechtigungsmodelle benötigt, so dass es häufig erforderlich ist, mit externen Beratern zusammenzuarbeiten. Die Anbindung der verschiedenen IT-Systeme kann durch unterschiedliche technische Ansätze erfolgen, z. B. mit Verzeichnisdiensten. Eine Herausforderung ist es, die unterschiedliche Berechtigungsverwaltung heterogener Anwendungen zentral zu integrieren.

Zu klären sind u. a. folgende Punkte:

- Soll eine zentrale oder dezentrale Lösung eingesetzt werden?
- Soll ein Single-Sign-On-Verfahren genutzt werden?
- Soll die Authentisierung über Besitz, Wissen beziehungsweise biometrische Eigenschaften erfolgen?
- Soll bei einer zentralen Lösung (Reduced Sign-On) die Anwendung auf Synchronisation oder einem zentralem Datenbank-Abgleich basieren?
- Welche Schnittstellen zur Anbindung von IT-Systemen mit dem Identitäts- und Berechtigungsmanagement-System werden benötigt?

Mit einer Einführung eines Identitäts- und Berechtigungsmanagement-Systems entsteht schnell der Wunsch, dass sich Benutzer nicht an jedem IT-System mit einem anderen Passwort anmelden müssen. Vielmehr möchten sich die Benutzer auch bei großen heterogen Netzen nur am ersten benutzten IT-System authentisieren (Single-Sign-On). Ein solches Verfahren reicht die Authentisierungsinformationen dann an alle weiteren IT-Systeme weiter.

In der Praxis hat es sich bewährt, zunächst einmal ein Reduced-Sign-On anzustreben, also die Anzahl der Anmeldevorgänge je Benutzer zu reduzieren. Bereits dadurch können Benutzer, aber auch die Administratoren, deutlich entlastet werden.

Es gibt eine Vielzahl verschiedener Mechanismen zur Identifikation ebenso wie zur Authentisierung. Bei der Auswahl geeigneter Mechanismen sollte der Schutzbedarf der damit geschützten Informationen und Geschäftsprozesse im Vordergrund stehen (siehe auch ORP.4.M13 *Geeignete Auswahl von Authentisierungsmechanismen*).

Für eine geeignete Auswahl eines Identitäts- und Berechtigungsmanagement-Systems sind aus den konkreten Anforderungen der Institution Auswahlkriterien abzuleiten (siehe hierzu auch die Maßnahmen *ORP.4.M13 Geeignete Auswahl von Authentisierungsmechanismen und* ORP.4.M12 *Entwicklung eines Authentisierungskonzeptes für Anwendungen*).

Im Folgenden sind einige Auswahlkriterien für ein Identitäts- und Berechtigungsmanagement-System beispielhaft aufgelistet:

- Kann der Grundsatz der Funktionstrennung realisiert werden (ORP.4.M4 *Aufgabenverteilung und Funktionstrennung*)?
- Ist das Identitäts- und Berechtigungsmanagement-System in der Lage, die unterschiedliche Berechtigungsverwaltung heterogener Anwendungen zentral zu integrieren?
- Unterstützt die Anwendung den Einsatz der geplanten Authentisierungsfaktoren Wissen, Besitz und Biometrie?
- Können die Authentisierungsanforderungen je nach Schutzbedarf skaliert werden?
- Sind durchgängige Rechte-Änderungen bis hin zum Rechte-Entzug kurzfristig möglich, wenn diese akut benötigt werden, etwa wenn ein Mitarbeiter fristlos gekündigt wird?
- Werden Authentisierungsdaten bei Speicherung und Verarbeitung ausreichend geschützt, d. h., nicht als Klartext, sondern stets verschlüsselt gespeichert und übertragen?
- Entsprechen die im Identitäts- und Berechtigungsmanagement-System vorhandenen kryptographischen Funktionen dem Schutzbedarf und besitzen sie eine ausreichende Stärke im Prozess?
- Werden die Authentisierungsdaten sicher verwaltet? Ist sichergestellt, dass beispielsweise Passwörter nie unverschlüsselt auf den entsprechenden IT-Systemen gespeichert werden?
- Wie schnell können die Identitäten, Berechtigungen oder Passwörter geändert werden, z. B. bei einem Verdacht auf Kompromittierung?
- Kann die Reaktion auf fehlerhafte Authentisierungsversuche entsprechend der Sicherheitsvorgaben eingerichtet werden?
- Lassen sich die sicherheitskritischen Parameter, wie Authentisierungsanforderungen, entsprechend der Sicherheitsvorgaben konfigurieren?
- Lassen sich auf dem Identitäts- und Berechtigungsmanagement-System differenzierte Rechtestrukturen in zugewiesenen Bereichen für das Verwaltungspersonal einrichten, wie Lesen, Schreiben, Ausführen oder Ändern? Werden die für die Rechteverwaltung relevanten Daten manipulationssicher vom Produkt gespeichert?
- Verfügt das Identitäts- und Berechtigungsmanagement-System über eine angemessene Protokollierung? Ist sichergestellt, dass die Protokollierung von Unberechtigten nicht deaktiviert werden kann? Sind die Protokolle selbst für Unberechtigte weder lesbar noch modifizierbar? Ist die Protokollierung übersichtlich, vollständig und korrekt?
- Verfügt das Identitäts- und Berechtigungsmanagement-System über eine übersichtliche und einfach nutzbare Protokollauswertung?

ORP.4.M18 Einsatz eines zentralen Authentisierungsdienstes (S)

Oft sollen sich die Anwender nicht nur gegenüber einem einzelnen Dienst oder auf einem einzelnen IT-System authentisieren, sondern es sollen für verschiedene Dienste und auf unterschiedlichen Systemen dieselben Authentisierungsdaten genutzt werden können, wie etwa Benutzername und Passwort. In einem

solchen Fall ist ein zentraler, netzbasierter Authentisierungsdienst erforderlich, damit die Authentisierungsdaten nicht auf jedem beteiligten System einzeln verwaltet und aktualisiert werden müssen.

Den Extremfall stellt hier das so genannte Single-Sign-On dar, bei dem eine Authentisierung zentral für alle Dienste eines Informationsverbunds erfolgt. Das hat den Vorteil, dass die Benutzer sich nur einmal anmelden müssen. Die Benutzer benötigen nur jeweils ein Passwort oder Token und müssen sich somit nicht verschiedene Passwörter merken oder mehrere Token aufbewahren. Andererseits wird einem Angreifer damit aber der Zugriff auf alle Dienste des Informationsverbunds ermöglicht, sobald er sich einmal als Benutzer anmelden konnte.

Soll ein zentrales, netzbasiertes Authentisierungssystem eingesetzt werden, so ist eine sorgfältige Planung besonders wichtig, da die Funktion und die Sicherheit eines solchen Systems entscheidende Faktoren für die Sicherheit des gesamten Informationsverbundes sind.

Die zentrale Authentisierung kann durch den Einsatz eines zentralen Authentisierungssystems wie Kerberos erreicht werden. Kerberos bietet den Vorteil, dass es neben Unix-Systemen auch unter Windows-Betriebssystemen funktioniert.

Auf wichtige Empfehlungen, die für die Auswahl und den Einsatz eines netzbasierten Authentisierungsdienstes berücksichtigt werden müssen, wird im Folgenden tiefer eingegangen:

Verschlüsselung der Netz-Protokolle

Im Gegensatz zu einer lokalen Benutzerverwaltung werden kritische Informationen, die für eine netzbasierte Authentisierung benötigt werden, über ein LAN oder WAN übertragen. Daher ist es zwingend erforderlich, dass diese Informationen nicht mitgelesen oder verändert werden können.

Außerdem muss sichergestellt werden, dass ein Angreifer sich nicht anmelden kann, indem er aufgezeichnete Anmeldeinformationen wieder einspielt. Daher müssen die Anmeldeinformationen, die für die Authentisierung zwischen Server und Client ausgetauscht werden, verschlüsselt und zusätzlich dynamisiert werden, beispielsweise mit Challenge-Response-Verfahren.

Schutz des Authentisierungsservers

Generell werden alle für eine Authentisierung benötigten Informationen auf zentrale Server abgelegt. Daher ist sicherzustellen, dass keine unautorisierten Personen an diese kritischen Informationen gelangen können. Ein Authentisierungsserver muss also auf allen Ebenen sorgfältig geschützt werden. Der Schutzbedarf ist vergleichbar mit dem eines Sicherheitsgateways. Folgende Aspekte sollten rund um die Sicherheit des Authentisierungsservers berücksichtigt werden:

- Er sollte nach Möglichkeit räumlich getrennt oder in einem separaten Serverraum aufgestellt werden. Die hierbei zu erfüllenden Anforderungen sind in Baustein INF.2 *Rechenzentrum sowie Serverraum* beschrieben.
- Er darf sich nur innerhalb eines geschützten Netzes befinden.
- Auf einem Authentisierungsserver sollten nur die dafür erforderlichen Dienste verfügbar sein und möglichst keine weiteren Dienste angeboten werden. Außerdem dürfen darauf nur Programme installiert sein, die für die Funktionsfähigkeit des Servers erforderlich sind.
- Für die Konzeption und den Betrieb eines Authentisierungsservers muss geeignetes Personal mit ausreichend Ressourcen vorhanden sein. Der zeitliche Aufwand für den Betrieb eines Authentisierungsservers darf nicht unterschätzt werden. Alleine die Auswertung der anfallenden Protokolldaten beansprucht oft viel Zeit. Die Administratoren müssen fundierte Kenntnisse der eingesetzten IT-Komponenten besitzen und entsprechend geschult werden.
- Nur dafür vorgesehene Administratoren dürfen sich auf diesen Systemen anmelden können. Die Vergabe von Administrationsrechten muss sorgfältig dokumentiert sein. Besonders sicherheitskritische Eingriffe sollten möglichst nach dem Vier-Augen-Prinzip erfolgen. Administratoren sollten für die Anmeldung starke Authentisierungsmethoden nutzen.

- Die Administration des Authentisierungsservers darf nur über einen gesicherten Zugang möglich sein, z. B. über eine gesicherte Konsole, eine verschlüsselte Verbindung oder ein separates Netz (Administrationsnetz).
- Die korrekte Konfiguration eines Authentisierungsservers ist wesentlich für dessen sicheren Betrieb. Fehler in der Konfiguration können zu Sicherheitslücken oder Ausfällen führen. Die Konfiguration muss sorgfältig dokumentiert sein.
- Betriebssystem und Programme eines Authentisierungsservers müssen jederzeit auf einem sicheren Patch-Stand sein.
- Es müssen in regelmäßigen Abständen Integritätstests der eingesetzten Software durchgeführt werden. Im Fehlerfall muss der Authentisierungsserver abgeschaltet werden.
- Es muss klar dokumentiert sein, welche Ereignisse protokolliert werden müssen und wo diese gespeichert werden. Außerdem muss festgehalten werden, wie und in welchen Abständen die Ereignisse ausgewertet werden.
- Authentisierungsserver müssen in das institutionsweite Datensicherungskonzept sowie in das Notfallvorsorgekonzept integriert sein. Dabei sollte die Sicherung auf gesonderte Backup-Medien bzw. -Speicherbereiche erfolgen.Werden gesicherte Datenbestände wieder eingespielt, muss darauf geachtet werden, dass Benutzer- und Rechteverwaltung auf dem aktuellen Stand sind.
- Für einen sicheren Betrieb eines Authentisierungsservers sind die umgesetzten Sicherheitsmaßnahmen regelmäßig auf ihre korrekte Einhaltung zu überprüfen. Durch regelmäßige Audits muss der sichere Betrieb überprüft werden.

Weiterhin ist bei einer zentralen Authentisierung ein Ausfall des Servers oder des Netzes zu berücksichtigen, was z. B. nach einem Denial-of-Service-Angriff der Fall sein kann. Denn wenn alle weiteren IT-Systeme im Netz von dem Server für eine Authentisierung abhängig sind, weitet sich der Denial-of-Service-Angriff auf alle IT-Systeme im Netz aus. Daher wird der Einsatz eines hochverfügbaren Systems empfohlen, etwa mithilfe eines redundanten Servers.

Da eine verlässliche Authentisierung für die Sicherheit jedes Netzes eine zentrale Rolle spielt, ist der sichere und ordnungsgemäße Betrieb des Authentisierungsservers besonders wichtig. Daher muss das gewählte Vorgehen in die bestehende institutionsweite Sicherheitsleitlinie integriert werden.

Passwörter

Analog zur Maßnahme ORP.4.M8 *Regelung des Passwortgebrauchs* sind geeignete Vorkehrungen für eine hohe Passwortgüte zu treffen.

Protokollierung

Das Authentisierungssystem muss die aus dem Baustein OPS.1.1.7 *Protokollierung* bekannten Ereignisse erfassen können.

Wird ein zentraler Protokollierungsserver eingesetzt, sollte gewährleistet werden, dass die übertragenen Daten nicht abgehört werden können. Das kann beispielsweise durch verschlüsselte Anwendungsprotokolle, VPN-Verbindungen oder durch ein separates Datennetz zwischen dem zentralen Authentisierungsserver und dem Protokollierungsserver ermöglicht werden.

ORP.4.M19 Einweisung aller Mitarbeiter in den Umgang mit Authentisierungsverfahren und -mechanismen (S)

Alle Mitarbeiter sind in den sicheren Umgang mit den in der Institution eingesetzten Authentisierungsverfahren und -mechanismen einzuweisen. Außerdem müssen alle Mitarbeiter über die Richtlinien und Anweisungen zum Umgang mit Authentisierungsverfahren und -mechanismen informiert werden (siehe beispielsweise ORP.4.M8 *Regelung des Passwortgebrauchs*). Besonders wichtig ist dabei, die Mitarbeiter darüber zu unterrichten, warum die Richtlinien notwendig und angemessen sind. So sind sie motiviert, die Vorgaben auch einzuhalten. Die Richtlinien müssen für die Mitarbeiter verständlich sein und

dürfen nur Regelungen enthalten, die auch umgesetzt werden können. Sie sollten zudem so positiv wie möglich formuliert werden.

Die Einweisung sollte mindestens folgende Punkte umfassen:

- Grundlagen von Identifizierung und Authentisierung: Erläuterungen von Begriffsdefinitionen wie Wissen, Besitz und Eigenschaft,
- Hinweise zur Handhabung der eingesetzten Authentisierungsverfahren und -mechanismen (z. B. Aufbewahrung von Authentisierungstoken),
- Vorgaben zur Auswahl und Nutzung von Passwörtern (siehe ORP.4.M8 *Regelung des Passwortgebrauchs*),
- Umgang mit Berechtigungen: Überblick über das Berechtigungskonzept der Institution, Gestaltung der Rechtevergabe,
- Übersicht über Sicherheitsfunktionen des eingesetzten Produktes zum Identitäts- und Berechtigungsmanagement,
- Beschreibung, wie der Prozess (Wieder-)Freigabe bei Sperrung von Benutzerkennungen funktioniert,
- Überblick über die verschiedenen Aufgaben und Rollen bei der Verwaltung von Identitäten, Benutzerkennungen und Berechtigungen sowie
- Benennung von Ansprechpartnern.

ORP.4.M20 Notfallvorsorge für das Identitäts- und Berechtigungsmanagement-System (H)

Fällt das Identitäts- und Berechtigungsmanagement-System aus, können Benutzerprofile nicht mehr geändert, neu angelegt oder gelöscht werden. Es ist zu prüfen, inwieweit sich das sicherheitskritisch auf die Geschäftsprozesse auswirkt. Auch ist zu untersuchen, wie sich ein Angriff mit Rechten auswirkt, die aufgrund des Ausfalls des Identitäts- und Berechtigungsmanagement-Systems nicht gelöscht werden konnten.

Es müssen regelmäßige und umfassende Datensicherungen erfolgen, damit alle im Identitäts- und Berechtigungsmanagement-System gespeicherten Daten auch bei Störungen, Ausfällen der Hardware oder Veränderungen wieder verfügbar gemacht werden können. Die notwendigen Maßnahmen sind im Baustein CON.3 *Datensicherungskonzept* beschrieben.

Wird ein zentrales Werkzeug zum Identitäts- und Berechtigungsmanagement eingesetzt, so ist dessen ordnungsmäßiger Betrieb essenziell, um alle damit verknüpften Prozesse und Anwendungen aufrechtzuerhalten. Bei der Notfallvorsorge ist daher zu hinterfragen, wie sich ein Ausfall der Werkzeuge auswirkt und wie diese im Notfall möglichst schnell wieder betriebsfähig gemacht werden können (siehe Baustein DER.4 N*otfallmanagement*).

In Notfallsituationen kann es erforderlich sein, dass Spezialisten, z. B. vom Krisenstab, kurzfristig weitreichende Berechtigungen benötigen, um den Notfall zu beheben und damit den Betriebszustand wiederherzustellen. Der Prozess für die Vergabe, Dokumentation und den Entzug muss im Notfallkonzept beschrieben werden. Im Notfallkonzept sollte außerdem überprüft werden, ob die für Notfälle vorgesehenen Berechtigungskonzepte auch noch anwendbar sind, wenn das Identitäts- und Berechtigungsmanagement-System ebenfalls ausgefallen ist.

ORP.4.M21 Mehr-Faktor-Authentisierung (H)

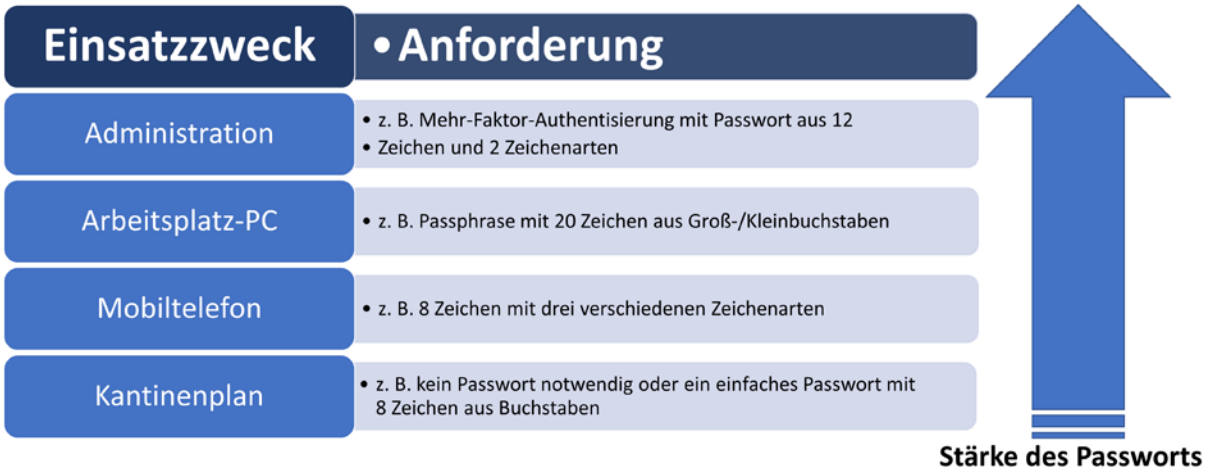
Bei höherem Schutzbedarf sollte eine sichere Mehr-Faktor-Authentisierung, z. B. mit kryptographischen Zertifikaten, Chipkarten oder Token, zur Authentisierung verwendet werden.

ORP.4.M22 Regelung zur Passwortqualität (B)

Werden in einem IT-System oder einer Anwendung Passwörter zur Authentisierung verwendet, so ist dafür zu sorgen, dass sichere Passwörter genutzt werden. Die Vorgaben für Passwörter müssen so gestaltet sein, dass sie einen praktikablen Kompromiss zwischen Komplexität und mit vertretbarem Aufwand nutzbar darstellen. Die Anzahl der möglichen Passwörter eines Authentisierungsverfahrens muss dabei so groß sein, dass ein Passwort nicht in kurzer Zeit durch einfaches Ausprobieren ermittelt werden kann.

Folgende Regeln zu Passwortgestaltung und -gebrauch müssen deshalb beachtet werden:

- Ein Passwort darf nicht leicht zu erraten sein, daher darf es keine Informationen aus dem persönlichen oder beruflichen Umfeld des Benutzers enthalten wie z. B. Namen, Kfz-Kennzeichen oder das Geburtsdatum.
- Passwörter dürfen nicht mehrfach verwendet werden, sondern für jedes IT-System bzw. jede Anwendung muss ein eigenständiges Passwort verwendet werden.
- Bei einem guten Passwort sind die Länge und die Anzahl der verwendeten Zeichenarten wie Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen in sinnvoller Kombination und in Abhängigkeit des verwendeten Verfahrens zu wählen:
    - z. B. 20 – 25 Zeichen Länge und zwei genutzte Zeichenarten (weniger komplex, längeres Passwort beziehungsweise Passphrase),
    - z. B. 8 – 12 Zeichen Länge und vier genutzte Zeichenarten (komplexer, geringere Länge des Passworts),
    - z. B. bei Mehr-Faktor-Authentisierung 8 Zeichen Länge und drei genutzte Zeichenarten.
- Der Einsatzzweck von Passwörtern beeinflusst die Anforderungen an die Sicherheit von Passwörtern, siehe folgende Abbildung:



- Passwörter, die im Rahmen von Mehr-Faktor-Authentisierung eingesetzt werden, können eine geringere Komplexität haben, als wenn sie alleiniger Sicherheitsfaktor sind.
- Die Sicherheit hängt bei Verwendung eines zweiten Faktors nicht allein vom Passwort ab, sondern auch vom zweiten Faktor. Um die Gesamtsicherheit bestehend aus Passwort und zweitem Faktor zu gewährleisten, muss auch mit dem zweiten Faktor entsprechend sorgsam umgegangen werden. Hardware-Token dürfen z. B. nicht unbeaufsichtigt bleiben.

ORP.4.M23 Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme (B)

Passwort-verarbeitende Anwendungen und IT-Systeme müssen, falls technisch möglich, folgende Randbedingungen einhalten:

- Die Wahl von Trivialpasswörtern und gängigen Zeichenketten, z. B. "123456“, "password", Namen, Geburtsdaten sowie Tastaturmustern wie "asdf“, muss vermieden werden. Dies kann z. B. verhindert werden, indem Passwörter bei Eingabe gegen Listen von Trivialpasswörtern bzw. Listen von öffentlich bekannt gewordenen Passwörtern geprüft werden.
- Jeder Benutzer muss sein eigenes Passwort ändern können.
- Nach einem Passwortwechsel darf das Passwort für einen bestimmten Zeitraum, z. B. einen Tag, nicht geändert werden können.

- Die Benutzer sollten bei der Änderung eines Passwortes durch Hinweise zur Passwort-Güte unterstützt werden, die diese Anforderungen beachten.
- Es sollte nur Software eingesetzt werden, die die gesamte Benutzereingabe für das Passwort auch tatsächlich verwendet. Sollte es eine maximale Anzahl an Zeichen geben, sollte dieser Umstand dem Benutzer bewusst gemacht werden.
- IT-Systeme oder Anwendungen sollten Anwender nur mit einem validen Grund auffordern, das Passwort zu wechseln, reine zeitgesteuerte Wechsel werden nicht empfohlen.
- Es müssen Maßnahmen ergriffen werden, um die Kompromittierung von Passwörtern zu erkennen, z. B. parallele Anmeldungen von verschiedenen Systemen oder Standorten, Häufung von Fehleingaben und so weiter. So kann bspw. über Protokollierung und die entsprechende Auswertung der Log-Files herausgefunden werden, ob es ungewöhnliche Zugriffe oder Hackingversuche gegeben hat. Hierzu gibt es bei Datenbanken, Betriebssystemen, Webservern und anderen Anwendungen z. B. auch spezielle Sicherheitsprodukte. Wenn keine ausreichenden Maßnahmen zum Erkennen von Kompromittierung von Passwörtern möglich sind, so ist zu überlegen, ob die Nachteile eines zeitgesteuerten Passwortwechsels in diesem Fall in Kauf genommen werden können und Passwörter in gewissen Abständen, z. B. alle 6 Monate, gewechselt werden sollen.
- Passwörter für Dienste oder technische Benutzer, die meist in Konfigurationsdateien auf einem System hinterlegt sind, müssen so sicher wie möglich gespeichert werden. Konfigurationsdateien können z. B. über Zugriffsrechte abgesichert werden. Für die Erstanmeldung neuer Benutzer sollten Initial-Passwörter vergeben werden, die nach einmaligem Gebrauch gewechselt werden müssen. Für die Erstanmeldung muss für jeden neuen Benutzer ein individuelles Passwort verwendet und dieses nach dem einmaligen Gebrauch geändert werden. Das Passwort zur Erstanmeldung ist vertraulich zu übermitteln, z. B. in einem versiegelten Briefumschlag.
- Erfolglose Anmeldeversuche sollten mit einer kurzen Fehlermeldung ohne Angabe von näheren Einzelheiten abgelehnt werden. Insbesondere darf bei erfolglosen Anmeldeversuchen nicht erkennbar sein, ob der eingegebene Benutzername oder das eingegebene Passwort falsch ist. Nach mehreren aufeinander folgenden fehlerhaften Passworteingaben sollte das Authentisierungssystem eine erneute Passworteingabe von dem für die Fehleingaben verantwortlichen System für eine bestimmte Zeitspanne verzögern. Die Sperrung von Kennungen nach mehreren fehlgeschlagenen Authentisierungsversuchen sollte nur in Ausnahmefällen gewählt werden. Stattdessen ist es empfehlenswert, weitere Authentisierungsversuche zeitlich zu verzögern und erst nach mehrmaligen Fehlversuchen die Kennung zu sperren.
- Bei der Authentisierung in vernetzten Systemen sollten Passwörter selbst in einem Intranet nicht unverschlüsselt übertragen werden. Erfolgt die Authentisierung über ein ungesichertes Netz hinweg, so dürfen Passwörter keinesfalls unverschlüsselt übertragen werden.
- Bei der Eingabe sollte das Passwort nicht auf dem Bildschirm angezeigt werden. Bei kleinen IT-Systemen wie Smartphones kann es aber sinnvoll sein, kurz das letzte eingegebene Zeichen im Klartext anzuzeigen.
- Die Passwörter dürfen im IT-System nicht im Klartext gespeichert werden, sie sollten z. B. mittels sicherer Einweg-Funktion (Hashfunktionen mit Salt und ggf. Pepper) geschützt werden.
- Die Wiederholung alter Passwörter beim Passwortwechsel muss vom IT-System verhindert werden (Passwort-Historie).

3. Weiterführende Informationen

3.1 Wissenswertes

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

3.2 Quellenverweise

Für den Umsetzungshinweis ORP.4 *Identitäts- und Berechtigungsmanagement* sind keine Quellenverweise vorhanden.