Bundesamt
für Sicherheit in der
Informationstechnik

ORP: Organisation und Personal

ORP.4: Identitäts- und Berechtigungsmanagement

1 Beschreibung

1.1 Einleitung

Der Zugang zu schützenswerten Ressourcen einer Institution ist auf berechtigte Benutzer und berechtigte IT-Komponenten einzuschränken. Benutzer und IT-Komponenten 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, ihnen also basierend auf dem Benutzerprofil Zutritt, Zugang oder Zugriff zu gewähren oder zu verweigern ist. Berechtigungsmanagement bezeichnet die Prozesse, die für Zuweisung, Entzug und Kontrolle der Rechte erforderlich sind.

Die Übergänge zwischen den beiden Begriffen sind fließend, daher wird in diesem Baustein der Begriff Identitäts- und Berechtigungsmanagement (englisch Identity and Access Management, IAM) benutzt. Zur besseren Verständlichkeit wird in diesem Baustein der Begriff „Benutzerkennung“ bzw. „Kennung“ synonym für „Benutzerkonto“, „Login“ und „Account“ verwendet. In diesem Baustein wird der Begriff „Passwort“ als allgemeine Bezeichnung für „Passphrase“, „PIN“ oder „Kennwort“ verwendet.

1.2 Zielsetzung

Ziel des Bausteins ist es, dass Benutzer oder auch IT-Komponenten ausschließlich auf die IT-Ressourcen und Informationen zugreifen können, die sie für ihre Arbeit benötigen und für die sie autorisiert sind, und unautorisierten Benutzern oder IT-Komponenten den Zugriff zu verwehren. Dazu werden Anforderungen formuliert, mit denen Institutionen ein sicheres Identitäts- und Berechtigungsmanagement aufbauen sollten.

1.3 Abgrenzung und Modellierung

Der Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* ist für den Informationsverbund einmal anzuwenden.

In diesem Baustein werden grundsätzliche Anforderungen für den Aufbau eines Identitäts- und Berechtigungsmanagements beschrieben.

Anforderungen, die Komponenten eines Identitäts- und Berechtigungsmanagement betreffen, wie

Betriebssysteme oder Verzeichnisdienste, sind in den entsprechenden Bausteinen zu finden (z. B. SYS.1.3 *Server unter Linux und Unix*, SYS.1.2.2 *Windows Server 2012*, APP.2.1 *Allgemeiner Verzeichnisdienst*, APP.2.2 *Active Directory*).

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* von besonderer Bedeutung:

2.1 Fehlende oder unzureichende Prozesse beim Identitäts- und Berechtigungsmanagement

Sind Prozesse beim Identitäts- und Berechtigungsmanagement unzureichend definiert oder implementiert, ist nicht gewährleistet, dass Zugriffe auf das erforderliche Maß eingeschränkt sind und so gegen die Prinzipien Need-to-Know bzw. Least-Privilege verstoßen wird. Der Administrator erhält möglicherweise keine Informationen über personelle Veränderungen, so dass beispielsweise eine Benutzerkennung eines ausgeschiedenen Mitarbeiters nicht gelöscht wird. Dieser kann somit weiterhin auf schützenswerte Informationen zugreifen.

Auch ist es möglich, dass Mitarbeiter, die in eine neue Abteilung versetzt wurden, ihre alten Berechtigungen behalten und dadurch mit der Zeit umfangreiche Gesamtberechtigungen ansammeln.

2.2 Fehlende zentrale Deaktivierungsmöglichkeit von Benutzerzugängen

In Institutionen haben Mitarbeiter oft Benutzerzugänge zu diversen IT-Systemen, wie Produktiv-, Test-, Qualitätssicherungs- oder Projekt-Systeme. Diese befinden sich meist in unterschiedlichen Zuständigkeitsbereichen und werden oft von unterschiedlichen Administratoren verwaltet. Das führt unter Umständen dazu, dass nicht auf allen IT-Systemen eine gleiche und eindeutige Benutzerkennung verwendet wird und es auch keine zentrale Übersicht über die Benutzerzugänge auf den einzelnen IT-Systemen gibt. In einem solchen Szenario ist es nicht möglich, bei einem Angriff oder einem Passwortdiebstahl in einem Arbeitsschritt alle Benutzerzugänge eines Mitarbeiters zu deaktivieren. Auch können in diesem Szenario bei dem Ausscheiden eines Mitarbeiters aus der Institution nicht in einem Arbeitsschritt alle Zugänge gesperrt werden.

2.3 Ungeeignete Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten

Wenn die Vergabe von Zutritts-, Zugangs- und Zugriffsrechten schlecht geregelt ist, führt das schnell zu gravierenden Sicherheitslücken, z. B. durch Wildwuchs in der Rechtevergabe. Bei der Einführung von Identitätsmanagement-Systemen oder Revisionen stellt sich häufig heraus, dass verschiedene Personen in unterschiedlichsten Organisationseinheiten für die Vergabe von Berechtigungen zuständig sind. Dies führt unter Umständen dazu, dass Benutzer Berechtigungen auf Zuruf erhalten oder umgekehrt nur über unnötig komplizierte Wege an diese kommen. Dadurch können einerseits fehlende Berechtigungen die tägliche Arbeit behindern, andererseits können so Berechtigungen ohne Erfordernis vergeben werden und so ein Sicherheitsrisiko darstellen.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins ORP.4 *Identitäts- und Berechtigungsmanagement* aufgeführt. Grundsätzlich ist der Informationssicherheitsbeauftragte (ISB) dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Informationssicherheitsbeauftragter (ISB)
Weitere Zuständigkeiten	Benutzer, IT-Betrieb

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* vorrangig erfüllt werden:

ORP.4.A1 Regelung für die Einrichtung und Löschung von Benutzern und Benutzergruppen [IT-Betrieb] (B)

Es MUSS geregelt werden, wie Benutzerkennungen und Benutzergruppen einzurichten und zu löschen sind. Jede Benutzerkennung MUSS eindeutig einem Benutzer zugeordnet werden können. Benutzerkennungen, die längere Zeit inaktiv sind, SOLLTEN deaktiviert werden. Alle Benutzer und Benutzergruppen DÜRFEN NUR über separate administrative Rollen eingerichtet und gelöscht werden. Nicht benötigte Benutzerkenngen, wie z.B. standardmäßig eingerichtete Gastkonten oder Standard-Administratorkennungen, MÜSSEN geeignet deaktiviert oder gelöscht werden.

ORP.4.A2 Einrichtung, Änderung und Entzug von Berechtigungen [IT-Betrieb] (B)

Benutzerkennungen und Berechtigungen DÜRFEN NUR aufgrund des tatsächlichen Bedarfs und der Notwendigkeit zur Aufgabenerfüllung vergeben werden (Prinzip der geringsten Berechtigungen, engl. Least Privileges und Erforderlichkeitsprinzip, engl. Need-to-know). Bei personellen Veränderungen MÜSSEN die nicht mehr benötigten Benutzerkennungen und Berechtigungen entfernt werden. Beantragen Mitarbeiter Berechtigungen, die über den Standard hinausgehen, DÜRFEN diese NUR nach zusätzlicher Begründung und Prüfung vergeben werden. Zugriffsberechtigungen auf Systemverzeichnisse und -dateien SOLLTEN restriktiv eingeschränkt werden. Alle Berechtigungen MÜSSEN über separate administrative Rollen eingerichtet werden.

ORP.4.A3 Dokumentation der Benutzerkennungen und Rechteprofile [IT-Betrieb] (B)

Es MUSS dokumentiert werden, welche Benutzerkennungen, angelegte Benutzergruppen und Rechteprofile zugelassen und angelegt wurden. Die Dokumentation der zugelassenen Benutzer, angelegten Benutzergruppen und Rechteprofile MUSS regelmäßig 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. Die Dokumentation MUSS vor unberechtigtem Zugriff geschützt werden. Sofern sie in elektronischer Form erfolgt, SOLLTE sie in das Datensicherungsverfahren einbezogen werden.

ORP.4.A4 Aufgabenverteilung und Funktionstrennung [IT-Betrieb] (B)

Die von der Institution definierten unvereinbaren Aufgaben und Funktionen (siehe Baustein ORP.1 *Organisation)* MÜSSEN durch das Identitäts- und Berechtigungsmanagement getrennt werden.

ORP.4.A5 Vergabe von Zutrittsberechtigungen [IT-Betrieb] (B)

Es MUSS festgelegt werden, welche Zutrittsberechtigungen an welche Personen im Rahmen ihrer Funktion vergeben bzw. ihnen entzogen werden. Die Ausgabe bzw. der Entzug von verwendeten Zutrittsmittel wie Chipkarten MUSS dokumentiert werden. Wenn Zutrittsmittel kompromittiert wurden, MÜSSEN sie ausgewechselt werden. Die Zutrittsberechtigten SOLLTEN für den korrekten Umgang mit den Zutrittsmitteln geschult werden. Bei längeren Abwesenheiten SOLLTEN berechtigte Personen vorübergehend gesperrt werden.

ORP.4.A6 Vergabe von Zugangsberechtigungen [IT-Betrieb] (B)

Es MUSS festgelegt werden, welche Zugangsberechtigungen an welche Personen im Rahmen ihrer

Funktion vergeben bzw. ihnen entzogen werden. Werden Zugangsmittel wie Chipkarten verwendet, so MUSS die Ausgabe bzw. der Entzug dokumentiert werden. Wenn Zugangsmittel kompromittiert wurden, MÜSSEN sie ausgewechselt werden. Die Zugangsberechtigten SOLLTEN für den korrekten Umgang mit den Zugangsmitteln geschult werden. Bei längeren Abwesenheiten SOLLTEN berechtigte Personen vorübergehend gesperrt werden.

ORP.4.A7 Vergabe von Zugriffsrechten [IT-Betrieb] (B)

Es MUSS festgelegt werden, welche Zugriffsrechte an welche Personen im Rahmen ihrer Funktion vergeben bzw. ihnen entzogen werden. Werden im Rahmen der Zugriffskontrolle Chipkarten oder Token verwendet, so MUSS die Ausgabe bzw. der Entzug dokumentiert werden. Die Anwender SOLLTEN für den korrekten Umgang mit Chipkarten oder Token geschult werden. Bei längeren Abwesenheiten SOLLTEN berechtigte Personen vorübergehend gesperrt werden.

ORP.4.A8 Regelung des Passwortgebrauchs [Benutzer, IT-Betrieb] (B)

Die Institution MUSS den Passwortgebrauch verbindlich regeln (siehe auch ORP.4.A22 *Regelung zur Passwortqualität* und *ORP.4.A23 Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme*). Dabei MUSS geprüft werden, ob Passwörter als alleiniges Authentisierungsverfahren eingesetzt werden sollen, oder ob andere Authentisierungsmerkmale bzw. -verfahren zusätzlich zu oder anstelle von Passwörtern verwendet werden können.

Passwörter DÜRFEN NICHT mehrfach verwendet werden. Für jedes IT-System bzw. jede Anwendung MUSS ein eigenständiges Passwort verwendet werden. Passwörter, die leicht zu erraten sind oder in gängigen Passwortlisten geführt werden, DÜRFEN NICHT verwendet werden. Passwörter MÜSSEN geheim gehalten werden. Sie DÜRFEN NUR dem Benutzer persönlich bekannt sein. Passwörter DÜRFEN NUR unbeobachtet eingegeben werden. Passwörter DÜRFEN NICHT auf programmierbaren Funktionstasten von Tastaturen oder Mäusen gespeichert werden. Ein Passwort DARF NUR für eine Hinterlegung für einen Notfall schriftlich fixiert werden. Es MUSS dann sicher aufbewahrt werden. Die Nutzung eines Passwort-Managers SOLLTE geprüft werden. 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. Ein Passwort MUSS gewechselt werden, wenn es unautorisierten Personen bekannt geworden ist oder der Verdacht dazu besteht.

ORP.4.A9 Identifikation und Authentisierung [IT-Betrieb] (B)

Der Zugriff auf alle IT-Systeme und Dienste MUSS durch eine angemessene Identifikation und Authentisierung der zugreifenden Benutzer, Dienste oder IT-Systeme abgesichert sein. Vorkonfigurierte Authentisierungsmittel MÜSSEN vor dem produktiven Einsatz geändert werden.

ORP.4.A22 Regelung zur Passwortqualität [IT-Betrieb] (B)

In Abhängigkeit von Einsatzzweck und Schutzbedarf MÜSSEN sichere Passwörter geeigneter Qualität gewählt werden. Das Passwort MUSS so komplex sein, dass es nicht leicht zu erraten ist. Das Passwort DARF NICHT zu kompliziert sein, damit der Benutzer in der Lage ist, das Passwort mit vertretbarem Aufwand regelmäßig zu verwenden.

ORP.4.A23 Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme [IT-Betrieb] (B)

IT-Systeme oder Anwendungen SOLLTEN NUR mit einem validen Grund zum Wechsel des Passworts auffordern. Reine zeitgesteuerte Wechsel SOLLTEN vermieden werden. Es MÜSSEN Maßnahmen ergriffen werden, um die Kompromittierung von Passwörtern zu erkennen. Ist dies nicht möglich, so SOLLTE geprüft werden, ob die Nachteile eines zeitgesteuerten Passwortwechsels in Kauf genommen werden können und Passwörter in gewissen Abständen gewechselt werden.

Standardpasswörter MÜSSEN durch ausreichend starke Passwörter ersetzt und vordefinierte Kennungen MÜSSEN geändert werden. Es SOLLTE sichergestellt werden, dass die mögliche Passwortlänge auch im vollen Umfang von verarbeitenden IT-Systemen geprüft wird. Nach einem

Passwortwechsel DÜRFEN alte Passwörter NICHT mehr genutzt werden. Passwörter MÜSSEN so sicher wie möglich gespeichert werden. Bei Kennungen für technische Benutzer, Dienstkonten, Schnittstellen oder Vergleichbares SOLLTE ein Passwortwechsel sorgfältig geplant und gegebenenfalls mit den Anwendungsverantwortlichen abgestimmt werden.

Bei der Authentisierung in vernetzten Systemen DÜRFEN Passwörter NICHT unverschlüsselt über unsichere Netze übertragen werden. Wenn Passwörter in einem Intranet übertragen werden, SOLLTEN sie verschlüsselt werden. Bei erfolglosen Anmeldeversuchen SOLLTE das System keinen Hinweis darauf geben, ob Passwort oder Benutzerkennung falsch sind.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein ORP.4 *Identitäts- und Berechtigungsmanagement*. Sie SOLLTEN grundsätzlich erfüllt werden.

ORP.4.A10 Schutz von Benutzerkennungen mit weitreichenden Berechtigungen [IT-Betrieb] (S)

Benutzerkennungen mit weitreichenden Berechtigungen SOLLTEN mit einer Mehr-Faktor-Authentisierung, z. B. mit kryptografischen Zertifikaten, Chipkarten oder Token, geschützt werden.

ORP.4.A11 Zurücksetzen von Passwörtern [IT-Betrieb] (S)

Für das Zurücksetzen von Passwörtern SOLLTE ein angemessenes sicheres Verfahren definiert und umgesetzt werden. Die Support-Mitarbeiter, die Passwörter zurücksetzen können, SOLLTEN entsprechend geschult werden. Bei höherem Schutzbedarf des Passwortes SOLLTE eine Strategie definiert werden, falls ein Support-Mitarbeiter aufgrund fehlender sicherer Möglichkeiten der Übermittlung des Passwortes die Verantwortung nicht übernehmen kann.

ORP.4.A12 Entwicklung eines Authentisierungskonzeptes für IT-Systeme und Anwendungen [IT-Betrieb] (S)

Es SOLLTE ein Authentisierungskonzept erstellt werden. Darin SOLLTE für jedes IT-System und jede Anwendung definiert werden, welche Funktions- und Sicherheitsanforderungen an die Authentisierung gestellt werden. Authentisierungsinformationen MÜSSEN kryptografisch sicher gespeichert werden. Authentisierungsinformationen DÜRFEN NICHT unverschlüsselt über unsichere Netze übertragen werden.

ORP.4.A13 Geeignete Auswahl von Authentisierungsmechanismen [IT-Betrieb] (S)

Es SOLLTEN dem Schutzbedarf angemessene Identifikations- und Authentisierungsmechanismen verwendet werden. Authentisierungsdaten SOLLTEN durch das IT-System bzw. die IT-Anwendungen bei der Verarbeitung jederzeit gegen Ausspähung, Veränderung und Zerstörung geschützt werden. 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. Nach Überschreitung der vorgegebenen Anzahl erfolgloser Authentisierungsversuche SOLLTE das IT-System bzw. die IT-Anwendung die Benutzerkennung sperren.

ORP.4.A14 Kontrolle der Wirksamkeit der Benutzertrennung am IT-System bzw. an der Anwendung [IT-Betrieb] (S)

In angemessenen Zeitabständen SOLLTE überprüft werden, ob die Benutzer von IT-Systemen bzw. Anwendungen sich regelmäßig nach Aufgabenerfüllung abmelden. Ebenso SOLLTE kontrolliert werden, dass nicht mehrere Benutzer unter der gleichen Kennung arbeiten.

ORP.4.A15 Vorgehensweise und Konzeption der Prozesse beim Identitäts- und Berechtigungsmanagement [IT-Betrieb] (S)

Für das Identitäts- und Berechtigungsmanagement SOLLTEN folgenden Prozesse definiert und umgesetzt werden:

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

ORP.4.A16 Richtlinien für die Zugriffs- und Zugangskontrolle [IT-Betrieb] (S)

Es SOLLTE eine Richtlinie für die Zugriffs- und Zugangskontrolle von IT-Systemen, IT-Komponenten und Datennetzen erstellt werden. Es SOLLTEN Standard-Rechteprofile benutzt werden, die den Funktionen und Aufgaben der Mitarbeiter entsprechen. Für jedes IT-System und jede IT-Anwendung SOLLTE eine schriftliche Zugriffsregelung existieren.

ORP.4.A17 Geeignete Auswahl von Identitäts- und Berechtigungsmanagement-Systemen [IT-Betrieb] (S)

Beim Einsatz eines Identitäts- und Berechtigungsmanagement-Systems SOLLTE dieses für die Institution und deren jeweilige Geschäftsprozesse, Organisationsstrukturen und Abläufe sowie deren Schutzbedarf geeignet sein. Das Identitäts- und Berechtigungsmanagement-System SOLLTE die in der Institution vorhandenen Vorgaben zum Umgang mit Identitäten und Berechtigungen abbilden können. Das ausgewählte Identitäts- und Berechtigungsmanagement-System SOLLTE den Grundsatz der Funktionstrennung unterstützen. Das Identitäts- und Berechtigungsmanagement-System SOLLTE angemessen vor Angriffen geschützt werden.

ORP.4.A18 Einsatz eines zentralen Authentisierungsdienstes [IT-Betrieb] (S)

Um ein zentrales Identitäts- und Berechtigungsmanagement aufzubauen, SOLLTE ein zentraler netzbasierter Authentisierungsdienst eingesetzt werden. Der Einsatz eines zentralen netzbasierten Authentisierungsdienstes SOLLTE sorgfältig geplant werden. Dazu SOLLTEN die Sicherheitsanforderungen dokumentiert werden, die für die Auswahl eines solchen Dienstes relevant sind.

ORP.4.A19 Einweisung aller Mitarbeiter in den Umgang mit Authentisierungsverfahren und -mechanismen [Benutzer, IT-Betrieb] (S)

Alle Mitarbeiter SOLLTEN in den korrekten Umgang mit dem Authentisierungsverfahren eingewiesen werden. Es SOLLTE verständliche Richtlinien für den Umgang mit Authentisierungsverfahren geben. Die Mitarbeiter SOLLTEN über relevante Regelungen informiert werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

ORP.4.A20 Notfallvorsorge für das Identitäts- und Berechtigungsmanagement-System [IT-Betrieb] (H)

Es SOLLTE geprüft werden, inwieweit ein ausgefallenes Identitäts- und Berechtigungsmanagement-System sicherheitskritisch für die Geschäftsprozesse ist. Es SOLLTEN Vorkehrungen getroffen werden, um bei einem ausgefallenen Identitäts- und Berechtigungsmanagement-System weiterhin arbeitsfähig zu sein. Insbesondere SOLLTE das im Notfallkonzept vorgesehene Berechtigungskonzept weiterhin anwendbar sein, wenn das Identitäts- und Berechtigungsmanagement-System ausgefallen ist.

ORP.4.A21 Mehr-Faktor-Authentisierung [IT-Betrieb] (H)

Es SOLLTE eine sichere Mehr-Faktor-Authentisierung, z. B. mit kryptografischen Zertifikaten, Chipkarten oder Token, zur Authentisierung verwendet werden.

ORP.4.A24 Vier-Augen-Prinzip für administrative Tätigkeiten [IT-Betrieb] (H)
Administrative Tätigkeiten SOLLTEN nur durch zwei Personen durchgeführt werden können. Dazu SOLLTEN bei Mehr-Faktor-Authentisierung die Faktoren auf die zwei Personen verteilt werden. Bei der Nutzung von Passwörtern SOLLTEN diese in zwei Teile zerlegt werden und jede der zwei Personen enthält einen Teil.

4 Weiterführende Informationen

4.1 Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 „Information technology-Security techniques-Information security management systems-Requirements“ im Anhang A.9 Zugangssteuerung Vorgaben für die Identitäts- und Berechtigungsmanagement.

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 29146:2016 “Information technology - Security techniques - A framework for access management“ Vorgaben für die Identitäts- und Berechtigungsmanagement.

Das Infomation Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ im Kapitel TS1.4 Identity and Access Management Vorgaben für die Identitäts- und Berechtigungsmanagement.

Das National Institute of Standards and Technology (NIST) gibt in der NIST Special Publication 800-53A, insbesondere Bereiche AC und IA, Hinweise für Identitäts- und Berechtigungsmanagement.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die Kreuzreferenztabelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tabelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.36 Identitätsdiebstahl

G 0.37 Abstreiten von Handlungen

G 0.44 Unbefugtes Eindringen in Räumlichkeiten

G 0.46 Integritätsverlust schützenswerter Informationen