Identitäts- und Berechtigungsmanagement

1 Beschreibung

1.1 Einleitung

Der Zugang zu schützenswerten Ressourcen eines Unternehmens 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 und durch den Datenschutzbeauftragten Michael Klein datenschutzrechtlich angewendet.

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 Unternehmen und Institutionen ein sicheres Identitäts- und Berechtigungsmanagement aufbauen sollten.

1.3 Abgrenzung und Modellierung

Der Baustein P.4 *Identitäts- und Berechtigungsmanagement* ist für den gesamtenInformationsverbund 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 P.4 *Identitäts- und Berechtigungsmanagement* von besonderer Bedeutung:

2.1 Fehlende oder unzureichende Prozesse beim Identitäts- und Berechtigungsmanagement

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

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

2.2 zentrale Aktivierungsmöglichkeit von Benutzerzugängen

In dem Unternehmen Ingenieurbüro Klein haben Mitarbeiter oft Benutzerzugänge zu diversen IT-Systemen, wie Produktiv-, Test-,Qualitätssicherungs- oder Projekt-Systeme. Diese befinden sich meist in unterschiedlichen Verantwortungsbereichen und werden oft von unterschiedlichen Administratoren verwaltet. Das führt unter Umständen dazu, dass nicht auf allen IT-Systemen eine gleiche und eindeutige Benutzerkennungverwendet 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 aktivieren.
Auch können in diesem Szenario bei dem Ausscheiden eines Mitarbeiters aus dem Unternehmen 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 P.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.

Weitere Zuständigkeiten	Benutzer, IT-Unternehmen

3.1 Basis-Anforderungen

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

P.4.A1 Regelung für die Einrichtung und Löschung von Benutzern und Benutzergruppen [IT-Betrieb]

Es MUSS geregelt werden, wie Benutzerkennungen und Benutzergruppen einzurichten und zu löschen sind. Alle Benutzer und Benutzergruppen DÜRFEN NUR über separate administrative Rollen eingerichtet und gelöscht werden.

P.4.A2 Regelung für Einrichtung, Änderung und Entzug von Berechtigungen [IT-Betrieb]

Benutzerkennungen und Berechtigungen DÜRFEN NUR aufgrund des tatsächlichen Bedarfs vergeben werden. 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 vergeben werden. Alle Berechtigungen MÜSSEN über separate administrative Rollen eingerichtet werden.

P.4.A3 Dokumentation der Benutzerkennungen und Rechteprofile [IT-Unternehmen]

(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 auf Aktualität überprüft werden. Die Dokumentation MUSS vor unberechtigtem Zugriff geschützt werden. Sofern sie in elektronischer Form erfolgt, SOLLTE sie in das Datensicherungsverfahren einbezogen werden.

P.4.A4 Aufgabenverteilung und Funktionstrennung [IT-Unternehmen]

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

P.4.A5 Vergabe von Zutrittsberechtigungen [IT-Unternehmen]

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 auf den korrekten Umgang mit den Zutrittsmitteln geschult werden. Bei längeren Abwesenheiten SOLLTEN berechtigte Personen vorübergehend gesperrt werden.

P.4.A6 Vergabe von Zugangsberechtigungen [IT-Unternehmen]

Es MUSS festgelegt werden, welche Zugangsberechtigungen an welche Personen im Rahmen ihrer Funktion vergeben bzw. ihnen entzogen werden. Werden Zugangsmittel wie Karten verwendet, so MUSS die Ausgabe bzw. der Entzug dokumentiert werden. Wenn Zugangsmittel kompromittiert wurden, MÜSSEN sie ausgewechselt werden. Die Zugangsberechtigten SOLLTEN auf den korrekten Umgang mit den Zugangsmitteln geschult werden. Bei längeren Abwesenheiten SOLLTEN berechtigte Personen vorübergehend gesperrt werden.

P.4.A7 Vergabe von Zugriffsrechten [IT-Unternehmen]

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

P.4.A8 Regelung des Passwortgebrauchs [Benutzer, IT-Unternehmen]

Die Unternehmen oder Unternehmen MUSS den Passwortgebrauch verbindlich regeln (siehe auch P.4.A22 *Regelung zur Passwortqualität* und *P.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. Ein Passwort MUSS gewechselt werden, wenn es autorisierten Personen bekannt geworden ist oder der Verdacht dazu besteht.

P.4.A9 Identifikation und Authentisierung [IT-Unternehmen]

Der Zugriff auf alle IT-Systemen und Diensten 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.

P.4.A22 Regelung zur Passwortqualität [IT-Unternehmen]

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.

P.4.A23 Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme[IT-Unternehmen]

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 überprüft 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 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 umgesetzt werden.

A10 Schutz von Benutzerkennungen mit weitreichenden Berechtigungen[IT-Unternehmen] (S)

Benutzerkennungen mit weitreichenden Berechtigungen SOLLTEN mit einer Mehr-Faktor-Authentisierung, z. B. mit kryptografischen Zertifikaten geschützt werden. Art. 40 DS-GVO.