FFHS
Fernfachhochschule Schweiz
Zürich | Basel | Bern | Brig
Mitglied der SUPSI

Fernfachhochschule Schweiz
Studiengang BSc.INF

Sichere Einführung eines Passwortmanagers

Bachelor-Thesis im Studiengang Informatik

von

Peter Matijasic

Eingereicht bei:

Dr. Oliver Kamin
Departement Informatik
Departementsleiter

Referent:

Dr. Frank Möhle

Baar, 12. März 2021

Zusammenfassung

Was muss unternommen werden, damit im geschäftlichen Umfeld die Risiken bei der Einführung eines Passwortmanagers weitestgehend minimiert werden?
Um eine Antwort auf diese Frage zu erhalten, wird zunächst ein spezifisches Bedrohungsmodell anhand der üblichen Architektur der gängigsten Passwortmanager erstellt. Mittels der im Bedrohungsmodell gefundenen potentiellen Schwachstellen werden anschliessend Gegenmassnahmen erarbeitet. Diese Gegenmassnahmen werden dann in eine Zeremonie verpackt, die die sichere Einführung des Passwortmanagers gewährleistet.
Die vorgeschlagene Zeremonie umfasst Sicherheitsmassnahmen im Bereich Testing, Abhörsicherheit, Client- und Serversicherheit, Netzwerksicherheit, personelle Sicherheit, organisatorische Massnahmen, Nachvollziehbarkeit und Beurkundung durch Zeugen.
Die abschliessende Anwendung der Zeremonie auf die exemplarische Anwendung auf die Einführung von LastPass belegt die Praktikabilität und die Minimierung der Risiken wie in der Fragestellung gefordert.

Abstract

What must be done to ensure that in the business environment risks associated with the introduction of a password manager are minimized as far as possible?
In order to obtain an answer to this question, a specific threat model is first created based on the common architecture of the most popular password managers. With the assistance of the potential vulnerabilities identified in the threat model, countermeasures are then developed. These countermeasures are then packaged into a ceremony that ensures the secure implementation of the password manager.
The proposed ceremony includes security measures in the areas of testing, eavesdropping, client and server security, network security, personnel security, organizational measures, traceability by witness attestation.
The final application of the ceremony to the exemplary application to the implementation of LastPass proves the practicability and the minimization of risks as required by the objective of this thesis.

Inhaltsverzeichnis

Abkürzungen

AD	Active Directory
APP	Applikation (BSI-Grundschutz-Bausteine)
BSI	Bundesamt für Sicherheit in der Informationstechnik
BYOD	Bring your own Device
CIA	Confidentiality Integrity Availability
COBIT	Control Objectives for Information and Related Technology
CVSS	Common Vulnerability Scoring System
CWSS	Common Weakness Scoring System
DFD	Data Flow Diagram
GUI	Graphical User Interface
INF	Infrastruktur (BSI-Grundschutz-Bausteine)
ISO	International Organization for Standardization
MITM	Man in the middle
NIST	National Institute of Standards and Technology
NET	Netzwerk (BSI-Grundschutz-Bausteine)
OPS	Operations (BSI-Grundschutz-Bausteine)
ORP	Organisation und Personal (BSI-Grundschutz-Bausteine)
OWASP	Open Web Application Security Project
PASTA	Process for Attack Simulation and Threat Analysis
RZ	Rechenzentrum
SSL	Secure Sockets Layer
SYS	Systeme (IT-Systeme) (BSI-Grundschutz-Baustein)
TLS	Transport Layer Security
URL	Uniform Ressource Locator
VPN	Virtual Private Network

1 Einleitung

Mit dem Fortschreiten der Digitalisierung in unserer Gesellschaft, steigt auch die Anzahl der Log-Ins, welche man sich merken muss. Man tritt einem sozialen Netzwerk bei und muss ein Log-In erstellen. Dabei braucht man seine E-Mail-Adresse und ein Passwort. Man bestellt online eine neue Kaffeemaschine und muss sich beim Onlineshop anmelden. Wieder braucht man ein Log-In. Diese Auflistung liesse sich beinahe beliebig weiterführen. Die einfachste Variante um sich alle Log-Ins zu merken: man verwendet überall dasselbe Passwort. Aber ist das sicher? Wird das Passwort an einer Stelle geknackt, sind auch alle anderen Log-Ins betroffen. Jetzt könnte man ja noch den Namen der Website, bei welcher man sich anmeldet, noch ins Passwort mitaufnehmen. Ja, das ist etwas sicherer, aber mit ein klein wenig Aufwand wird der potentielle Angreifer diese Taktik durchschauen.

Man könnte natürlich auch seine Passwörter auf einen Zettel schreiben, aber sicher ist man immer noch nicht. Den Zettel hat man nicht immer dabei und es besteht die Gefahr, dass eine Drittperson den Zettel und damit die Passwörter sieht. Oder, da wir ja im digitalen Zeitalter sind, kann man die Passwörter ja auch in eine Excel-Tabelle eintragen und diese Tabelle mit einem Passwort schützen. Wirklich handlich wird das aber auch nicht und Excel ist sicherlich vieles, aber kein geeignetes Tool, um Passwörter sicher zu verwalten.

Spätestens, wenn man die oberen Punkte aus Sicht eines Unternehmens betrachtet, scheitern die obigen Varianten. Was ist, wenn man sein Log-In beim Distributor mit einem Arbeitskollegen[1] teilen muss? Wie entzieht man ihm das Log-In wieder, wenn er die Firma verlässt? Wie teile ich ein Passwort vorübergehend mit einem Mitarbeiter?

Die einfachste und sicherste Lösung: Man setzt einen Passwortmanager ein.

1.1 Ausgangslage

Im geschäftlichen Umfeld soll also ein Passwortmanager eingeführt werden. Man zieht die für die IT verantwortliche Person bei und beauftragt sie damit. Die übliche Vorgehensweise wird sein, dass man zuerst mal die Anforderungen aufnimmt, welche an das neue Tool gestellt werden. Anhand derer wird dann aus einer Vielzahl von Angeboten das für den

[1] Die Benutzung der männlichen Form geschieht aus reinen Vereinfachungsgründen und intendiert weder eine Ausgrenzung noch eine Geringschätzung der weiblichen Form.

jeweiligen Betrieb passendste Produkt ausgewählt, installiert und den Nutzenden zur Verfügung gestellt. Mit etwas «Glück» bekommen die anwendenden Personen sogar noch eine Einführung in das Tool und das war es dann.

1.2 Problemstellung

Die alleinige Installation und Nutzung eines Passwortmanagers ist aber noch keine Garantie dafür, dass die Log-Ins nun sicher sind. Damit kommen wir zur Forschungsfrage:
Was muss unternommen werden, damit im geschäftlichen Umfeld die Risiken bei der Einführung eines Passwortmanagers weitestgehend minimiert werden?

Alleine bei der Auswahl des Tools müssen schon einige Sicherheitsaspekte beachtet werden. Darf ein Cloud-Dienst zum Einsatz kommen? Müssen die Nutzenden auch von extern auf die Log-Ins Zugriff haben? Wer darf welche Passwörter benutzen?

Der BSI-Standard wurde hier als Leitlinie genommen, da vom BSI mit dem Grundschutzkompendium ein umfangreiches Framework zur Verfügung steht. Mit den Bausteinen aus diesem Framework kann in einem Unternehmen ein solider Grundschutz für die IT aufgebaut werden. Durch den modularen Aufbau lässt sich das Framework an die eigenen Anforderungen und Bedürfnisse anpassen.

In dieser Thesis soll ein Verfahren zur sicheren Einführung eines Passwortmanagers erarbeitet werden. Da das Verfahren ein kritischer Schritt ist, welcher diverse Angriffspunkte bietet, wird das Verfahren in Form einer Zeremonie beschrieben. In dieser Zeremonie werden detailliert Schritte aufgezeigt, welche eingehalten werden müssen, um die Einführung so sicher wie möglich zu gestalten.

1.3 Aktueller Forschungsstand

Die Recherche zum aktuellen Forschungsstand zeigt, dass Passwortmanager Gegenstand von einigen Studien sind. Untersucht wurde in erster Linie die Sicherheit von Passwortmanagern. Das Paper von (Oesch & Ruoti, 2020) zeigt beispielsweise den Fortschritt der Sicherheit von Passwortmanagern. Untersucht wurden sowohl die gängigsten Passwortmanager als auch die Browsererweiterungen in den verbreitetsten Browsern. Zum einen war die Sicherheit der Verschlüsselung und damit die der Vertraulichkeit der gespeicherten Passwörter Gegenstand der Untersuchung. Weiter wurde auch darauf eingegangen, wie sicher die durch den Passwortmanager generierten Passwörter sind. Also wie zufällig diese sind oder ob sich sogar Muster in den generierten Passwörtern erkennen lassen.

Eine relevante Studie kommt von (Pearman, Zhang, Bauer, Christin, & Cranor, 2019) welche untersucht, warum Menschen Passwortmanager (nicht) effektiv benutzen. Die Autoren untersuchten drei Arten von Benutzern: Diejenigen, welche keinen Passwortmanager benutzen, diejenigen, welche die Browsereigenen Tools nutzen und letztlich noch diejenigen, welche ein separates Tool zur Verwaltung der Passwörter installieren. Interessant war hier vor allem die Motivation zur Nutzung der Tools. Während die Gruppe mit den Browsereigenen Tools vor allem aus Bequemlichkeit handelte, war die Gruppe mit den separat installierten Passwortmanagern vom Sicherheitsgedanken motiviert. Anhand dieser Studie kann zumindest ein Stück weit postuliert werden, dass die Leser dieser Thesis schon mal einen wichtigen Schritt gemacht haben: Sie wollen einen Passwortmanager vor allem aus Sicherheitsüberlegungen.

Zur sicheren Einführung eines Passwortmanagers wurden keine Studien gefunden. Auch die Hersteller der Passwortmanager schreiben lediglich über die Funktionalitäten ihrer Produkte oder über deren Installation. Die Einführung des Passwortmanagers mit ihren möglichen Stolperfallen wird dabei aber nirgends thematisiert.

2 Aufbau eines Threat-Modells

“Threat modeling is the key to a focused defense.
Without threat modelling, you can never stop playing whack-a-mole.”
(Shostack, 2014)

Um ein Bewusstsein für die Angriffsflächen eines Passwortmanagers, sowohl bei der Einführung als auch im Betrieb, zu erhalten, wird ein Threat-Modell erstellt. Der Betrieb des Passwortmanagers ist zwar nicht im Scope dieser Thesis, aber im Sinne einer umfassenden Bewertung möglicher Schwachstellen wurde der Betrieb mit in das Threat-Modell integriert. Die Erkenntnisse aus dem Threat-Modell sind im Anschluss an die Einführung sicherlich ein gutes Hilfsmittel.

Eine Übersicht über die Methoden zur Erarbeitung eines Threat-Modells wurden aus (Sevchenko, Chick, O'Riordan, Scanlon, & Woody, 2018)übernommen. Aus diesen Methoden wurde der «Process for Attack Simulation and Threat Analysis», kurz PASTA, ausgewählt. Die Wahl fiel aus diversen Gründen auf diese Methode. Besonders herauszuheben ist hier, dass diese Methode eine integrierte Priorisierung der gefunden Schwachstellen besitzt und bei der Identifizierung mildernder Techniken hilft.

Anhand des (OWASP Threat Modeling Cheat Sheet, 2020) wurden dann die notwendigen Schritte für den Aufbau des Modells genauer untersucht. Bei näherer Betrachtung der Methode wurde im Rahmen dieser Thesis klar, dass nicht für alle Punkte der Methode ausreichend Daten vorhanden sind. Dies begründet sich vor allem damit, dass die Methode auf die Untersuchung eines spezifischen Produktes ausgelegt ist. Die Thesis hat aber als Ziel, unabhängig von der Wahl des Passwortmanagers eine Einführungszeremonie für eben diesen zu bieten. Deshalb wurde das Threat-Modell in Anlehnung an die gewählte Methode erstellt. Die Findung von potentiellen Schwachstellen ist dadurch aber nicht beeinträchtigt.

Der Ablauf der PASTA-Methode ist in Abbildung 1 skizziert. Die Abbildung entstand nach Vorlage von (Uceda Velez, 2013) und wurde im Wesentlichen lediglich ins Deutsche übersetzt.

Der Aufbau des Threat-Modells erfolgte so generisch wie möglich. Es gilt zu beachten, dass je nach Umgebung die Anforderungen variieren können. Vor der Anwendung der fertigen Zeremonie sollte überprüft werden, ob die erkannten Schwachstellen auch den eigenen Anforderungen entsprechen.

Abbildung 1: PASTA-Methode. Die einzelnen Schritte der PASTA-Methode (Uceda Velez, 2013). In dieser Thesis werden ausgewählte Elemente behandelt. Insbesondere der vierte Schritt musste aufgrund mangelnder Daten stark modifiziert werden.

2.1 Ziele definieren

In jeder Firma existieren Daten, welche geheim gehalten werden müssen. Werden diese Daten elektronisch verarbeitet, müssen sie durch entsprechende Sicherheitsmechanismen geschützt sein. In der Regel wird für den Zugriff auf solche Daten ein Passwort benötigt. Laut Obligationenrecht ist sowohl der Arbeitnehmer (Sutter-Somm, 2020) gemäss Art. 321a Abs. 4 als auch die Geschäftsleitung / der Verwaltungsrat gemäss Art. 753 ff. zur Wahrung dieser Geheimnisse verpflichtet. Die Wahl eines schlechten Passwortes verstösst aber gegen die Sorgfaltsplicht. Es ist also im Sinne der Unternehmung, dass sichere Passwörter verwendet werden.

Je nach Geschäftsfeld der Unternehmung können auch noch weitere Compliance-Anforderungen bestehen, welche sichere Passwörter voraussetzen.

Gemäss dem (verizon data breach investigations report, 2020) richteten sich 43% der Sicherheitsverletzungen gegen Webanwendungen. Davon wurden in über 80% der Fälle gestohlene oder per Brute-Force-Methode geknackte Passwörter verwendet. Dies zeigt die Wichtigkeit von sicheren Passwörtern auf.

Der Business-Impact hängt vom Tätigkeitsfeld des Unternehmens und den daraus resultierenden Daten ab. Für die Erstellung dieses Threat-Modells wird davon ausgegangen, dass ein Sicherheitsvorfall infolge von schlechten Passwörtern sowohl einen grossen finanziellen Schaden als auch einen Reputationsschaden verursacht. Es kann also von einem erhöhten Schutzbedarf ausgegangen werden.

Da das primäre Ziel der Thesis die Einführung des Passwortmanagers ist, wird ein besonderes Augenmerk auf die Erstinstallation des Passwortmanagers und auf die Erfassung von Passwörtern in diesem gelegt.

2.2 Technischen Umfang definieren

Um diesen Punkt umsetzen zu können, muss die Architektur des zum Einsatz kommenden Passwortmanagers bekannt sein. Stellvertretend wird hier die Architektur von LastPass[2] herangezogen. Dieser wurde in erster Linie gewählt, weil hier die entsprechende Dokumentation frei verfügbar und hinreichend umfänglich ist.

[2] www.lastpass.com

Die aktuell verbreiteten Passwortmanager mögen sich im Funktionsumfang oder auch in der eingesetzten Technik unterscheiden. Das Grundprinzip eines «Passwortsafes», aus welchem die Passwörter mithilfe eines Masterpasswortes abgerufen werden können, ist aber allen gemein.

Die grundlegende Architektur ist in Abbildung 2 ersichtlich, welche aus dem Technical Whitepaper von LastPass stammt (LastPass, 2019).

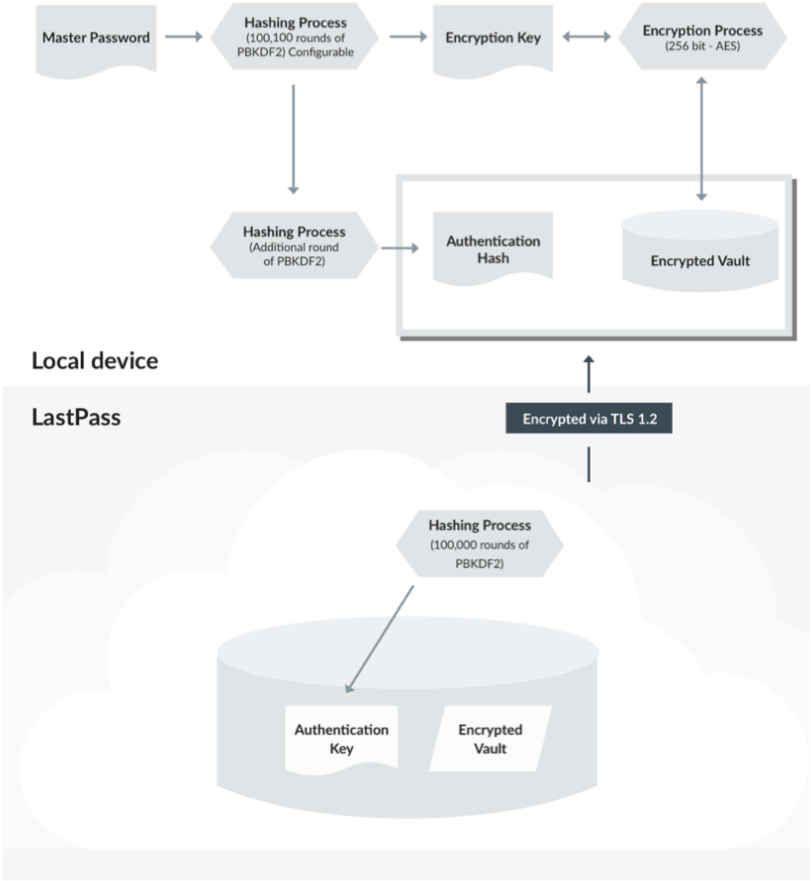

Abbildung 2: Architektur LastPass (LastPass, 2019)

Grundsätzlich kommen zwei Arten von Passwortmanagern zum Einsatz: Die eine Variante setzt auf eine lokale Datenbank, wie beispielsweise KeePass[3], die andere setzt auf eine zentrale Datenbank im eigenen RZ oder in der Cloud. Bei LastPass handelt es sich um die letztere Variante mit einer Datenbank beim Anbieter. Für das Threat-Modell ist diese Variante die ergiebigere, da durch den Datenaustausch über das Internet zusätzliche Angriffsvektoren entstehen. Ausserdem ist mit dieser Art von Passwortmanager die Verwaltung von Benutzern und Gruppen deutlich einfacher. Weiterhin werden der Zugriff auf den Passwortmanager vereinfacht und Inkosistenzen der Datenbank vermieden.

[3] www.keepass.info

Die Abgrenzung der technischen Umgebung wird in Abbildung 3 dargestellt. Im hier erstellten Threat-Modell wird der Benutzer betrachtet, welcher an einem Endgerät im lokalen Netzwerk über eine Firewall und das Internet mit der Datenbank des Passwortmanagers kommuniziert.

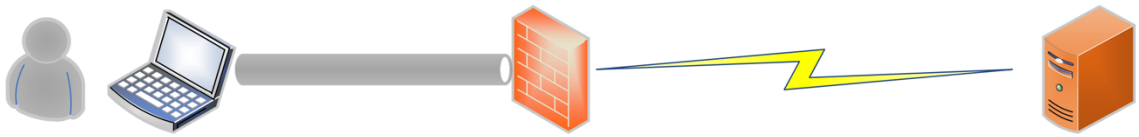

Abbildung 3: Stark vereinfachtes Prinzipschema der Kommunikation des Passwortmanagers mit dem Server.

Nachfolgend wird auf die Abhängigkeiten dieser Konstellation eingegangen. Der Benutzer benötigt ein Endgerät, von welchem aus er Zugriff ins Internet und somit auf die Passwortdatenbank hat. Weiter muss auf dem Gerät eine Clientsoftware des Passwortmanagers installiert sein. Als Grundlage für den sicheren Betrieb wird davon ausgegangen, dass der Client den Anforderungen nach dem BSI-Grundschutz, insbesondere dem Baustein SYS.2.1: Allgemeiner Client (BSI, 2020) entspricht.

Weiter besteht eine Abhängigkeit in der Konnektivität zum Internet. Und schlussendlich muss auch der Server, sei dies ein eigener oder der Server in der Cloud des Anbieters, erreichbar und funktionsfähig sein.

2.3 Anwendung dekomponieren

Für die Erarbeitung des Threat-Modells wurden die gängigsten Use-Cases bei der Verwendung eines Passwortmanagers identifiziert. Diese sind in Abbildung 4 ersichtlich.

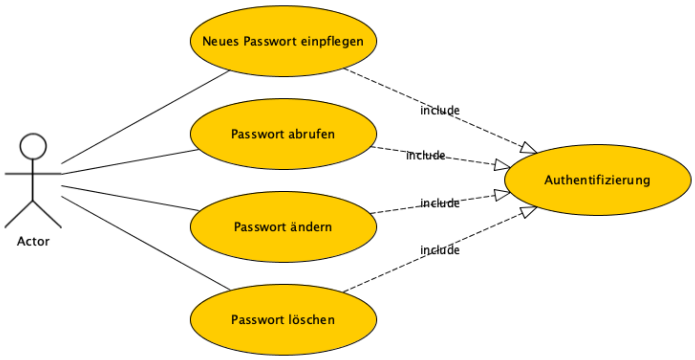

Abbildung 4: Use-Cases bei der Verwendung eines Passwortmanagers.

Der Zugriff auf den Passwortmanager erfolgt wie in Kapitel 2.2 beschrieben. Denkbar sind dabei mehrere Arten von Endgeräten, über welche der Benutzer auf den Passwortmanager zugreift. Dies kann sowohl ein stationäres Gerät wie ein Computer oder Laptop sein, oder

ein mobiles Device wie beispielsweise ein Smartphone. Das Endgerät kann dabei wiederum in mehrere Unterkategorien unterteilt werden. Als sicherste Variante kann der durch die Firmen-IT verwaltete Computer angesehen werden. Die nächste Variante wäre das private Gerät des Benutzers. Durch die Verbreitung von BYOD wird diese Variante immer häufiger. Die letzte Variante eines Computers wäre noch der Zugriff über das Gerät eines Dritten. Hier wäre das Arbeiten aus einem Internet-Café oder dergleichen denkbar. Auch bei den mobilen Devices kann zwischen privaten und von der Firmen-IT verwalteten Geräten unterschieden werden.

Als Akteure können folgende Gruppen identifiziert werden:

- Unbefugter Nutzer
- Benutzer
- Leiter / Vorgesetzter
- Administrator

Die vier Gruppen von Akteuren unterscheiden sich grundsätzlich über die gewährten Rechte, wobei die Auflistung in aufsteigender Menge der Rechte sortiert wurde. Diese korrespondieren auch mit den Rollen, welche diesen zugewiesen sind.

Die Services können in zwei Kategorien eingeteilt werden. Es gibt die Services, welche den Benutzern den Zugriff auf und die Interaktion mit der Datenbank ermöglichen. Dann sind noch die Services für das Backend, über welche beispielsweise automatisierte Backups der Datenbank durchgeführt werden.

Als Grundlage für den Datenfluss, wird das DFD von LastPass (LastPass, 2019) verwendet. In Anlehnung daran ergibt sich das DFD in Abbildung 5.

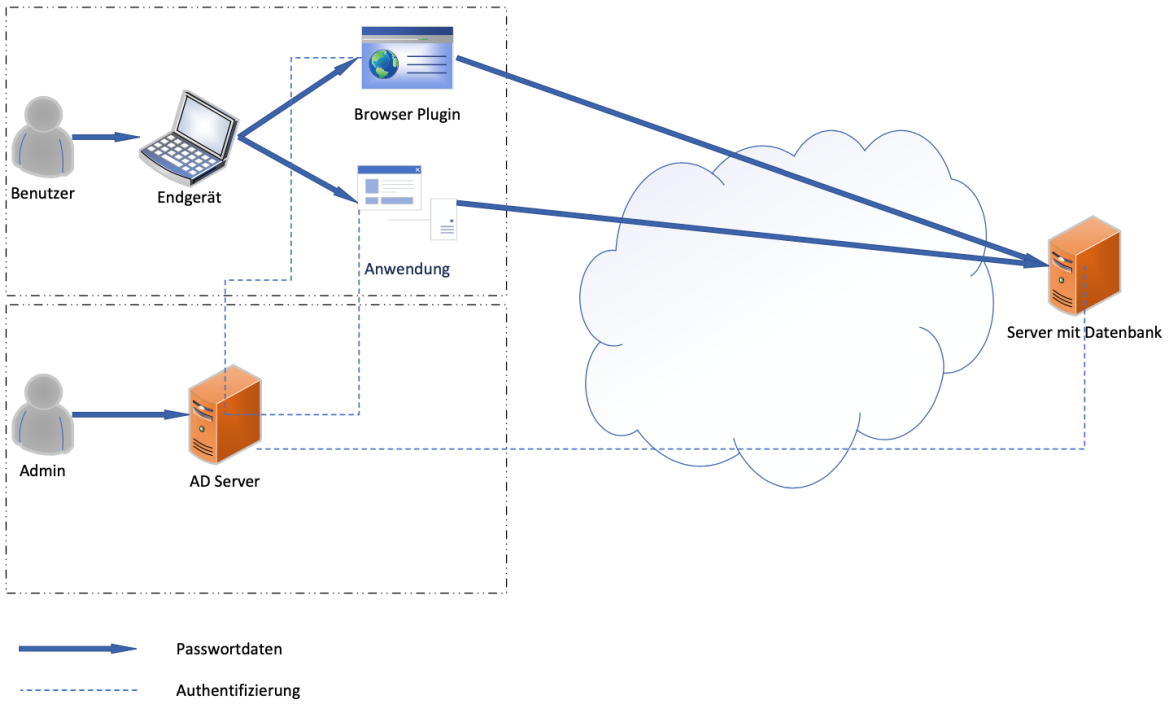

Abbildung 5: LastPass DFD (Data Flow Diagram). Der AD-Server kommt dabei nur zur Anwendung, falls LastPass für die Benutzerauthenzifizierung auch an das Active Directory angebunden wird.

2.4 Bedrohungsanalyse

Beim Einsatz eines Passwortmanagers sind grundsätzlich drei Arten von Daten bedroht:

- Einzelnes Log-In
- Masterpasswort eines Benutzers
- Passwortdatenbank

Die oben aufgeführten Daten sind in aufsteigender Kritikalität aufgeführt. Diese Daten können sowohl durch interne als auch externe Akteure angegriffen werden. Die möglichen Angriffsszenarien auf diese Daten sind dieselben. Die Art der Bedrohung zielt jeweils auf einen oder mehrere Punkte des CIA-Prinzips ab.

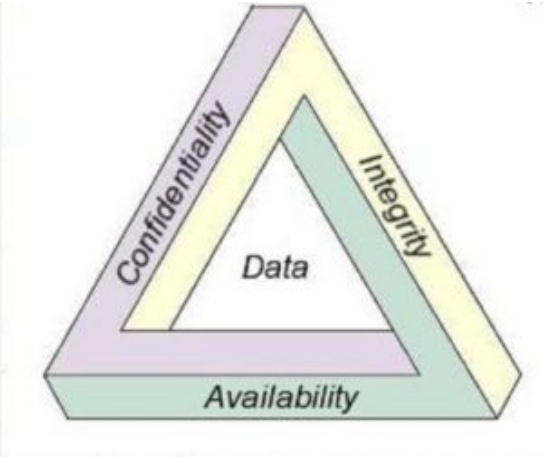

Abbildung 6: CIA Prinzip[4]

Confidentiality: Vertraulichkeit der Daten; Die Daten dürfen nur für berechtigte Personen zugänglich sein.
Integrity: Integrität der Daten; Die Daten müssen integer sein. Sie dürfen nicht unberechtigt verändert werden.
Availability: Verfügbarkeit der Daten; Die Daten müssen für die Benutzer verfügbar sein.

Ein Angreifer, sei es ein interner oder ein externer, kann also versuchen eine der drei Datenarten zu stehlen, zu manipulieren oder ihre Verfügbarkeit einzuschränken oder zu unterbinden.

An dieser Stelle wird etwas von den Vorgaben durch die PASTA-Methode abgewichen. Gemäss der Methode wäre hier eine probabilistische Analyse gefordert. Im vorliegenden Fall liegen aber keine belegbaren Zahlen für alle Szenarien vor, anhand welcher dieser

[4] Bildquelle: https://informedfuture.org/wp-content/uploads/2018/02/cia-triad-300x252.jpg Zugriffsdatum: 14.11.2020

Analyse dementsprechend durchgeführt werden könnte. Dementsprechend ist auch eine Regressionsanalyse nicht durchführbar.
Anhand der aus den vorherigen Schritten der PASTA-Methode gewonnen Erkenntnisse ergeben sich neun Bedrohungen. Diese sind in der nachfolgenden Tabelle aufgeführt und nummeriert.

	Confidentiality	Integrity	Availability
Einzelnes Log-In	M1	M2	M3
Master-Log-In	M4	M5	M6
Passwortdatenbank	M7	M8	M9

Tabelle 1: Bedrohungsmatrix

Bei diesen neun Bedrohungen wird in diesem Schritt nicht zwischen einem Innen- und einem Aussentäter unterschieden.
Weiter lassen sich aus den vorherigen Schritten der PASTA-Methode, insbesondere aus der Dekomponierung, folgende Angriffspunkte identifizieren. In Abbildung 7 sind mögliche Angriffspunkte eingezeichnet, welche nachfolgend benannt und nummeriert werden.

- A1 Benutzer
- A2 Interaktion des Benutzers mit dem Endgerät
- A3 Endgerät
- A4 Browser Plug-In / Clientanwendung
- A5 Kommunikation Client / Plug-In mit dem Server
- A6 Authentifizierung Client / Plug-In
- A7 Administrator
- A8 AD / Verzeichnisdienst
- A9 Kommunikation des Verzeichnisdienstes mit der Datenbank
- A10 Datenbank
- A11 Backup

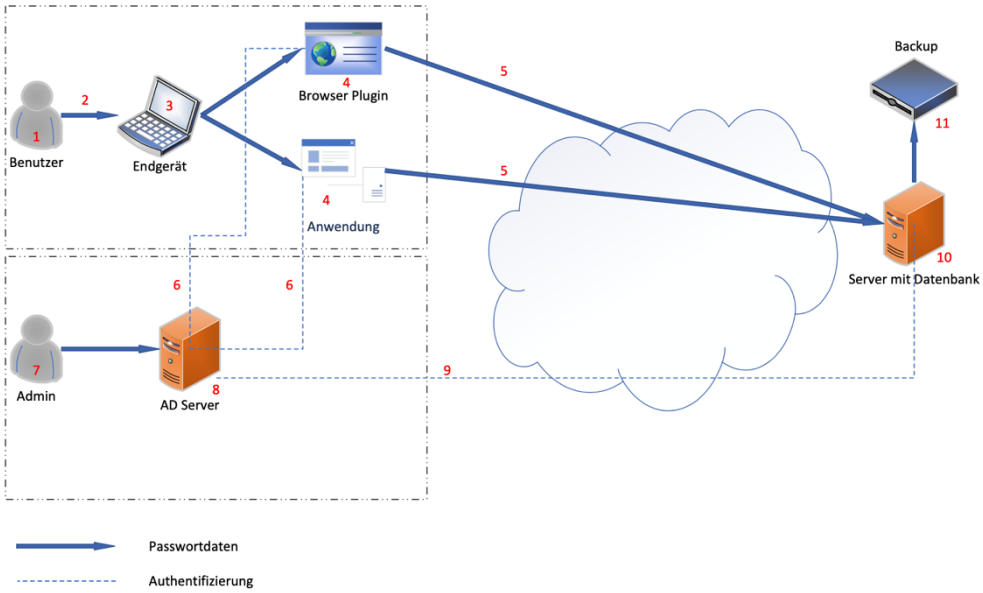

Abbildung 7: Angriffspunkte

2.5 Schwachstellen & Schwachstellenanalyse

Aus den vorangegangenen Schritten sind nun Bedrohungen (M1 bis M9) und Angriffspunkte (A1 bis A11) bekannt. Anhand der Bedrohungen wurden nun Bedrohungsbäume erstellt. Jeder Bedrohungsbaum zeigt potentielle Schwachstellen auf. Einige der Punkte aus der Bedrohungsmatrix lassen sich dabei in einem Baum zusammenfassen.

Die Angriffsschritte (AS1 bis AS18) wurden dabei nummeriert. Anhand dieser Angriffsschritte werden die Scorings erstellt. Das Scoring ist dabei der Faktor aus der Eintrittswahrscheinlichkeit des Ereignisses und dessen Auswirkung. Dieses Scoring wird in Tabelle 2 als Muster gezeigt.

Angriffsbaum Integrität und Vertraulichkeit einzelnes Login und Masterpasswort

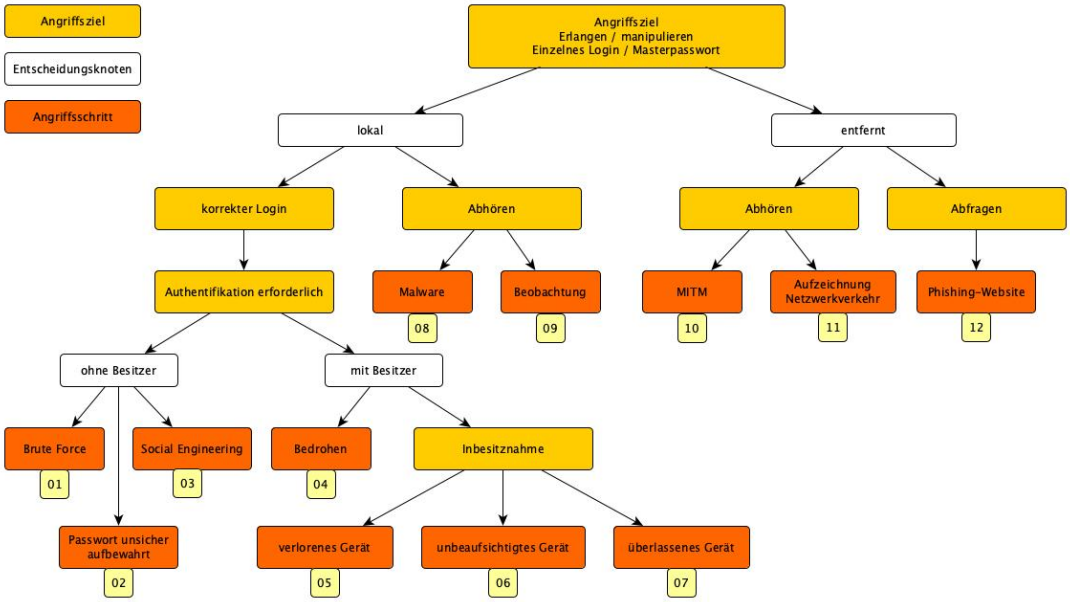

Abbildung 8: Bedrohungsbaum 1 zeigt die möglichen Angriffe auf die Integrität und / oder Vertraulichkeit eines einzelnen Logins oder des Masterpasswortes. Die Nummern in den gelben Kästchen dienen der Zuordnung der einzelnen Angriffsschritte.

Abbildung 8 zeigt den Bedrohungsbaum für die Bedrohungen 1, 2, 4 und 5 aus der Bedrohungsmatrix. Also jeweils eine Bedrohung der Vertraulichkeit oder Integrität eines einzelnen Logins oder des Masterpasswortes für den Zugang eines Benutzers zum Passwortmanager. Diese wurden zusammengefasst, da das Vorgehen zur Realisierung eines Angriffs über die entsprechende Bedrohung sehr ähnlich ist.

Angriffsbaum Integrität und Vertraulichkeit Passwortdatenbank

Abbildung 9 zeigt den Baum für die Bedrohungen 7 und 8 aus der Bedrohungsmatrix, die Bedrohung von Vertraulichkeit und Integrität der Passwortdatenbank. Auch hier kann mit vergleichbaren Methoden eines der beiden Ziele erreicht werden. Lediglich ab dem Entscheidungspunkt «Backup» ist nur noch eine Bedrohung für die Vertraulichkeit der Daten bedroht. Die Integrität der Daten kann über das Backup nur noch bedroht werden, falls das Backup wiederhergestellt werden muss.

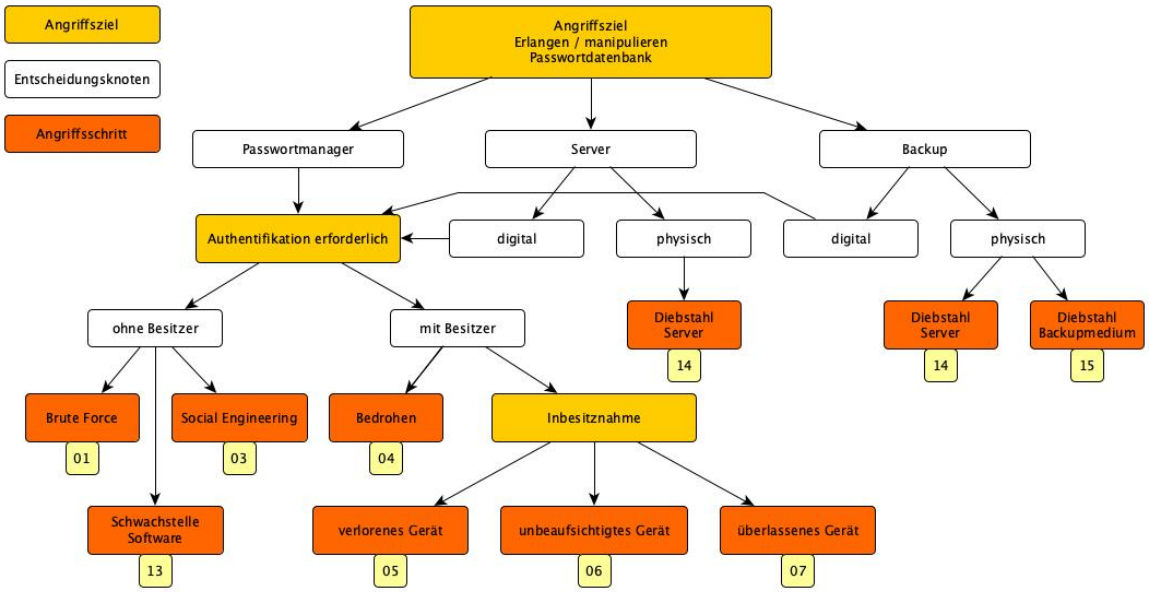

Abbildung 9: Bedrohungsbaum 2 zeigt die möglichen Angriffe auf die Integrität und / oder Vertraulichkeit der Passwortdatenbank. Die Nummern in den gelben Kästchen dienen der Zuordnung der einzelnen Angriffsschritte.

Angriffsbaum Verfügbarkeit

In Abbildung 10 ist schliesslich der Bedrohungsbaum für die Bedrohungen 3, 6 und 9 aus der Bedrohungsmatrix. Hier geht es um die Bedrohungen zur Verfügbarkeit von einzelnen Logins, dem Masterlogin zum Passwortmanager und der Passwortdatenbank selbst.

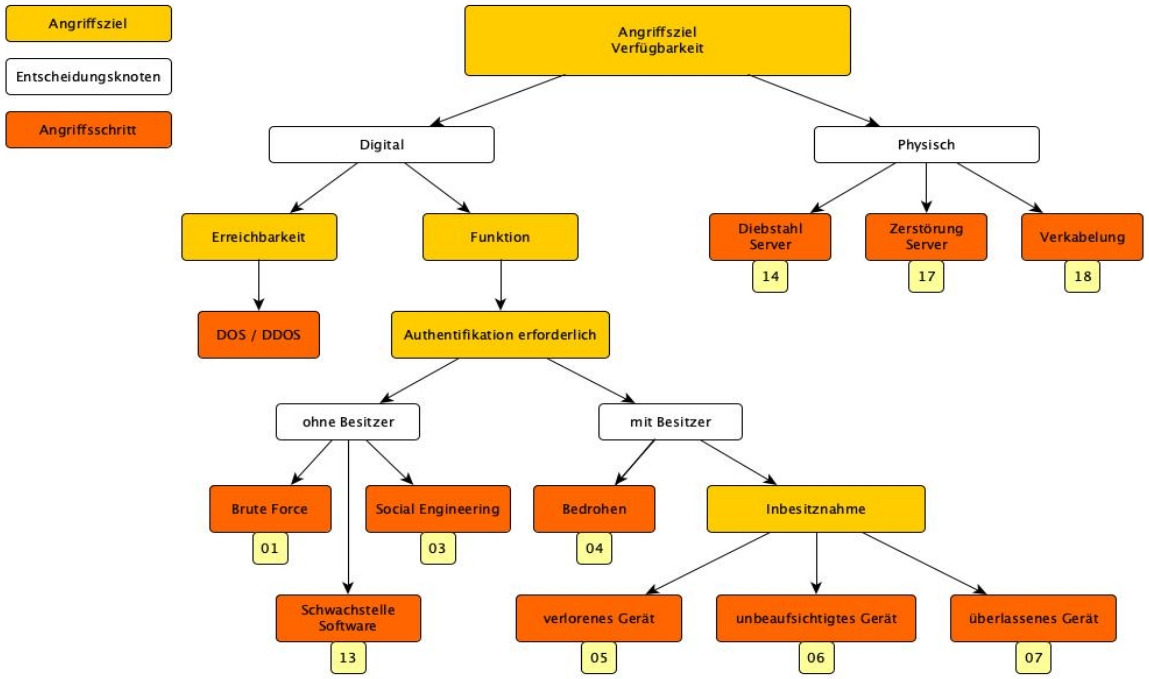

Abbildung 10: Bedrohungsbaum 3 zeigt die möglichen Angriffe auf die allgemeine Verfügbarkeit des Passwortmanagers. Die Nummern in den gelben Kästchen dienen der Zuordnung der einzelnen Angriffsschritte.

Im nächsten Schritt werden alle Angriffsschritte in einer Tabelle mit den einzelnen Bedrohungen verknüpft. Jede dieser Schwachstellen wurde anschliessend nach Wahrscheinlichkeit und Auswirkung bewertet. Dabei bedeutet 1 eine geringe Wahrscheinlichkeit / Auswirkung und 5 eine hohe Wahrscheinlichkeit / Auswirkung. Als Grundlage für die Bewertung der Wahrscheinlichkeit und der Auswirkung wurden zwei Quellen verwendet. Dies sind (BSI, Bundesamt für Sicherheit in der Informationstechnik, 2020) und (Schultz, 2020).

2.6 Angriffsmodellierung

Aus den Angriffsbäumen im vorangehenden Kapitel ergeben sich total 18 mögliche Angriffe mit neun verschiedenen Zielen. Den möglichen Angriffen wurden dabei Wahrscheinlichkeiten und den Zielen Auswirkungen auf einer Skala von 1 bis 5 zugewiesen (1=gering/unwahrscheinlich 5=hoch/wahrscheinlich). Die Bewertung dieser beiden Punkte erfolgte dabei in Anlehnung an (Schultz, 2020), (BSI, Bundesamt für Sicherheit in der Informationstechnik, 2020) und (verizon data breach investigations report, 2020). Die Bewertung ist nicht allgemeingültig und muss auf die eigene Situation und Bedrohungslage angepasst werden.

Angriffsschritt / Ziel (Bedrohung)	<- Wahrscheinlichkeit	Vertraulichkeit einzelnes Login	Integrität einzelnes Login	Erreichbarkeit einzelnes Log-In	Vertraulichkeit Master-Log-In	Integrität Master-Log-In	Erreichbarkeit Master-Log-In	Vertraulichkeit Datenbank	Integrität Datenbank	Erreichbarkeit Datenbank
Auswirkung ->		3	2	1	4	3	2	5	4	3
Brute Force	3	9	6	3	12	9	6	15	12	9
Passwort unsicher aufbewahrt	2	6	4	x	8	6	x	x	x	x
Social Engineering	3	9	6	3	12	9	6	15	12	9
Bedrohen	1	3	2	1	4	3	2	5	4	3
Verlorenes Gerät	2	6	4	2	8	6	4	10	8	6
Unbeaufsichtigtes Gerät	3	9	6	3	12	9	6	15	12	9
Überlassenes Gerät	1	3	2	1	4	3	2	5	4	3
Malware	5	15	10	5	20	15	10	25	20	15
Beobachtung	2	6	4	x	8	6	x	x	x	x
MITM	1	3	2	x	4	3	x	x	x	x
Aufzeichnung Netzwerkverkehr	2	6	4	x	8	6	x	x	x	x
Phishing Website	5	15	10	x	20	15	x	x	x	x
Schwachstelle Software	1	x	x	1	x	x	2	5	4	3
Diebstahl Server	1	3	x	1	4	x	2	5	4	3
Diebstahl Backupmedium	2	x	x	x	x	x	x	10	x	x
DOS / DDOS	2	x	x	2	x	x	4	x	x	6
Zerstörung Server	1	x	x	1	x	x	2	x	x	3
Verkabelung	1	x	x	1	x	x	2	x	x	3

Tabelle 2: Scoring Schwachstellen Möglicher Fleckenteppich zur Einschätzung der Gefahr einzelner Angriffe. Die Bewertung der Gefahr ergibt sich dabei aus dem Produkt der Wahrscheinlichkeit des Angriffs und der Auswirkung des Angriffs. Die Zahlen sind nicht repräsentativ und müssen für jedes Unternehmen erarbeitet werden. Die Angriffswahrscheinlichkeit muss anhand der momentanen Bedrohungslage abgeschätzt werden.

Um einen Score zu erhalten, wird die Eintrittswahrscheinlichkeit mit der Auswirkung multipliziert. Tabelle 2: Scoring Schwachstellen zeigt eine mögliche Matrix nach einer solchen Bewertung und dient hier lediglich als Beispiel, wie das Resultat eines solchen Scorings aussehen kann.

Mit dieser Tabelle wurde auch gleichzeitig der siebte Schritt aus der PASTA-Methode, die Risiko- und Auswirkungsanalyse, vorgezogen.

Im Rahmen dieser Thesis wird lediglich auf diejenigen Angriffe eingegangen, welche sich direkt auf die Einführung des Passwortmanagers auswirken. Alle weiteren Angriffe müssen natürlich auch beachtet und entsprechende Gegenmassnahmen getroffen werden. Dies sollte dabei schon vor der eigentlichen Einführung erfolgen.

Nachfolgend werden die Angriffsschritte, welche bei der Einführung des Passwortmanagers eine Auswirkung haben näher beschrieben und anhand dieser Schritte mögliche Angriffe entwickelt.

Passwort unsicher aufbewahrt: Die unsichere Aufbewahrung des Passwortes kann zwei unterschiedliche Arten von Passwörtern betreffen. Zum einen kann es sich um das Masterpasswort des Anwenders für den Passwortmanager selbst handeln. Das Post-it unter der Tastatur ist ein Klassiker für die unsichere Aufbewahrung. Hier wäre dann das Angriffsziel die Vertraulichkeit respektive Integrität des Masterpasswortes. Zum anderen kann es aber auch sein, dass der Anwender den Passwortmanager nicht nutzt oder schlicht die alten Passwörter in den Passwortmanager übernommen hat. In diesem Fall handelt es sich um einen Angriff auf die Integrität oder Vertraulichkeit eines einzelnen Logins. Bei mehreren identischen Passwörtern sind dabei sogar mehrere Logins betroffen.

Der eigentliche Angriff bei diesem Angriffsschritt ist dabei nicht technischer Natur. Ein Angreifer braucht in diesem Fall lediglich physischen Zugang zum Arbeitsplatz des Anwenders. Die Wahrscheinlichkeit, dass auch ein etwas kreativeres Versteck gefunden wird, ist hierbei ziemlich gross. Verwendet der Benutzer trotz eines Passwortmanagers weiterhin schwache Passwörter, können diese auch durch Social-Engineering herausgefunden werden. Ein Beispiel ist die Verwendung der eigenen Postleitzahl im Passwort.

Social Engineering: Das Social Engineering ist in der Regel ein Schritt in der Vorbereitung eines Angriffs. Dabei wird versucht, soviel wie möglich über eine Person oder über einen Betrieb in Erfahrung zu bringen um so beispielsweise einen Phishing-Angriff gezielt durchführen zu können. Im Zusammenhang mit der Einführung eines Passwortmanagers kann das Social Engineering einem Angreifer auch wichtige Informationen liefern. Ist beispielsweise der Zeitpunkt der Einführung bekannt, kann gezielt zu diesem Zeitpunkt ein Angriff

geplant werden. Auch lässt sich mit dieser Methode unter Umständen in Erfahrung bringen, welches Produkt eingesetzt wird.

Unbeaufsichtigtes Gerät: Ein unbeaufsichtigtes Gerät und im besten Fall (aus Sicht des Angreifers) nicht gesperrtes Gerät ermöglicht dem Angreifer viele Möglichkeiten. Vor allem während der Einführung des Passwortmanagers kann davon ausgegangen werden, dass der Benutzer des Gerätes noch beim Passwortmanager angemeldet ist. Somit kann ein Angreifer direkt auf die Passwörter zugreifen und beispielsweise auch gleich das Masterpasswort des Benutzers ändern. Handelt es sich um das Gerät eines Anwenders mit erweiterten Rechten, kann auch gleich ein weiteres Konto für den Angreifer angelegt werden.
Ein weiterer möglicher Angriff ist hier das Installieren einer Malware. Auf Angriffe mit Malware wird im nächsten Unterkapitel genauer eingegangen.

Malware: Malware kann in ganz unterschiedlichen Arten und mit unterschiedlichen Auswirkungen zum Einsatz kommen. Dabei kann die Malware Clients oder Server infizieren. Bei der Einführung eines Passwortmanagers sind beide Möglichkeiten für einen Angreifer interessant.

Ein möglicher Angriff ist der Einsatz eines Überwachungstools. Gelingt es dem Angreifer vor der Einführung des Passwortmanagers eine Malware auf einem Client zu installieren, welche sämtliche Vorgänge aufzeichnet, bekommt der Angreifer alle getätigten Eingaben mit. Es kann also die Eingabe des Masterpasswortes aufgezeichnet werden oder die Generierung jedes neuen Passwortes. Somit wird der Passwortmanager ad absurdum geführt. Der Angriff erfolgt dann auf die Vertraulichkeit einzelner Logins und auf das Masterlogin. Kommt ein derartiges Tool auf den Server mit der Datenbank des Passwortmanagers, hängt es vom Passwortmanager ab, inwiefern die Vertraulichkeit verletzt wird. Bei einer Ende-zu-Ende Verschlüsselung ist diese nicht betroffen.

Ein weiterer möglicher Angriff wäre eine Ransomware. Schlägt diese während oder kurz nach der Einführung des Passwortmanagers zu, ist im schlimmsten Fall die Verfügbarkeit von einzelnen Logins und auch der Datenbank verletzt. Werden während der Einführung noch die Passwörter der erfassten Logins geändert, ist der Schaden erheblich. Bis die Datenbank mit den Passwörtern den Backupzyklus durchlaufen hat, kann auch noch eine gewisse Zeit vergehen. Gerade in kleineren Firmen ist ein tägliches Backup häufig anzutreffen. Schlägt die Malware nun nach der Einführung und vor dem ersten Backup zu, ist das für den Angreifer der perfekte Zeitpunkt.

Beobachtung: Ein physischer Angriff bei der Einführung eines Passwortmangers ist die Beobachtung. Bei diesem Angriff wird es sich eher um einen Innen- als um einen Aussentäter handeln. Eine unbekannte Person würde in dieser Situation wohl Aufsehen erregen. Klassisch wäre der Blick über die Schulter, während der Benutzer sein Passwort eingibt. Bei Passwortmanagern wird zwar die Eingabe auf dem Bildschirm unkenntlich gemacht, aber wenn jemand nicht sehr schnell tippt, oder aber beim Eintippen des Passwortes gefilmt wird, kann dieses nachvollzogen werden.

Eine weitere Möglichkeit der Beobachtung ist aber auch bei der Erstellung neuer Passwörter gegeben. Werden Passwörter in diesem Schritt auf dem Bildschirm in Klartext angezeigt, ist es für den Angreifer verhältnismässig einfach, in den Besitz des Passwortes zu kommen. Insbesondere beim Filmen der Passworteingabe oder der Passwortanzeige auf dem Bildschirm, kann dies aber auch von ausserhalb des Gebäudes passieren. Mit entsprechender Ausrüstung, wie beispielsweise einem Tele-Objektiv, kann auch aus dem Nachbarhaus die Eingabe gefilmt werden.

Eine ähnliche Kategorie eines Angriffes, ist das Abhören. In (Giallanza, et al., 2019) wurde aufgezeigt, dass mit den Sensoren eines Smartphones auch in geräuschvollen Umgebungen Tastatureingaben abgehört und rekonstruiert werden können. Ein Angreifer könnte also das Smartphone oder den PC des Opfers mit einer Malware infizieren, welche das Mikrofon zur Aufzeichnung der Tastatureingaben verwendet. Es wäre auch möglich, im Büro des Opfers ein Smartphone zu verstecken und auf diese Art die Passwörter abzuhören.

Eine Kombination der beiden oben genannten Methoden haben (Davis, et al., 2014) in einem Artikel beschrieben. Hier wurde anhand von durch Schall verursachten Vibrationen eines Gegenstandes in einem Raum der Schall wieder hörbar gemacht. Dabei wurde dieser Gegenstand mit einer Highspeed-Kamera gefilmt und aus den Bildern dann der Schall zurück gerechnet. Mit so einer Side-Channel Attacke können dann entweder Gespräche mitgelauscht oder auch Tastatureingaben abgehört werden.

Man in the middle / Aufzeichnung Netzwerkverkehr: Bei einem Man in the middle Angriff, wird der Datenverkehr des Opfers über den Rechner des Angreifers geleitet. Beim Passwortmanager können wir aber davon ausgehen, dass der Datenverkehr hinreichend gut verschlüsselt ist. Gelingt es dem Angreifer, den Datenverkehr abzuhören, hat er grundsätzlich zwei Möglichkeiten. Man kann versuchen, die Daten im Nachhinein zu

entschlüsseln. Dabei hat man zwar normalerweise viel Zeit zur Verfügung, aber das Brechen einer Verschlüsselung kann auch mit enormen Mitteln zu lange dauern. An dieser Stelle wird im Normalfall aber auch nicht die Verschlüsselung selbst gebrochen, sondern eine Schwachstelle in der Implementierung der Verschlüsselung ausgenutzt.

Die zweite Variante ist der Einsatz eines Proxy-Servers, welcher den verschlüsselten Verkehr aufbrechen kann. Diese Technik wird häufig eingesetzt, wenn beispielsweise der Verschlüsselte Verkehr zum Internet auf Bedrohungen untersucht werden soll. Dabei muss aber beim Anwender ein Zertifikat installiert sein, welches von diesem als vertrauenswürdig eingestuft wird. Der Angreifer muss also entweder sein Opfer dazu bringen, ein Zertifikat zu installieren, oder er muss Zugriff auf einen entsprechenden Proxy-Server erlangen, welcher beispielsweise auch auf einer Firewall laufen kann.

Bei LastPass, welches bei der Dekomponierung als Beispiel herangezogen wurde, werden die Passwörter aber Ende-zu-Ende verschlüsselt. Das heisst, dass das Passwort auf dem Client verschlüsselt respektive entschlüsselt wird. Auf den Server gelangen nur die verschlüsselten Passwörter. In diesem Fall wird das Aufbrechen der Verschlüsselten Verbindung nicht zum Erfolg führen.

Die Aufzeichnung des Netzwerkverkehrs ist einfacher durchzuführen. Hier kann der Angreifer beispielsweise sein Gerät in die Netzwerkverbindung des Opfers einschleifen oder einen Port auf dem Switch spiegeln. Geht die Datenverbindung über WLAN, können auch dort alle gesendeten Daten mitgehört werden. Da aber sowohl die Übertragung selbst als auch deren Inhalt selbst verschlüsselt sind, wird dieser Angriff keinen Erfolg haben. Respektive die Entschlüsselung der Daten wird einen extrem hohen Aufwand bedingen.

Phishing Website: Während der Einführung eines Passwortmangers kann ein Phishing-Angriff sowohl auf das Masterpasswort als auch auf ein einzelnes Login erfolgen. Betrachten wir zunächst den Angriff auf das Masterpasswort. Der Benutzer wird zu diesem Zeitpunkt noch nicht sehr vertraut mit dem Web-GUI des Passwortmanagers sein. Weiss ein Angreifer von der Einführung, ist dies ein sehr guter Zeitpunkt für so einen Angriff. Mit einem entsprechend gestalteten Mail können die Benutzer auf eine entsprechende Seite geleitet und dort ihre Passwörter abgefischt werden. Kommt das Mail vermeintlich von der IT-Abteilung mit der Bitte, sich nochmals beim Passwortmanager anzumelden, wird die Erfolgsquote entsprechend hoch sein. Um diesen Angriff zu tarnen, ist auch eine Weiterleitung

nach dem Login auf die richtige Seite denkbar. So kann ein Angreifer unbemerkt an das Masterpasswort kommen.
Während der Einführung werden die Benutzer voraussichtlich auch viele Passwörter ihrer bestehenden Accounts ändern. Auch hier kann beispielsweise mit einem Mail über ungewöhnliche Aktivitäten auf einem Account der Benutzer zum Login verleitet werden.

DOS / DDOS: Ein (Distributed) Denial Of Service Angriff während der Einführung eines Passwortmanagers ist ein gutes Mittel, um die Akzeptanz des Passwortmanagers anzugreifen. Ist ein Benutzer gerade dabei, seine Passwörter einzupflegen oder den Passwortmanager einzurichten, kann eine Nichtverfügbarkeit des Dienstes die Akzeptanz beeinträchtigen. Danach ist die Chance auch höher, dass dieser Benutzer den Passwortmanager nicht nutzen wird. Somit hat der Angreifer die Chance, dass der Benutzer weiterhin alte und möglicherweise schwache Passwörter nutzt.

3 Erarbeitung von Gegenmassnahmen

Im vorangegangenen Kapitel wurde Schritt für Schritt der Aufbau eines Passwortmanagers dargestellt. Anhand dessen konnten mögliche Bedrohungen und daraus abgeleitet Schwachstellen erarbeitet werden. Zuletzt wurden dann mögliche Angriffe auf diese Schwachstellen erarbeitet.

In diesem Kapitel werden nun für alle Angriffe, welche in der Einführungsphase von Relevanz sind, Gegenmassnahmen erarbeitet. Für die Erarbeitung der Gegenmassnahmen werden die IT-Grundschutz-Bausteine des BSI (BSI, BSI IT-Grundschutz, 2020) herangezogen. Die für die Gegenmassnahmen relevanten Bausteine sind im Anhang zu finden. Diese haben den Stand vom Februar 2021. Diese Bausteine werden vom BSI immer wieder überarbeitet. Vor der Umsetzung der Gegenmassnahmen sind deshalb die Bausteine auf allfällige Änderungen zu prüfen.

Vorab gilt es zu beachten, dass je nach Angriffspunkt auch ein Dienstleister für die Sicherheit zuständig sein kann. In der Threat-Analyse wurde für den grundlegenden Aufbau LastPass als Beispiel verwendet. Dabei handelt es sich um einen Cloud-Dienst. Kommt also ein derartiger Passwortmanager zum Einsatz, hat man selbst keinen Einfluss auf die sichere Speicherung der Daten und muss dem Anbieter vertrauen.

Wird stattdessen ein Passwortmanager verwendet, welcher auch die Möglichkeit bietet, in einer eigenen Umgebung betrieben zu werden, ist man natürlich selbst für die Sicherheit verantwortlich. Dies wäre beispielsweise bei Bitwarden[5] oder KeePass[6] der Fall. Dieser Aspekt muss bei der Umsetzung der Gegenmassnahmen stets mitberücksichtigt werden. In Kapitel 3.2 Technische Massnahmen und in Kapitel **Fehler! Verweisquelle konnte nicht g efunden werden.** Zeremonie wird vertieft auf die Unterschiede zwischen einer selbst gehosteten und einer Cloud-Lösung eingegangen.

[5] https://bitwarden.com

[6] https://keepass.info

3.1 Organisatorische Massnahmen

Der Passwortmanager ist dafür gedacht, dass die Benutzer keine schwachen Passwörter mehr verwenden und für jedes Login ein anderes Passwort nutzen. Diese beiden Massnahmen, welche durch den korrekten Einsatz eines Passwortmanagers einfach umgesetzt werden können, bringen einen grossen Sicherheitsgewinn. Die Benutzer müssen also motiviert werden, den Passwortmanager auch aktiv zu nutzen. Weiterhin müssen sie bei der Überführung von bestehenden Passwörtern in den Passwortmanager diese auch entsprechend anpassen, das heisst, die Passwörter zu ändern.

Die organisatorischen Massnahmen beschränken sich aber nicht lediglich auf den einzelnen Nutzer. Die Einführung des Passwortmanagers muss auch durch die Geschäftsleitung getragen werden. Es müssen die notwendigen Mittel zur Verfügung gestellt werden und der Entscheid zur Einführung gegenüber der Belegschaft getragen werden. Zu guter Letzt muss auch die IT-Abteilung den Passwortmanager in ihre organisatorischen Abläufe aufnehmen. Für die organisatorischen Gegenmassnahmen bietet das BSI unter anderem in den «ORP: Organisation und Personal» Bausteinen die entsprechenden Massnahmen an. Die wichtigsten Punkte aus diesen Bausteinen in Bezug auf die Einführung eines Passwortmanagers werden nachfolgend beschrieben.

Die Verantwortlichkeit und Zuständigkeit für den Betrieb des Passwortmanagers muss festgelegt werden. Auf der einen Seite muss die Person (oder die Personen), welche für den Betrieb zuständig ist, ihre diesbezüglichen Aufgaben kennen. Auf der anderen Seite müssen auch die anderen Mitarbeiter im Betrieb wissen, wer für den Betrieb zuständig ist. Dies zum einen um technische Hilfestellung leisten zu können, aber auch, um allfällige Vorfälle bei der richtigen Stelle melden zu können. Der Umgang mit dem Passwortmanager muss auch in den Richtlinien für die sichere IT-Nutzung aufgenommen werden. Diese Richtlinien müssen für alle Mitarbeiter zugänglich sein. Die Mitarbeiter sind auch darauf hinzuweisen, dass die Informationssicherheit der Institution auch ausserhalb der Arbeitszeit und ausserhalb des Betriebsgeländes zu schützen ist.

Wie bei der Einführung jeglicher Software, müssen auch beim Passwortmanager organisatorische Massnahmen für dessen Einführung getroffen werden. Es muss definiert werden, wofür die Software eingesetzt werden darf und welche Daten damit verarbeitet werden dürfen. Weiter muss auch klar geregelt sein, auf welchen Geräten der Passwortmanager verwendet werden darf. Diese beiden Punkte sind insbesondere bei privater Nutzung durch die Mitarbeiter ein wichtiger Punkt. Die Installation auf privaten, nicht durch die Organisation

überwachten Geräten sollte dabei nicht erlaubt werden, da die Datensicherheit auf diesen nicht durch das Unternehmen sichergestellt werden kann. Weiter ist zu prüfen, ob man sich in Abhängigkeit zu einem Hersteller begibt.

Für den Einsatz des Passwortmanagers muss auch ein Berechtigungskonzept erstellt werden. Neben der offensichtlichen Trennung von Administratoren und Benutzern, müssen auch bei den Benutzern gewisse Trennungen vorgenommen werden. So gilt es zu definieren, welche Logins im Betrieb genutzt werden. Neben persönlichen Logins wird es auch solche geben, welche unter den Mitarbeitern geteilt werden. Hier ist ein Konzept gefragt, wer auf welches Login den Zugriff haben darf und wer Logins mit anderen Benutzern teilen darf. Hierbei muss der Grundsatz des «Least-privilege» beachtet werden. Also sowenig wie möglich und soviel wie nötig. Die erteileten Zugänge müssen dabei in geeigneter Form dokumentiert werden. Diese Dokumentation ist stets auf dem aktuellen Stand zu halten.

Ein sehr wichtiger organisatorischer Punkt ist die Sensibilisierung und Schulung der Mitarbeiter. Bei der Sensibilisierung sollte dabei nicht auf rein theoretische Massnahmen gesetzt werden. Ein eindrückliches Beispiel dazu wurde von Linus Neumann bei einem Talk[7] während des 36C3 aufgezeigt. Er erläutert dabei die Auswirkungen und Resultate aus mehreren Phishing-Kampagnen, welche für Firmen durchgeführt wurden. Dabei zeigte sich zum einen, dass doch einige Mitarbeiter mit Phishing-Kampagnen «erwischt» werden können. Es zeigte sich aber auch, dass das erlernte nach so einer Kampagne mit der Zeit auch wieder abflacht. Durch wiederholte Sensibilisierungsmassnahmen wird das Bewusstsein für IT-Sicherheit gestärkt. Bezogen auf den Passwortmanager und auf dessen Nutzen kann beispielsweise die Vorführung einer Brute-Force Attacke auf ein schwaches Passwort einen nachhaltigen Effekt haben. Neben der Sensibilisierung bedarf es aber auch einer Schulung im Umgang mit dem neuen Passwortmanager. Hier kann alleine der Fakt des bequemeren Umgangs mit Passwörtern die Mitarbeiter zum Einsatz desselben motivieren.

Sollte die Wahl auf einen Passwortmanager mit einer Cloud-Anbindung fallen, muss zusätzlich noch der Baustein «OPS.2.2 Cloud-Nutzung» in die Massnahmen integriert werden. Bevor ein derartiger Cloud-Dienst genutzt wird, müssen die rechtlichen Rahmenbedingungen für dessen Einsatz abgeklärt werden. Dabei muss auch abgeklärt werden, in welchem Land die Daten lagern.

[7] https://www.youtube.com/watch?v=BreKdM7CKnY

Weiter wird auch ein Notfallkonzept benötigt, falls der Cloud-Dienst mal nicht verfügbar sein sollte oder falls der Cloud-Anbieter selbst einem Cyberangriff zum Opfer fällt. Hier muss zum einen sichergestellt sein, dass auch ein eigenes Backup der Daten existiert und die Daten darin auch ausgelesen werden können. Zum anderen muss auch sichergestellt sein, dass die Passwörter beim Cloud-Anbieter genügend gut verschlüsselt sind.

3.2 Technische Massnahmen

Beim Aufbau des Threat-Modells wurden einige technische Schwachstellen aufgezeigt, welchen in diesem Unterkapitel mit entsprechenden technischen Massnahmen begegnet werden soll. Auch bei den technischen Massnahmen gilt, dass es nicht reicht, diese einmalig durchzuführen und es dann dabei zu belassen. Es benötigt einen stetigen Prozess, welcher fortlaufend die Wirksamkeit der Massnahmen untersucht und dementsprechende Massnahmen ableitet, getreu dem Plan-Do-Check-Act (PDCA) Prinzip.

Essentiell für den Prozess der Einführung ist eine sichere Infrastruktur. Während der Einführung wird mit den «Kronjuwelen eines Unternehmens», respektive den Zugriffen darauf, hantiert. Um zu einer sicheren Infrastruktur zu kommen, wird wiederum auf den Grundschutzkatalog des BSI referenziert. Es werden die Bausteine beleuchtet, welche massgeblich für die während der Einführung benutzte Infrastruktur sind.

Wird der Passwortmanager lokal betrieben, benötigt man einen Server.[8] Für den sicheren Betrieb des Servers wird dabei auf den Baustein «SYS.1.1» referenziert. Je nach eingesetztem Betriebssystem kommen noch die Bausteine «SYS.1.2.2» oder «SYS.1.3» hinzu.

Der Server muss an einem dafür geeigneten Ort aufgestellt und betrieben werden. Dies kann ein Rechenzentrum, ein Rechnerraum oder ein abschliessbarer Serverschrank sein. Server dürfen zudem nicht als Arbeitsplatz und im Umkehrschluss Arbeitsplätze nicht als Server genutzt werden. Für die Benutzeranmeldung am Server muss ein angemessenes Anmeldeverfahren genutzt werden. Auf dem Server müssen alle nicht benötigten Dienste deaktiviert werden. Allgemein empfiehlt es sich hier, pro Aufgabe einen Server zu Verwenden und keinen Monolithen zu bauen.

[8] Eine Ausnahme ist z.B. KeePass, welches die Passwörter in einem Datenbank-File vorhält.

Alle sicherheitsrelevanten Systemereignisse müssen protokolliert werden, dazu gehören gemäss (BSI, SYS.1.1 Allgemeiner Server, 2021) mindestens:

- Systemstarts und Reboots
- erfolgreiche und erfolglose Reboots
- fehlgeschlagene Berechtigungsprüfungen
- blockierte Datenströme (Verstösse gegen ACLs oder Firewallregeln)
- Einrichtung oder Änderungen von Benutzern, Gruppen und Berechtigungen
- Sicherheitsrelevante Fehlermeldungen (z.B. Hardwaredefekte, Überschreitung von Kapazitätsgrenzen
- Warnmeldungen von Sicherheitssystemen (z.B. Virenschutz)

Die ein- und ausgehende Kommunikation muss dabei auf die erforderlichen Protokolle und Kommunikationspartner eingeschränkt werden. Die Identität von Remotesystemen und die Integrität der Verbindungen sollte dabei soweit wie möglich kryptografisch abgesichert sein. Beim Server sollten Arbeiten, welche an diesem durchgeführt werden, nachvollziehbar dokumentiert werden. Also wer hat wann was gemacht. In regelmässigen Abständen sollte der Server einer Sicherheitsüberprüfung unterzogen werden.

Auf Seite der Clients kommt der Baustein «SYS.2.1» des BSI zum Einsatz. Je nach verwendetem Betriebssystem sind zusätzlich noch die Bausteine «SYS.2.2.2» und «SYS.2.2.3» für Windows, «SYS.2.3» für Linux und Unix und «SYS.2.4» für MacOS von Bedeutung.

Zuerst muss eine sichere Benutzerauthentisierung an den Clients sichergestellt sein. Neben einem geeigneten Authentisierungsverfahren muss auch eine Bildschirmsperre eingerichtet sein. Zum einen müssen hier die Benutzer verpflichtet werden, sich beim Verlassen des Arbeitsplatzes vom Client abzumelden. Zum anderen muss sich die Bildschirmsperre auch nach einer definierten kurzen Zeit automatisch aktivieren, falls keine Interaktion des Benutzers mehr erfolgt ist. Um die Clients stets auf dem aktuellen Stand zu halten und damit auch mit den Sicherheitsupdates der Betriebssystemhersteller zu versorgen, müssen Autoupdate-Mechanismen aktiviert sein. Eine Ausnahme kann hier gemacht werden, falls es eine regelmässige manuelle Wartung oder ein zentrales Softwareverteilungssystem gibt. Weiter müssen Clients durch den Einsatz von Schutzprogrammen gegen Schadsoftware geschützt sein. Ob ein solcher Schutz notwendig ist, kann aus dem entsprechenden Baustein des BSI zum jeweiligen Betriebssystem abgeleitet werden. Entdeckt ein

Schutzprogramm, dass ein Client infiziert wurde, muss auf diesem Client analysiert werden, ob vertrauliche Daten gesammelt, Schutzfunktionen deaktiviert oder Code aus dem Internet nachgeladen wurde.

Ein weiterer potentiell gefährdeter Bereich während der Einführung des Passwortmanagers ist das Netzwerk. Das BSI stellt uns hier die Bausteine aus der NET Reihe zur Verfügung. Für die Einführung des Passwortmanagers wird im Rahmen dieser Thesis davon ausgegangen, dass die beteiligten Clients nicht über drahtlose Verbindungen am Netzwerk angeschlossen sind. Diese Massnahme verhindert schon einige Möglichkeiten des Abhörens. Die restliche Absicherung erfolgt gemäss den Angaben aus dem Baustein «NET.1.1».
Den Grundstein der Absicherung bildet dabei die Zonierung des Netzwerks. Dabei werden mindestens drei Zonen gebildet: das interne Netz, in welche nur Vertrauenswürdige Clients eingebunden sein dürfen, eine demilitarisierte Zone für Geräte, welche von aussen erreichbar sein müssen und schliesslich noch die Zone für Aussenanbindungen wie das Internet. Die Kommunikation zwischen den einzelnen Zonen muss über geeignete Firewall-Strukturen voneinander getrennt und abgesichert sein. Neben dem eingehenden Datenverkehr muss auch der abgehende Datenverkehr auf das notwendige Minimum beschränkt sein und überwacht werden.

Beim Netzwerk muss auch wieder unterschieden werden, ob der Passwortmanager lokal oder in der Cloud betrieben wird. Bei einem lokalen Betrieb gilt es abzuwägen, inwiefern der Passwortmanager auch von extern erreichbar sein muss. Ist der Schutzbedarf des Unternehmens hoch und wird trotzdem eine externe Erreichbarkeit des Passwortmanagers, beispielsweise durch Home-Office benötigt, empfiehlt sich der Einsatz einer VPN-Architektur für derartige Zugriffe.

Zu guter Letzt muss noch der Büroarbeitsplatz betrachtet werden. Auch für diesen wird vom BSI der geeignete Baustein «INF.7» zur Verfügung gestellt. An dieser Stelle wird für den Prozess der Einführung über die Anforderungen des BSI gegangen. Im entsprechenden Baustein wird empfohlen, die Büroräume nach dem Verlassen abzusperren und die Fenster zu schliessen. Weiter wird darauf eingegangen, dass dienstliche Unterlagen geeignet aufzubewahren sind und unbefugte keine vertraulichen Informationen einsehen können.

Beim Aufbau des Threat-Modells wurden anhand von (Davis, et al., 2014) und (Giallanza, et al., 2019) Side-Channel Attacken aufgezeigt, welche rein durch die Massnahmen des BSI nicht abgewehrt werden. Vor Beginn der Arbeiten sind die verwendeten Büroräume auf

mögliche Abhör- und Beobachtungsgeräte zu untersuchen. Weiter ist darauf zu achten, dass die Fenster geschlossen und mit Gardinen oder dergleichen vor Einblicken von aussen geschützt sind.

Eine zusätzliche Massnahme zu den aus den BSI-Bausteinen abgeleiteten Abwehrmassnahmen ist noch die Zweifaktor- oder Multifaktorauthentifizierung. Dabei wird mit Hilfe eines zusätzlichen Faktors der Zugang abgesichert. Dieser Faktor kann ein Fingerabdruck, ein Time-based One-Time Password wie beispielweise vom Google-Authenticator bereitgestellt oder eine Smartcard sein. So kommt für die Logins neben dem Wissen des Passwortes noch der Besitz dazu. Dies kann sowohl zum Schutz des Passwortmanagers (je nach eingesetzter Software) als auch zum Schutz einzelner Logins (wo verfügbar) verwendet werden. Dies Massnahme erhöht die Sicherheit von Logins erheblich.

Werden alle in diesem Kapitel aufgeführten Massnahmen umgesetzt, wurden die Voraussetzung für die sichere Einführung des Passwortmanagers geschaffen. Natürlich muss hier erwähnt werden, dass durch diese Massnahmen keine allumfassende Sicherheit besteht. Insbesondere, wenn der Angreifer über grosse Ressourcen verfügt und ausreichend Zeit hat, einen Angriff vorzubereiten. So wird sich beispielsweise ein staatlicher Angreifer nicht alleine durch diese Massnahmen abhalten lassen. Auch ein sehr extremer Angriff, welcher in Form einer Erpressung oder Bedrohung des Administrators erfolgt, würde weitreichendere Massnahmen zur Abwehr benötigen.

4 Einführungszeremonie

In den vorangegangenen Kapiteln wurde ein Threat-Modell aufgebaut, um mögliche Schwachstellen aufzuzeigen. Anhand dieser erkannten Schwachstellen wurden entsprechende Gegenmassnahmen entwickelt. Wie sieht nun also die konkrete Einführungszeremonie aus? Betrachtet man die Gegenmassnahmen, zielen diese auf eine Infrastruktur ab, welche dem Grundschutz des BSI entspricht. Zusätzlich müssen die Mitarbeiter für die gefahren sensibilisiert und entsprechend geschult werden.

Was hat das jetzt aber mit einer Zeremonie zu tun? Schauen wir uns erstmal die Definition einer Zeremonie an. Sucht man bei Wikipedia nach «Zeremonie[9]», erhält man folgende Beschreibung: «Eine Zeremonie ist ein nach einem festgelegten Protokoll oder Ritus ablaufender förmlich-feierlicher Akt.» Weiter wird in dem Artikel von einem Zeremonienmeister gesprochen, welcher «... den Ablauf einer Zeremonie plant und organisiert und während der Veranstaltung darauf achtet, dass die vorgegebenen Regeln beachtet und die vorgesehenen Handlungen in der vorgeschriebenen Form und Reihenfolge durchführt werden».
Sucht man nun die Parallelen zur Einführung eines Passwortmanagers, findet man den Zeremonienmeister in der Person, welche für die Einführung des Passwortmanagers verantwortlich ist. Der förmlich-feierliche Akt, welcher nach einem festgelegten Protokoll erfolgt, ist dann der gesamte Einführungsprozess.

Kommen wir also zur eigentlichen Zeremonie. Als erstes muss eine Person bestimmt werden, welche für die Einführung des Passwortmanagers verantwortlich ist. Zu diesem Zeitpunkt gehen wir davon aus, dass die Geschäftsführung den Einsatz eines Passwortmanagers gutgeheissen und die nötigen Mittel zur Verfügung gestellt hat. Die verantwortliche Person muss nun also einen geeigneten Passwortmanager evaluieren. Hierbei gilt es auch zu berücksichtigen, ob das ausgewählte Tool lokal betrieben werden muss oder ob auch der Einsatz eines Cloud-basierten Dienstes möglich ist. Je nachdem ob das Tool in der Cloud oder lokal betrieben wird, müssen die betroffenen Systeme entsprechend den jeweiligen BSI-Bausteinen abgesichert werden.

Ist die Umgebung soweit bereit, muss der Einsatz des Passwortmanagers geplant werden. Hierzu gehört die Erfassung der Benutzer und der Zuweisung der Benutzer in Gruppen mit entsprechenden Rechten und Zugängen. Diese Zuordnungen müssen entsprechend

[9] https://de.wikipedia.org/wiki/Zeremonie

dokumentiert werden. Weiter müssen die entsprechenden Weisungen und Reglemente überarbeitet werden. Diese müssen bei der Schulung der Mitarbeiter bereit sein. Darin werden die Mitarbeiter instruiert, wie mit dem Passwortmanager umgegangen werden muss. Neben den Weisungen und Reglementen sind auch die Dokumentation der IT-Infrastruktur und des Notfallplans anzupassen und um den Passwortmanager zu ergänzen.

Wurde das geeignete Tool gewählt, wird eine Testumgebung aufgebaut und erste Tests durch die verantwortliche Person durchgeführt. Hierbei können bei Bedarf noch weitere Personen hinzugezogen werden, um den Testlauf etwas weiter zu fassen. Der Testlauf verfolgt zwei Ziele. Zum einen soll die technische Funktion überprüft werden. Also funktioniert alles so wie es soll und wurde nichts übersehen. Zum anderen erhalten so die Testpersonen Übung im Umgang mit dem Tool. Dies hilft bei der späteren Schulung der Mitarbeiter. Auch eventuelle Fragen zur Bedienung können schon hier erkannt werden und die Erkenntnisse daraus können später in die Schulung einfliessen. Die Tests dürfen aber nicht nur die reine Funktion beinhalten, auch die Notfallplanung muss zu diesem Zeitpunkt getestet werden. Nach Abschluss der Tests steht der Passwortmanager soweit bereit, dass das Rollout erfolgen kann. Hierbei darf nicht einfach die Testumgebung in Produktivumgebung umbenannt werden, sondern muss neu installiert werden.

Der Passwortmanager wird nun durch die verantwortliche Person unter Berücksichtigung aller Vorsichtsmassnahmen in Betrieb genommen. Dabei wird nach untenstehendem Protokoll vorgegangen:

	Tätigkeit	Datum	Visum
1	Der Administrator begibt sich mit zwei Zeugen in einen abhörsicheren und nicht einsehbaren Raum. ➔ Verhindert Abhörmassnahmen wie Beobachtung und Side-Channel Attacken ➔ Die Zeugen protokollieren unabhängig voneinander die Tätigkeiten des Administrators		
2	Der Administrator bestätigt, dass die Anforderungen aus den BSI-Grundschutz-Bausteinen umgesetzt wurden.		
2.1	ORP.1 Organisation		
2.2	ORP.2 Personal		
2.3	ORP.3 Sensibilisierung und Schulung		
2.4	ORP.4 Identitäts- und Berechtigungsmanagement		

2.5	APP.6 Allgemeine Software		
2.6	OPS.2.2 Cloud-Nutzung (Cloud) SYS.1.1 Allgemeiner Server (on premise)		
2.7	SYS.2.1 Allgemeiner Client		
2.8	NET.1.1 Netzarchitektur und -design		
2.9	INF.7 Büroarbeitsplatz		
3	Der Administrator geht an einen Computer, welcher mit zwei gespiegelten Bildschirmen ausgestattet ist. Dabei ist ein Bildschirm für den Administrator und der zweite für die Zeugen, damit diese die Schritte des Administrators mitverfolgen können.		
4	Der Administrator logt sich auf dem Computer ein und lädt ein aktuelles Live-Installations-Image einer Linux-Distribution mit Desktopoberfläche herunter. Die Checksumme des Downloads wird mit einem geeigneten Tool überprüft, um die Integrität sicherzustellen. Aus diesem Image wird ein bootfähiger USB-Stick erstellt. Der Computer wird mit diesem USB-Stick in eine saubere Linux Installation gestartet. ➔ Stellt sicher, dass der Computer für die Inbetriebnahme nicht kompromittiert ist ➔ Verhindert Abhörmassnahmen durch Malware		
5	Der Administrator öffnet einen Browser und geht auf die Anmeldeseite des Passwortmanagers.		
6	Der Administrator überprüft das SSL / TLS Zertifikat der Anmeldeseite auf dessen Gültigkeit. ➔ Verhindert Phishing		
7	Der Administrator generiert ein Masterpasswort, welches den Firmenrichtlinien entspricht und erstellt damit das Administratorenkonto für den Passwortmanager. Die Zeugen dürfen dabei das Passwort nicht sehen.		
8	Das Masterpasswort wird notiert und in einem blickdichten Umschlag verschlossen.		
9	Der Umschlag mit dem Passwort wird einem Notar übergeben. ➔ Stellt den Zugriff auf den Passwortmanager bei Ausfall des Administrators sicher		

Tabelle 3: Protokoll der Einführungszeremonie

Ist der Passwortmanager bereit, erfolgt eine Schulung der Mitarbeiter zur Verwendung des Passwortmangers. Während dieser Schulung sollten die Mitarbeiter für den Einsatz von sicheren Passwörtern sensibilisiert werden. Zum Schluss der Schulung werden die Mitarbeiter darüber instruiert, welche Weisungen und Reglemente angepasst wurden. Je nach Organisation der Firma müssen diese geänderten Dokumente auch noch durch die Mitarbeiter visiert oder unterschrieben werden.

5 Diskussion

Die Erwartung an die Arbeit war ein Verfahren, welches es einem Unternehmen ermöglicht, die Risiken bei der Einführung eines Passwortmanagers zu minimieren. Dabei sollten sowohl technische als auch organisatorische Massnahmen betrachtet werden.

Das Ergebnis der Thesis, die Zeremonie zur Einführung des Passwortmanagers, bietet dabei Hilfestellung in Form eines Ablaufs. Die notwendigen Voraussetzungen für die sichere Einführung lassen sich durch die Umsetzung ausgewählter Bausteine aus dem BSI-Grundschutzkatalog erreichen. Nach der Entwicklung des Threat-Modells hat sich gezeigt, dass diese ausgewählten Bausteine die Risiken schon sehr weit minimieren können. Die Minimierung der Risiken muss aber nicht zwingend durch die Umsetzung von Bausteinen aus dem BSI Grundschutzkatalog erfolgen. Hier kann durchaus auch ein anderes Framework zum Erfolg führen. Ein Informatiker mit entsprechender Erfahrung und Affinität zur Sicherheit wird einen Teil der Massnahmen wahrscheinlich schon anhand seiner Erfahrung im Bereich IT-Sicherheit umsetzen. Die Gefahr ist aber gross, dass bei einer derartigen Vorgehensweise wichtige Punkte übersehen werden. Die BSI Bausteine bieten dank ihrer Übersichtlichkeit eine gute Leitlinie, möglichst umfassend die potentiellen Risiken minimieren zu können. Auch deren freie Verfügbarkeit und ständige Aktualisierung sprechen für den Einsatz dieses Frameworks.

Im Allgemeinen lässt sich sagen, dass die Grundvoraussetzung zur sicheren Einführung eines Passwortmanagers eine sichere IT-Infrastruktur und entsprechend sensibilisierte und geschulte Mitarbeiter sind. Durch die Umsetzung der Anforderungen aus neuen Bausteinen des BSI Grundschutzkatalogs werden eben diese Voraussetzungen geschaffen. Die Zeremonie als solches stellt dabei sicher, dass eine zielführende Reihenfolge eingehalten und keine wichtigen Aspekte vergessen werden.

Die in der Thesis erarbeiteten Massnahmen sind jedoch eher allgemeingültig formuliert und zielen nicht spezifisch auf *einen* Passwortmanager ab. Jedes Tool kann hier spezifische Eigenschaften haben, auf welche bei der Einführung gesondert geachtet werden muss. Auch besteht eine Einschränkung darin, dass als Ausgangsbasis für das Threat-Modell ein serverbasierter Passwortmanager verwendet wurde. Dementsprechend wurden auch die Gegenmassnahmen für eine derartige Architektur erarbeitet. Beim Einsatz einer anderen Architektur, wie diese beispielsweise bei KeePass vorhanden ist, müssen die Massnahmen entsprechend angepasst oder überarbeitet werden. Bei KeePass ist der Ansatz, dass die

Passwortdatenbank lediglich ein File ist, welches bei gemeinsamer Nutzung unter den Benutzern synchronisiert werden muss. Es gibt hier keine Benutzerverwaltung, welche beispielsweise eine granulare Rechtevergabe ermöglichen würde. Auch kann für einen Benutzer nicht einfach der Zugang gesperrt werden. Hat er eine Kopie des Files mit der Passwortdatenbank lokal gespeichert, kann ihm der Zugang nicht entzogen werden.

Nachfolgend werden mögliche Anknüpfungspunkte für weitere Forschungen in dieser Richtung angesprochen. Denkbar wäre die Erarbeitung weiterer Massnahmen, welche einen sicheren Betrieb des Passwortmanagers sicherstellen. Beispielsweise welche Backupkonzepte hier geeignet sind oder wie sichergestellt werden kann, dass die Benutzer den Passwortmanager auch aktiv nutzen. Auch die Überprüfung der effektiven Nutzung, wie sie bei (Pearman, Zhang, Bauer, Christin, & Cranor, 2019) für gewisse Benutzer in Frage gestellt wird, könnte untersucht werden. Hier wäre sicherlich auch spannend, wie die Benutzer zur effektiveren Benutzung motiviert werden können.

Ein weiterer Anknüpfungspunkt wäre die Präzisierung der Massnahmen auf ein spezifisches Produkt oder sogar auf eine andere Architektur. Ein Ansatz, wie er von KeePass mit dem Datenbankfile gewählt wurde, kann mit entsprechend angepassten Massnahmen durchaus auch sicher betrieben werden.

6 Fazit

Die Einführung eines Passwortmanagers umfasst wesentlich mehr als lediglich die Auswahl und Installation eines Tools. Im Vorfeld sind diverse vorbereitende Massnahmen zu treffen. So muss entschieden werden, ob der Passwortmanager lokal oder in der Cloud betrieben wird. Weiter gilt es sicherzustellen, dass die IT-Infrastruktur anerkannten Sicherheitsstandards entspricht. Hierfür können ausgewählte Bausteine aus dem IT-Grundschutzkompendium des BSI herangezogen und umgesetzt werden. Auch andere Frameworks, wie beispielsweise NIST, die ISO 27000er Reihe oder COBIT, können hier zum Ziel führen.

Neben der sicheren IT-Infrastruktur bedarf es auch entsprechend geschulter und sensibilisierter Mitarbeiter. Diese müssen sich der Risiken von unsicheren Passwörtern bewusst sein und wissen, wie sie mit dem Passwortmanager umgehen müssen. Neben der Sensibilisierung muss auch der verantwortungsvolle Einsatz des Passwortmanagers durch geeignete Regelungen und Weisungen sichergestellt werden.

Auf die Forschungsfrage: «Was muss unternommen werden, damit im geschäftlichen Umfeld die Risiken bei der Einführung eines Passwortmanagers weitestgehend minimiert werden?» kann also folgendermassen geantwortet werden: Wird nach den Vorgaben aus der Zeremonie vorgegangen, werden die Risiken bei der Einführung deutlich minimiert. Dies ist insbesondere die vorhergehende, gründliche Planung, die Absicherung der IT-Infrastruktur und eine penible Einhaltung von erhöhten Sicherheitsstandards während der Einführung selbst. Eine erweiterte Hilfestellung bieten dabei ausgewählte Bausteine aus dem Grundschutzkatalog des BSI.

7 Nachwort

Die Ausarbeitung der Thesis hat mir aufgezeigt, dass selbst ein so trivial wirkendes Thema wie die Einführung eines Passwortmanagers sehr viel Arbeit bedeuten kann. Trotzdem bin ich froh um diese Erfahrung und habe einiges dabei gelernt. Genau durch diese detaillierte Betrachtung lernt man, auch auf Details zu achten, welche im Nachhinein über den Erfolg oder Misserfolg eines Projekts oder einer Arbeit entscheiden können.

Meinen ursprünglichen Zeitplan konnte ich nach einem etwas holprigen Start trotzdem gut einhalten. Vor allem werde ich bei einer nächsten derartigen Arbeit den Rahmen im Vorfeld klarer abstecken. Die Versuchung, über das Thema hinaus zu gehen und noch viele andere Aspekte zu berücksichtigen war häufig gross und hat manchmal auch ziemlich viel Zeit in Anspruch genommen, welche anschliessend wieder für das eigentliche Thema nachgeholt werden musste.

An dieser Stelle möchte ich mich bei meinem Betreuer Dr. Frank Möhle bedanken, welcher mir immer wieder gute Hinweise und Denkansätze zu meiner Thesis gegeben hat. Weitere Danksagungen gehen an Even Meier und Adrian von Escher, welche mir mit ihren Feedbacks gute Inputs geliefert haben. Und last but not least an Erika Bütler, welche mir während des ganzen Studiums den Rücken freigehalten und mir damit die nötige Konzentration für das Studium ermöglicht hat.

Peter Matijasic

Baar, März 2021

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

BSI. (Februar 2020). *BSI Grundschutz.* Abgerufen am 11. Oktober 2020 von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs/07_SYS_IT_Systeme/SYS_2_1_Allgemeiner_Client_Edition_2020.pdf?__blob=publicationFile&v=1

BSI. (2020). *BSI IT-Grundschutz*. Abgerufen am 4. Dezember 2020 von https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/bausteine_node.html

BSI. (September 2020). *Bundesamt für Sicherheit in der Informationstechnik.* Abgerufen am 4. Dezember 2020 von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=2

BSI. (Februar 2021). *SYS.1.1 Allgemeiner Server.* Abgerufen am 9. Februar 2021 von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/07_SYS_IT_Systeme/SYS_1_1_Allgemeiner_Server_Edition_2021.pdf?__blob=publicationFile&v=2

Davis, A., Rubinstein, M., Wadhwa, N., Mysore, G., Durand, F., & Freeman, W. T. (2014). The Visual Microphone: Passive Recovery of Sound from Video. *ACM Transactions on Graphics (Proc. SIGGRAPH), 4*(33), 79.

Geschonneck, A. (2014). Computer Forensik. Heidelberg: dpunkt.verlag.

Giallanza, T., Siems, T., Smith, E., Gabrielsen, E., Johnson, I., Thornton, M. A., & Larson, E. C. (Juni 2019). *ACM.* Abgerufen am 7. Januar 2021 von Keyboard Snooping from Mobile Phone Arrays with Mixed Convolutional and Recurrent Neural Networks: https://doi.org/10.1145/3328916

LastPass. (2019). *LastPass Technical Whitepaper.* Abgerufen am 22. November 2020 von https://assets.cdngetgo.com/1c/e4/e53646f14a91a7c9cb7dd7afbb61/lastpass-technical-whitepaper.pdf

Oesch, S., & Ruoti, S. (August 2020). *That Was Then, This Is Now: A Security Evaluation of Password Generation, Storage, and Autofill in Browser-Based Password Managers.* Abgerufen am 18. Dezember 2020 von https://www.usenix.org/conference/usenixsecurity20/presentation/oesch

OWASP Threat Modeling Cheat Sheet. (2020). Abgerufen am 25. Oktober 2020 von https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html

Pearman, S., Zhang, S. A., Bauer, L., Christin, N., & Cranor, F. (August 2019). *Why people (don't) use password managers effectively.* Abgerufen am 18. Dezember 2020 von https://www.usenix.org/conference/soups2019/presentation/pearman

Pohl, K., & Rupp, C. (2015). Basiswissen Requirements Engineering. Heidelberg: dpunkt.verlag.

Schultz, E. (11. November 2020). *Statista.* Abgerufen am 6. Dezember 2020 von https://de.statista.com/statistik/daten/studie/552495/umfrage/arten-von-cyberangriffen-auf-unternehmen-in-oesterreich/

Sevchenko, N., Chick, T. A., O'Riordan, P., Scanlon, T. P., & Woody, C. (Juli 2018). *Threat Modeling: A summary of available methods.* Abgerufen am 28. September 2020 von Software Engineering Institute: https://resources.sei.cmu.edu/asset_files/WhitePaper/2018_019_001_524597.pdf

Shostack, A. (2014). *Threat Modeling: Designing for Security.* Wiley.

Sutter-Somm, T. (2020). Obligationenrecht. Liberalis-Verlag.

Uceda Velez, T. (2013). *OWASP.* Abgerufen am 9. November 2020 von https://owasp.org/www-pdf-archive//APAC13_TonyUV.pdf

verizon data breach investigations report. (2020). *Verizon media.* Abgerufen am 18. Dezember 2020 von verizon data breach investigations report: https://enterprise.verizon.com/resources/de/executivebriefs/2020-dbir-executive-brief.pdf

Anhang

Die Dokumente im Anhang sind Auszüge mit den in der Thesis verwendeten Bausteinen.

Es wurden dabei jeweils nur die Seiten mit den Anforderungen übernommen.

Anhang A – ORP.1 Organisation

Beispiele:

- Unbegleitete Besucher können auf Unterlagen und Datenträger zugreifen oder Zugang zu Geräten haben, diese beschädigen oder schützenswerte Informationen ausspähen.
- Reinigungskräfte können versehentlich Steckverbindungen lösen, Wasser in Geräte laufen lassen, Unterlagen verlegen oder mit dem Abfall entsorgen.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins ORP.1 *Organisation* aufgeführt. Grundsätzlich ist die Zentrale Verwaltung für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der 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	Zentrale Verwaltung
Weitere Zuständigkeiten	Mitarbeiter, Benutzer, IT-Betrieb, Haustechnik, Institutionsleitung

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein ORP.1 *Organisation* vorrangig erfüllt werden:

ORP.1.A1 Festlegung von Verantwortlichkeiten und Regelungen [Institutionsleitung] (B)

Innerhalb einer Institution MÜSSEN alle relevanten Aufgaben und Funktionen klar definiert und voneinander abgegrenzt sein. Es MÜSSEN verbindliche Regelungen für die Informationssicherheit für die verschiedenen betrieblichen Aspekte übergreifend festgelegt werden. Die Organisationsstrukturen sowie verbindliche Regelungen MÜSSEN anlassbezogen überarbeitet werden. Die Änderungen MÜSSEN allen Mitarbeitern bekannt gegeben werden.

ORP.1.A2 Zuweisung der Zuständigkeiten [Institutionsleitung] (B)

Für alle Geschäftsprozesse, Anwendungen, IT-Systeme, Räume und Gebäude sowie Kommunikationsverbindungen MUSS festgelegt werden, wer für diese und deren Sicherheit zuständig ist. Alle Mitarbeiter MÜSSEN darüber informiert sein, insbesondere wofür sie zuständig sind und welche damit verbundenen Aufgaben sie wahrnehmen.

ORP.1.A3 Beaufsichtigung oder Begleitung von Fremdpersonen [Mitarbeiter] (B)

Institutionsfremde Personen MÜSSEN von Mitarbeitern zu den Räumen begleitet werden. Die Mitarbeiter der Institution MÜSSEN institutionsfremde Personen in sensiblen Bereichen beaufsichtigen. Die Mitarbeiter SOLLTEN dazu angehalten werden, institutionsfremde Personen in den Räumen der Institution nicht unbeaufsichtigt zu lassen.

ORP.1.A4 Funktionstrennung zwischen unvereinbaren Aufgaben (B)

Die Aufgaben und die hierfür erforderlichen Rollen und Funktionen MÜSSEN so strukturiert sein, dass unvereinbare Aufgaben wie operative und kontrollierende Funktionen auf verschiedene Personen verteilt werden. Für unvereinbare Funktionen MUSS eine Funktionstrennung festgelegt und dokumentiert sein. Auch Vertreter MÜSSEN der Funktionstrennung unterliegen.

ORP.1.A5 ENTFALLEN (B)
Diese Anforderung ist entfallen.

ORP.1.A15 Ansprechpartner zu Informationssicherheitsfragen (B)
In jeder Institution MUSS es Ansprechpartner für Sicherheitsfragen geben, die sowohl scheinbar einfache wie auch komplexe oder technische Fragen beantworten können. Die Ansprechpartner MÜSSEN allen Mitarbeitern der Institution bekannt sein. Diesbezügliche Informationen MÜSSEN in der Institution für alle verfügbar und leicht zugänglich sein.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein ORP.1 *Organisation*. Sie SOLLTEN grundsätzlich erfüllt werden.

ORP.1.A6 ENTFALLEN (S)
Diese Anforderung ist entfallen.

ORP.1.A7 ENTFALLEN (S)
Diese Anforderung ist entfallen.

ORP.1.A8 Betriebsmittel- und Geräteverwaltung [IT-Betrieb] (S)
Alle Geräte und Betriebsmittel, die Einfluss auf die Informationssicherheit haben und die zur Aufgabenerfüllung und zur Einhaltung der Sicherheitsanforderungen erforderlich sind, SOLLTEN in ausreichender Menge vorhanden sein. Es SOLLTE geeignete Prüf- und Genehmigungsverfahren vor Einsatz der Geräte und Betriebsmittel geben. Geräte und Betriebsmittel SOLLTEN in geeigneten Bestandsverzeichnissen aufgelistet werden. Um den Missbrauch von Daten zu verhindern, SOLLTE die zuverlässige Löschung oder Vernichtung von Geräten und Betriebsmitteln geregelt sein (siehe hierzu *CON.6 Löschen und Vernichten*).

ORP.1.A9 ENTFALLEN (S)
Diese Anforderung ist entfallen.

ORP.1.A10 ENTFALLEN (S)
Diese Anforderung ist entfallen.

ORP.1.A11 ENTFALLEN (S)
Diese Anforderung ist entfallen.

ORP.1.A12 ENTFALLEN (S)
Diese Anforderung ist entfallen.

ORP.1.A13 Sicherheit bei Umzügen [IT-Betrieb, Haustechnik] (S)
Vor einem Umzug SOLLTEN frühzeitig Sicherheitsrichtlinien erarbeitet bzw. aktualisiert werden. Alle Mitarbeiter SOLLTEN über die vor, während und nach dem Umzug relevanten Sicherheitsmaßnahmen informiert werden. Nach dem Umzug SOLLTE überprüft werden, ob das transportierte Umzugsgut vollständig und unbeschädigt bzw. unverändert angekommen ist.

ORP.1.A16 Richtlinie zur sicheren IT-Nutzung [Benutzer] (S)
Es SOLLTE eine Richtlinie erstellt werden, in der für alle Mitarbeiter transparent beschrieben wird, welche Rahmenbedingungen bei der IT-Nutzung eingehalten werden müssen und welche Sicherheitsmaßnahmen zu ergreifen sind. Die Richtlinie SOLLTE folgende Punkte abdecken:

- Sicherheitsziele der Institution,
- wichtige Begriffe,
- Aufgaben und Rollen mit Bezug zur Informationssicherheit,
- Ansprechpartner zu Fragen der Informationssicherheit sowie

- von den Mitarbeitern umzusetzende und einzuhaltende Sicherheitsmaßnahmen.

Die Richtlinie SOLLTE allen Benutzern zur Kenntnis gegeben werden. Jeder neue Benutzer SOLLTE die Kenntnisnahme und Beachtung der Richtlinie schriftlich bestätigen, bevor er die Informationstechnik nutzen darf. Benutzer SOLLTEN die Richtlinie regelmäßig oder nach größeren Änderungen erneut bestätigen. Die Richtlinie sollte zum Nachlesen für alle Mitarbeiter frei zugänglich abgelegt werden, beispielsweise im Intranet.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein ORP.1 *Organisation* 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.1.A14 ENTFALLEN (H)
Diese Anforderung ist entfallen.

4 Weiterführende Informationen

4.1 Wissenswertes

Für den Baustein ORP.1 *Organisation* sind keine weiterführenden Informationen vorhanden.

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.1 *Organisation* von Bedeutung.

G 0.14	Ausspähen von Informationen (Spionage)
G 0.16	Diebstahl von Geräten, Datenträgern oder Dokumenten
G 0.18	Fehlplanung oder fehlende Anpassung
G 0.19	Offenlegung schützenswerter Informationen
G 0.22	Manipulation von Informationen
G 0.25	Ausfall von Geräten oder Systemen
G 0.26	Fehlfunktion von Geräten oder Systemen
G 0.27	Ressourcenmangel
G 0.29	Verstoß gegen Gesetze oder Regelungen
G 0.38	Missbrauch personenbezogener Daten
G 0.45	Datenverlust
G 0.46	Integritätsverlust schützenswerter Informationen

Anhang B – ORP.2 Personal

2.2 Unzureichende Kenntnis über Regelungen

Regelungen festzulegen allein garantiert noch nicht, dass diese auch beachtet werden und der Betrieb störungsfrei funktionieren kann. Allen Mitarbeitern müssen die geltenden Regelungen bekannt sein, vor allem den Funktionsträgern. Ein Schaden, der entsteht, weil bestehende Regelungen nicht bekannt sind, sollte sich nicht mit den Aussagen entschuldigen lassen: „Ich habe nicht gewusst, dass ich dafür zuständig bin." oder „Ich habe nicht gewusst, wie ich zu verfahren hatte."

2.3 Sorglosigkeit im Umgang mit Informationen

Häufig ist zu beobachten, dass es in Institutionen zwar viele organisatorische und technische Sicherheitsverfahren gibt, diese jedoch durch den sorglosen Umgang der Mitarbeiter wieder umgangen werden. Ein typisches Beispiel hierfür sind etwa Zettel am Monitor, auf denen Zugangspasswörter notiert sind.

2.4 Unzureichende Qualifikationen der Mitarbeiter

Im täglichen IT-Betrieb einer Institution können viele Störungen und Fehler auftreten. Sind die verantwortlichen Mitarbeiter nicht ausreichend qualifiziert, sensibilisiert und geschult, haben sie z. B. einen veralteten Wissensstand für ihre Aufgabenerfüllung, könnten sie sicherheitsrelevante Ereignisse nicht als solche identifizieren und so Angriffe unerkannt bleiben. Auch wenn die Mitarbeiter ausreichend für die Belange der Informationssicherheit qualifiziert, sensibilisiert bzw. geschult sind, kann trotzdem nicht ausgeschlossen werden, dass sie Sicherheitsvorfälle nicht erkennen. In manchen Situationen, wie bei Personalmangel oder Kündigungen, kann es passieren, dass Mitarbeiter die Aufgaben andere Mitarbeiter vorübergehend übernehmen müssen. Hierbei können Fehler entstehen, wenn Mitarbeiter nicht die notwendigen Qualifikationen haben oder unzureichend geschult sind, um die Aufgabe zu übernehmen.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins ORP.2 *Personal* aufgeführt. Grundsätzlich ist die Personalabteilung für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festlegten 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	Personalabteilung
Weitere Zuständigkeiten	IT-Betrieb, Vorgesetzte

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein ORP.2 *Personal* vorrangig erfüllt werden:

ORP.2.A1 Geregelte Einarbeitung neuer Mitarbeiter [Vorgesetzte] (B)

Die Personalabteilung sowie die Vorgesetzten MÜSSEN dafür sorgen, dass Mitarbeiter zu Beginn ihrer Beschäftigung in ihre neuen Aufgaben eingearbeitet werden. Die Mitarbeiter MÜSSEN über bestehende Regelungen, Handlungsanweisungen und Verfahrensweisen informiert werden. Eine Checkliste und ein direkter Ansprechpartner („Pate") kann hierbei hilfreich sein und SOLLTE etabliert werden.

ORP.2.A2 Geregelte Verfahrensweise beim Weggang von Mitarbeitern [Vorgesetzte, IT-Betrieb] (B)

Verlässt ein Mitarbeiter die Institution, MUSS der Nachfolger rechtzeitig eingewiesen werden. Dies SOLLTE idealerweise durch den ausscheidenden Mitarbeiter erfolgen. Ist eine direkte Übergabe nicht möglich, MUSS vom ausscheidenden Mitarbeiter eine ausführliche Dokumentation angefertigt werden.

Außerdem MÜSSEN von ausscheidenden Mitarbeitern alle im Rahmen ihrer Tätigkeit erhaltenen Unterlagen, Schlüssel und Geräte sowie Ausweise und Zutrittsberechtigungen eingezogen werden.

Vor der Verabschiedung MUSS noch einmal auf Verschwiegenheitsverpflichtungen hingewiesen werden. Es SOLLTE besonders darauf geachtet werden, dass keine Interessenkonflikte auftreten. Um nach einem Stellenwechsel Interessenkonflikte zu vermeiden, SOLLTEN Konkurrenzverbote und Karenzzeiten vereinbart werden.

Weiterhin MÜSSEN Notfall- und andere Ablaufpläne aktualisiert werden. Alle betroffenen Stellen innerhalb der Institution, wie z. B. das Sicherheitspersonal oder die IT-Abteilung, MÜSSEN über das Ausscheiden des Mitarbeiters informiert werden. Damit alle verbundenen Aufgaben, die beim Ausscheiden des Mitarbeiters anfallen, erledigt werden, SOLLTE hier ebenfalls eine Checkliste angelegt werden . Zudem SOLLTE es einen festen Ansprechpartner der Personalabteilung geben, der den Weggang von Mitarbeitern begleitet.

ORP.2.A3 Festlegung von Vertretungsregelungen [Vorgesetzte] (B)

Die Vorgesetzten MÜSSEN dafür sorgen, dass im laufenden Betrieb Vertretungsregelungen umgesetzt werden. Dafür MUSS sichergestellt werden, dass es für alle wesentlichen Geschäftsprozesse und Aufgaben praktikable Vertretungsregelungen gibt. Bei diesen Regelungen MUSS der Aufgabenumfang der Vertretung im Vorfeld klar definiert werden. Es MUSS sichergestellt werden, dass die Vertretung über das dafür nötige Wissen verfügt. Ist dies nicht der Fall, MUSS überprüft werden, wie der Vertreter zu schulen ist oder ob es ausreicht, den aktuellen Verfahrens- oder Projektstand ausreichend zu dokumentieren. Ist es im Ausnahmefall nicht möglich, für einzelne Mitarbeiter einen kompetenten Vertreter zu benennen oder zu schulen, MUSS frühzeitig entschieden werden, ob externes Personal dafür hinzugezogen werden kann.

ORP.2.A4 Festlegung von Regelungen für den Einsatz von Fremdpersonal (B)

Wird externes Personal beschäftigt, MUSS dieses wie alle eigenen Mitarbeiter dazu verpflichtet werden, geltende Gesetze, Vorschriften und interne Regelungen einzuhalten. Fremdpersonal, das kurzfristig oder einmalig eingesetzt wird, MUSS in sicherheitsrelevanten Bereichen beaufsichtigt werden. Bei längerfristig beschäftigtem Fremdpersonal MUSS dieses wie die eigenen Mitarbeiter in seine Aufgaben eingewiesen werden. Auch für diese Mitarbeiter MUSS eine Vertretungsregelung eingeführt werden. Verlässt das Fremdpersonal die Institution, MÜSSEN Arbeitsergebnisse wie bei eigenem Personal geregelt übergeben und eventuell ausgehändigte Zugangsberechtigungen zurückgegeben werden.

ORP.2.A5 Vertraulichkeitsvereinbarungen für den Einsatz von Fremdpersonal (B)

Bevor externe Personen Zugang und Zugriff zu vertraulichen Informationen erhalten, MÜSSEN mit ihnen Vertraulichkeitsvereinbarungen in schriftlicher Form geschlossen werden. In diesen Vertraulichkeitsvereinbarungen MÜSSEN alle wichtigen Aspekte zum Schutz von institutionsinternen Informationen berücksichtigt werden.

ORP.2.A14 Aufgaben und Zuständigkeiten von Mitarbeitern [Vorgesetzte] (B)

Alle Mitarbeiter MÜSSEN dazu verpflichtet werden, geltende Gesetze, Vorschriften und interne Regelungen einzuhalten. Den Mitarbeitern MUSS der rechtliche Rahmen ihre Tätigkeit bekannt sein. Die Aufgaben und Zuständigkeiten von Mitarbeitern MÜSSEN in geeigneter Weise dokumentiert sein. Außerdem MÜSSEN alle Mitarbeiter darauf hingewiesen werden, dass alle während der Arbeit erhaltenen Informationen ausschließlich zum internen Gebrauch bestimmt sind. Den Mitarbeitern MUSS bewusstgemacht werden, die Informationssicherheit der Institution auch außerhalb der Arbeitszeit und außerhalb des Betriebsgeländes zu schützen.

ORP.2.A15 Qualifikation des Personals [Vorgesetzte] (B)
Mitarbeiter MÜSSEN regelmäßig geschult bzw. weitergebildet werden. In allen Bereichen MUSS sichergestellt werden, dass kein Mitarbeiter mit veralteten Wissensstand arbeitet. Weiterhin SOLLTE den Mitarbeitern während ihrer Beschäftigung die Möglichkeit gegeben werden, sich im Rahmen ihres Tätigkeitsfeldes weiterzubilden.

Werden Stellen besetzt, MÜSSEN die erforderlichen Qualifikationen und Fähigkeiten genau formuliert sein. Anschließend SOLLTE geprüft werden, ob diese bei den Bewerbern für die Stelle tatsächlich vorhanden sind. Es MUSS sichergestellt sein, dass Stellen nur von Mitarbeitern besetzt werden, für die sie qualifiziert sind.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein ORP.2 *Personal*. Sie SOLLTEN grundsätzlich erfüllt werden.

ORP.2.A6 ENTFALLEN (S)
Diese Anforderung ist entfallen.

ORP.2.A7 Überprüfung der Vertrauenswürdigkeit von Mitarbeitern (S)
Neue Mitarbeiter SOLLTEN auf ihre Vertrauenswürdigkeit hin überprüft werden, bevor sie eingestellt werden. Soweit möglich, SOLLTEN alle an der Personalauswahl Beteiligten kontrollieren, ob die Angaben der Bewerberinnen und Bewerber, die relevant für die Einschätzung ihrer Vertrauenswürdigkeit sind, glaubhaft sind. Insbesondere SOLLTE sorgfältig geprüft werden, ob der vorgelegte Lebenslauf korrekt, plausibel und vollständig ist. Dabei SOLLTEN auffällig erscheinende Angaben überprüft werden.

ORP.2.A8 ENTFALLEN (S)
Diese Anforderung ist entfallen.

ORP.2.A9 ENTFALLEN (S)
Diese Anforderung ist entfallen.

ORP.2.A10 ENTFALLEN (S)
Diese Anforderung ist entfallen.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein ORP.2 *Personal* 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.2.A11 ENTFALLEN (H)
Diese Anforderung ist entfallen.

ORP.2.A12 ENTFALLEN (H)
Diese Anforderung ist entfallen.

ORP.2.A13 Sicherheitsüberprüfung (H)
Im Hochsicherheitsbereich SOLLTE eine zusätzliche Sicherheitsüberprüfung zusätzlich zur grundlegenden Überprüfung der Vertrauenswürdigkeit von Mitarbeitern durchgeführt werden.

Arbeiten Mitarbeiter mit nach dem Geheimschutz klassifizierten Verschlusssachen, SOLLTEN sich die entsprechenden Mitarbeiter einer Sicherheitsüberprüfung nach dem Sicherheitsüberprüfungsgesetz (SÜG) unterziehen. Diesbezüglich SOLLTE der ISB den Geheimschutzbeauftragten bzw. Sicherheitsbevollmächtigten der Institution einbeziehen.

Anhang C – ORP.3 Sensibilisierung und Schulung zur Informationssicherheit

Systeme sich mit Schadsoftware infizieren oder sogar Geld an angebliche Geschäftspartner überweisen.

So wird beispielsweise beim sogenannten „CEO Fraud" Mitarbeitern, die Geld im Namen der Institution transferieren dürfen, ein fiktiver Auftrag des Chefs vorgegaukelt. Sie sollen für ein angeblich dringendes und vertrauliches Geschäft Transaktionen durchführen, die für das weitere Bestehen der Institution äußerst wichtig sind.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit* 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	IT-Betrieb, Vorgesetzte, Personalabteilung, Institutionsleitung

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit* vorrangig erfüllt werden:

ORP.3.A1 Sensibilisierung der Institutionsleitung für Informationssicherheit [Vorgesetzte, Institutionsleitung] (B)
Die Institutionsleitung MUSS ausreichend für Sicherheitsfragen sensibilisiert werden. Die Sicherheitskampagnen und Schulungsmaßnahmen MÜSSEN von der Institutionsleitung unterstützt werden. Vor dem Beginn eines Sensibilisierungs- und Schulungsprogramms zur Informationssicherheit MUSS die Unterstützung der Institutionsleitung eingeholt werden.

Alle Vorgesetzten MÜSSEN die Informationssicherheit unterstützen, indem sie mit gutem Beispiel vorangehen. Führungskräfte MÜSSEN die Sicherheitsvorgaben umsetzen. Hierüber hinaus MÜSSEN sie ihre Mitarbeiter auf deren Einhaltung hinweisen.

ORP.3.A2 ENTFALLEN (B)
Diese Anforderung ist entfallen.

ORP.3.A3 Einweisung des Personals in den sicheren Umgang mit IT [Vorgesetzte, Personalabteilung, IT-Betrieb] (B)
Alle Mitarbeiter und externen Benutzer MÜSSEN in den sicheren Umgang mit IT-, ICS- und IoT-Komponenten eingewiesen und sensibilisiert werden, soweit dies für ihre Arbeitszusammenhänge relevant ist. Dafür MÜSSEN verbindliche, verständliche und aktuelle Richtlinien zur Nutzung der jeweiligen Komponenten zur Verfügung stehen. Werden IT-, ICS- oder IoT-Systeme oder -Dienste in einer Weise benutzt, die den Interessen der Institution widersprechen, MUSS dies kommuniziert werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit*. Sie SOLLTEN

grundsätzlich erfüllt werden.

ORP.3.A4 Konzeption und Planung eines Sensibilisierungs- und Schulungsprogramms zur Informationssicherheit (S)
Sensibilisierungs- und Schulungsprogramme zur Informationssicherheit SOLLTEN sich an den jeweiligen Zielgruppen orientieren. Dazu SOLLTE eine Zielgruppenanalyse durchgeführt werden. Hierbei SOLLTEN Schulungsmaßnahmen auf die speziellen Anforderungen und unterschiedlichen Hintergründe fokussiert werden können.

Es SOLLTE ein zielgruppenorientiertes Sensibilisierungs- und Schulungsprogramm zur Informationssicherheit erstellt werden. Dieses Schulungsprogramm SOLLTE den Mitarbeitern alle Informationen und Fähigkeiten vermitteln, die erforderlich sind, um in der Institution geltende Sicherheitsregelungen und -maßnahmen umsetzen zu können. Es SOLLTE regelmäßig überprüft und aktualisiert werden.

ORP.3.A5 ENTFALLEN (S)
Diese Anforderung ist entfallen.

ORP.3.A6 Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit (S)
Alle Mitarbeiter SOLLTEN entsprechend ihren Aufgaben und Verantwortlichkeiten zu Informationssicherheitsthemen geschult werden.

ORP.3.A7 Schulung zur Vorgehensweise nach IT-Grundschutz (S)
Informationssicherheitsbeauftragte SOLLTEN mit dem IT-Grundschutz vertraut sein. Wurde ein Schulungsbedarf identifiziert, SOLLTE eine geeignete IT-Grundschutz-Schulung geplant werden. Für die Planung einer Schulung SOLLTE der Online-Kurs des BSI zum IT-Grundschutz berücksichtigt werden. Innerhalb der Schulung SOLLTE die Vorgehensweise anhand praxisnaher Beispiele geübt werden. Es SOLLTE geprüft werden, ob die Informationssicherheitsbeauftragten sich zu einem BSI IT-Grundschutz-Praktiker qualifizieren lassen sollten.

ORP.3.A8 Messung und Auswertung des Lernerfolgs [Personalabteilung] (S)
Die Lernerfolge im Bereich Informationssicherheit SOLLTEN zielgruppenbezogen gemessen und ausgewertet werden, um festzustellen, inwieweit die in den Sensibilisierungs- und Schulungsprogrammen zur Informationssicherheit beschriebenen Ziele erreicht sind. Die Messungen SOLLTEN sowohl quantitative als auch qualitative Aspekte der Sensibilisierungs- und Schulungsprogramme zur Informationssicherheit berücksichtigen. Die Ergebnisse SOLLTEN bei der Verbesserung des Sensibilisierungs- und Schulungsangebots zur Informationssicherheit in geeigneter Weise einfließen.

Der Informationssicherheitsbeauftragte SOLLTE sich regelmäßig mit der Personalabteilung und den anderen für die Sicherheit relevanten Ansprechpartnern (Datenschutz, Gesundheits- und Arbeitsschutz, Brandschutz etc.) über die Effizienz der Aus- und Weiterbildung austauschen.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit* 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.3.A9 Spezielle Schulung von exponierten Personen und Institutionen (H)
Besonders exponierte Personen SOLLTEN vertiefende Schulungen in Hinblick auf mögliche Gefährdungen sowie geeignete Verhaltensweisen und Vorsichtsmaßnahmen erhalten.

Anhang D – ORP.4 Identitäts- und Berechtigungsmanagement

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

Anhang E – OPS.2.2 Cloud-Nutzung

2.12 Ausfall der IT-Systeme eines Cloud-Diensteanbieters

Bei einem Cloud-Diensteanbieter können die dort betriebenen Prozesse, IT-Systeme und Anwendungen teilweise oder ganz ausfallen, wovon folglich auch der Cloud-Kunde betroffen ist. Werden die Mandanten unzureichend voneinander getrennt, kann auch ein ausgefallenes IT-System, das nicht dem Cloud-Kunden zugeordnet ist, dazu führen, dass der Cloud-Kunde seine vertraglich zugesicherte Dienstleistung nicht mehr abrufen kann. Ähnliche Probleme ergeben sich, wenn die Anbindung zwischen Cloud-Diensteanbieter und -Kunde ausfällt oder wenn die genutzte Cloud-Computing-Plattform erfolgreich angegriffen wird.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.2.2 *Cloud-Nutzung* aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der 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 Erfüllung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Fachverantwortliche, Datenschutzbeauftragter, Institutionsleitung, Personalabteilung

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein OPS.2.2 *Cloud-Nutzung* vorrangig erfüllt werden:

OPS.2.2.A1 Erstellung einer Strategie für die Cloud-Nutzung [Fachverantwortliche, Institutionsleitung, Datenschutzbeauftragter] (B)

Eine Strategie für die Cloud-Nutzung MUSS erstellt werden. Darin MÜSSEN Ziele, Chancen und Risiken definiert werden, die die Institution mit der Cloud-Nutzung verbindet. Zudem MÜSSEN die rechtlichen und organisatorischen Rahmenbedingungen sowie die technischen Anforderungen untersucht werden, die sich aus der Nutzung von Cloud-Diensten ergeben. Die Ergebnisse dieser Untersuchung MÜSSEN in einer Machbarkeitsstudie dokumentiert werden.

Es MUSS festgelegt werden, welche Dienste in welchem Bereitstellungsmodell zukünftig von einem Cloud-Diensteanbieter bezogen werden sollen. Zudem MUSS sichergestellt werden, dass bereits in der Planungsphase zur Cloud-Nutzung alle grundlegenden technischen und organisatorischen Sicherheitsaspekte ausreichend berücksichtigt werden.

Für den geplanten Cloud-Dienst SOLLTE eine grobe individuelle Sicherheitsanalyse durchgeführt werden. Diese SOLLTE wiederholt werden, wenn sich technische und organisatorische Rahmenbedingungen wesentlich verändern. Für größere Cloud-Projekte SOLLTE zudem eine Roadmap erarbeitet werden, die festlegt, wann und wie ein Cloud-Dienst eingeführt wird.

OPS.2.2.A2 Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung [Fachverantwortliche] (B)

Auf Basis der Strategie für die Cloud-Nutzung MUSS eine Sicherheitsrichtlinie für die Cloud-Nutzung erstellt werden. Sie MUSS konkrete Sicherheitsvorgaben beinhalten, mit denen sich Cloud-Dienste innerhalb der Institution umsetzen lassen. Außerdem MÜSSEN darin spezielle

Sicherheitsanforderungen an den Cloud-Diensteanbieter sowie das festgelegte Schutzniveau für Cloud-Dienste hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit dokumentiert werden. Wenn Cloud-Dienste internationaler Anbieter genutzt werden, MÜSSEN die speziellen länderspezifischen Anforderungen und gesetzlichen Bestimmungen berücksichtigt werden.

OPS.2.2.A3 Service-Definition für Cloud-Dienste durch den Cloud-Kunden [Fachverantwortliche] (B)

Für jeden Cloud-Dienst MUSS eine Service-Definition durch den Cloud-Kunden erarbeitet werden. Zudem SOLLTEN alle geplanten und genutzten Cloud-Dienste dokumentiert werden.

OPS.2.2.A4 Festlegung von Verantwortungsbereichen und Schnittstellen [Fachverantwortliche] (B)

Basierend auf der Service-Definition für Cloud-Dienste MUSS der Cloud-Kunde alle relevanten Schnittstellen und Verantwortlichkeiten für die Cloud-Nutzung identifizieren und dokumentieren. Es MUSS klar erkennbar sein, wie die Verantwortungsbereiche zwischen Cloud-Diensteanbieter und -Kunde voneinander abgegrenzt sind.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein OPS.2.2 *Cloud-Nutzung*. Sie SOLLTEN grundsätzlich erfüllt werden.

OPS.2.2.A5 Planung der sicheren Migration zu einem Cloud-Dienst [Fachverantwortliche] (S)

Bevor zu einem Cloud-Dienst migriert wird, SOLLTE durch den Cloud-Kunden ein Migrationskonzept erstellt werden. Dafür SOLLTEN zunächst organisatorische Regelungen sowie die Aufgabenverteilung festgelegt werden. Zudem SOLLTEN bestehende Betriebsprozesse hinsichtlich der Cloud-Nutzung identifiziert und angepasst werden. Es SOLLTE sichergestellt werden, dass die eigene IT ausreichend im Migrationsprozess berücksichtigt wird. Auch SOLLTEN die Verantwortlichen ermitteln, ob die Mitarbeiter der Institution zusätzlich geschult werden sollten.

OPS.2.2.A6 Planung der sicheren Einbindung von Cloud-Diensten (S)

Bevor ein Cloud-Dienst genutzt wird, SOLLTE sorgfältig geplant werden, wie er in die IT der Institution eingebunden werden soll. Hierfür SOLLTE mindestens geprüft werden, ob Anpassungen der Schnittstellen, der Netzanbindung, des Administrationsmodells sowie des Datenmanagementmodells notwendig sind. Die Ergebnisse SOLLTEN dokumentiert und regelmäßig aktualisiert werden.

OPS.2.2.A7 Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung (S)

Auf Grundlage der identifizierten Sicherheitsanforderungen (siehe OPS.2.2.A2 *Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung*) SOLLTE durch den Cloud-Kunden ein Sicherheitskonzept für die Nutzung von Cloud-Diensten erstellt werden.

OPS.2.2.A8 Sorgfältige Auswahl eines Cloud-Diensteanbieters [Institutionsleitung] (S)

Basierend auf der Service-Definition für den Cloud-Dienst SOLLTE durch den Cloud-Kunden ein detailliertes Anforderungsprofil für einen Cloud-Diensteanbieter erstellt werden. Eine Leistungsbeschreibung und ein Lastenheft SOLLTEN erstellt werden. Für die Bewertung eines Cloud-Diensteanbieters SOLLTEN auch ergänzende Informationsquellen herangezogen werden. Ebenso SOLLTEN verfügbare Service-Beschreibungen des Cloud-Diensteanbieters sorgfältig geprüft und hinterfragt werden.

OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter [Institutionsleitung] (S)

Die vertraglichen Regelungen zwischen dem Cloud-Kunden und dem Cloud-Diensteanbieter SOLLTEN in Art, Umfang und Detaillierungsgrad dem Schutzbedarf der Informationen angepasst sein, die im Zusammenhang mit der Cloud-Nutzung stehen. Es SOLLTE geregelt werden, an welchem Standort der

Cloud-Diensteanbieter seine Leistung erbringt. Zusätzlich SOLLTEN Eskalationsstufen und Kommunikationswege zwischen der Institution und dem Cloud-Diensteanbieter definiert werden. Auch SOLLTE vereinbart werden, wie die Daten der Institution sicher zu löschen sind. Ebenso SOLLTEN Kündigungsregelungen schriftlich fixiert werden. Der Cloud-Diensteanbieter SOLLTE alle Subunternehmer offenlegen, die er für den Cloud-Dienst benötigt.

OPS.2.2.A10 Sichere Migration zu einem Cloud-Dienst [Fachverantwortliche] (S)

Die Migration zu einem Cloud-Dienst SOLLTE auf Basis des erstellten Migrationskonzeptes erfolgen. Während der Migration SOLLTE überprüft werden, ob das Sicherheitskonzept für die Cloud-Nutzung an potenzielle neue Anforderungen angepasst werden muss. Auch SOLLTEN alle Notfallvorsorgemaßnahmen vollständig und aktuell sein.

Die Migration zu einem Cloud-Dienst SOLLTE zunächst in einem Testlauf überprüft werden. Ist der Cloud-Dienst in den produktiven Betrieb übergegangen, SOLLTE abgeglichen werden, ob der Cloud-Diensteanbieter die definierten Anforderungen des Cloud-Kunden erfüllt.

OPS.2.2.A11 Erstellung eines Notfallkonzeptes für einen Cloud-Dienst (S)

Für die genutzten Cloud-Dienste SOLLTE durch den Cloud-Kunden ein Notfallkonzept erstellt werden. Es SOLLTE alle notwendigen Angaben zu Zuständigkeiten und Ansprechpartnern enthalten. Zudem SOLLTEN detaillierte Regelungen hinsichtlich der Datensicherung getroffen werden. Auch Vorgaben zu redundant auszulegenden Management-Tools und Schnittstellensystemen SOLLTEN festgehalten sein.

OPS.2.2.A12 Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb (S)

Alle für die eingesetzten Cloud-Dienste erstellten Dokumentationen und Richtlinien SOLLTEN durch den Cloud-Kunden regelmäßig aktualisiert werden. Der Cloud-Kunde SOLLTE außerdem periodisch kontrollieren, ob der Cloud-Diensteanbieter die vertraglich zugesicherten Leistungen erbringt. Auch SOLLTEN sich der Cloud-Diensteanbieter und der Cloud-Kunde nach Möglichkeit regelmäßig abstimmen. Ebenso SOLLTE geplant und geübt werden, wie auf Systemausfälle zu reagieren ist.

OPS.2.2.A13 Nachweis einer ausreichenden Informationssicherheit bei der Cloud-Nutzung (S)

Der Cloud-Kunde SOLLTE sich vom Cloud-Diensteanbieter regelmäßig nachweisen lassen, dass die vereinbarten Sicherheitsanforderungen erfüllt sind. Der Nachweis SOLLTE auf einem international anerkannten Regelwerk basieren (z. B. IT-Grundschutz, ISO/IEC 27001, Anforderungskatalog Cloud Computing (C5), Cloud Controls Matrix der Cloud Security Alliance). Der Cloud-Kunde SOLLTE prüfen, ob der Geltungsbereich und Schutzbedarf die genutzten Cloud-Dienste erfasst.

Nutzt ein Cloud-Diensteanbieter Subunternehmer, um die Cloud-Dienste zu erbringen, SOLLTE er dem Cloud-Kunden regelmäßig nachweisen, dass diese die notwendigen Audits durchführen.

OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses [Fachverantwortliche, Institutionsleitung] (S)

Wenn das Dienstleistungsverhältnis mit einem Cloud-Diensteanbieter beendet wird, SOLLTE sichergestellt sein, dass dadurch die Geschäftstätigkeit oder die Fachaufgaben des Cloud-Kunden nicht beeinträchtigt wird. Der Vertrag mit dem Cloud-Diensteanbieter SOLLTE regeln, wie das Dienstleistungsverhältnis geordnet aufgelöst werden kann.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein OPS.2.2 *Cloud-Nutzung* 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.

OPS.2.2.A15 Sicherstellung der Portabilität von Cloud-Diensten [Fachverantwortliche] (H)

Der Cloud-Kunde SOLLTE alle Anforderungen definieren, die es ermöglichen, einen Cloud-Diensteanbieter zu wechseln oder den Cloud-Dienst bzw. die Daten in die eigene IT-Infrastruktur zurückzuholen. Zudem SOLLTE der Cloud-Kunde regelmäßig Portabilitätstests durchführen. Im Vertrag mit dem Cloud-Diensteanbieter SOLLTEN Vorgaben festgehalten werden, mit denen sich die notwendige Portabilität gewährleisten lässt.

OPS.2.2.A16 Durchführung eigener Datensicherungen [Fachverantwortliche] (H)

Der Cloud-Kunde SOLLTE prüfen, ob, zusätzlich zu den vertraglich festgelegten Datensicherungen des Cloud-Diensteanbieters, eigene Datensicherungen erstellt werden sollen. Zudem SOLLTE er detaillierte Anforderungen an einen Backup-Service erstellen.

OPS.2.2.A17 Einsatz von Verschlüsselung bei Cloud-Nutzung (H)

Wenn Daten durch einen Cloud-Diensteanbieter verschlüsselt werden, SOLLTE vertraglich geregelt werden, welche Verschlüsselungsmechanismen und welche Schlüssellängen eingesetzt werden dürfen. Wenn eigene Verschlüsselungsmechanismen genutzt werden, SOLLTE ein geeignetes Schlüsselmanagement sichergestellt sein. Bei der Verschlüsselung SOLLTEN die eventuellen Besonderheiten des gewählten Cloud-Service-Modells berücksichtigt werden.

OPS.2.2.A18 Einsatz von Verbunddiensten [Fachverantwortliche] (H)

Es SOLLTE geprüft werden, ob bei einem Cloud-Nutzungs-Vorhaben Verbunddienste (Federation Services) eingesetzt werden.

Es SOLLTE sichergestellt sein, dass in einem SAML (Security Assertion Markup Language)-Ticket nur die erforderlichen Informationen an den Cloud-Diensteanbieter übertragen werden. Die Berechtigungen SOLLTEN regelmäßig überprüft werden, sodass nur berechtigten Benutzern ein SAML-Ticket ausgestellt wird.

OPS.2.2.A19 Sicherheitsüberprüfung von Mitarbeitern [Personalabteilung] (H)

Mit externen Cloud-Diensteanbietern SOLLTE vertraglich vereinbart werden, dass in geeigneter Weise überprüft wird, ob das eingesetzte Personal qualifiziert und vertrauenswürdig ist. Dazu SOLLTEN gemeinsam Kriterien festgelegt werden.

4 Weiterführende Informationen

4.1 Wissenswertes

Das BSI beschreibt in seiner Publikation „Anforderungskatalog Cloud Computing (C5)“ Kriterien zur Beurteilung der Informationssicherheit von Cloud-Diensten.

Die Cloud Security Alliance (CSA) gibt in ihrer Publikationen „Security Guidance for Critical Areas of Focus in Cloud Computing“ Empfehlungen zur Nutzung von Cloud-Diensten.

Das National Institute of Standards and Technology (NIST) gibt in der NIST Special Publication 800-144 „Guidelines on Security and Privacy in Public Cloud Computing“ Empfehlungen zur Nutzung von Cloud-Diensten.

Die European Union Agency for Network and Information Security (ENISA) hat folgendes weiterführendes Dokument „Cloud Computing: Benefits, Risks and Recommendations for Information Security“ zum Themenfeld Cloud Computing veröffentlicht.

Das Infomation Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ in Kapitel SC 2 – Cloud Computing – Vorgaben zur Nutzung von Cloud-Diensten.

Anhang F – APP.6 Allgemeine Software

oder die Software schlicht über den Wartungszeitraum hinaus verwendet wird. Auch können Verstöße gegen die Lizenzbestimmungen dazu führen, dass z.B. (Auto-)Update-Mechanismen deaktiviert werden und somit die Software nicht mehr gewartet wird.

2.5 Datenverlust durch fehlerhafte Nutzung von Software

Durch falsch benutzte Software können Mitarbeiter Daten versehentlich löschen oder so verändern, dass diese unbrauchbar werden. Dadurch können ganze Geschäftsprozesse blockiert werden. Auch wenn Funktionen zur Verschlüsselung fehlerhaft benutzt werden, könnten die Daten zwar noch vorhanden sein, aber nicht mehr entschlüsselt werden. In diesem Fall können die Daten nicht mehr oder nur noch mit erhöhtem Aufwand wiederhergestellt werden.

2.6 Mangelhafte Ressourcen für die Ausführung von Software

Falls IT-Systeme über ungenügend Ressourcen verfügen, um die Software auszuführen, kann das die Bearbeitungs- und Reaktionszeit für die Benutzer erheblich erhöhen. Im schlimmsten Fall kann die Software auf solch einem System nicht ausgeführt werden. Das kann Geschäftsprozesse erheblich unterbrechen.

2.7 Nichtbeachtung von Anforderungen der Benutzer

Unabhängig davon, ob eine Software die funktionalen Anforderungen erfüllt, kann sie von den Benutzern nicht akzeptiert werden, wenn sie z. B. umständlich und somit benutzerunfreundlich zu bedienen ist. Dies kann wiederum dazu führen, dass Benutzer auf alternative Formen der Bearbeitung zurückgreifen und dafür anderweitige IT-Systeme oder Software zweckentfremden. So könnten z.B. private IT-Systeme ohne Abstimmung mit dem IT-Betrieb eingesetzt werden. Diese alternativen Formen der Bearbeitung entstehen dabei selten unter Gesichtspunkten der Informationssicherheit und stellen somit ein erhöhtes Risiko dar.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.6 *Allgemeine Software* aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der 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 Erfüllung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Fachverantwortliche, Beschaffungsstelle

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein APP.6 *Allgemeine Software* vorrangig erfüllt werden:

APP.6.A1 Planung des Software-Einsatzes [Fachverantwortliche] (B)
Bevor eine Institution eine (neue) Software einführt, MUSS sie entscheiden,

- wofür die Software genutzt und welche Informationen damit verarbeitet werden sollen,
- wie die Benutzer bei der Anforderungserhebung beteiligt und bei der Einführung unterstützt

werden sollen,

- wie die Software an weitere Anwendungen und IT-Systeme über welche Schnittstellen angebunden wird,
- auf welchen IT-Systemen die Software ausgeführt werden soll und welche Ressourcen zur Ausführung der Software erforderlich sind, sowie
- ob sich die Institution in Abhängigkeit zu einem Hersteller begibt, wenn sie diese Software einsetzt.

Hierbei MÜSSEN bereits Sicherheitsaspekte berücksichtigt werden. Zusätzlich MUSS die Institution die Zuständigkeiten für fachliche Betreuung, Freigabe und betriebliche Administration schon im Vorfeld klären und festlegen. Die Zuständigkeiten MÜSSEN dokumentiert und bei Bedarf aktualisiert werden.

APP.6.A2 Erstellung eines Anforderungskatalogs für Software [Fachverantwortliche] (B)

Auf Basis der Ergebnisse der Planung MÜSSEN die Anforderungen an die Software in einem Anforderungskatalog erhoben werden. Der Anforderungskatalog MUSS dabei die grundlegenden funktionalen Anforderungen umfassen. Darüber hinaus MÜSSEN die nichtfunktionalen Anforderungen und hier insbesondere die Sicherheitsanforderungen in den Anforderungskatalog integriert werden.

Hierbei MÜSSEN sowohl die Anforderungen von den Fachverantwortlichen als auch vom IT-Betrieb berücksichtigt werden. Insbesondere MÜSSEN auch die rechtlichen Anforderungen, die sich aus dem Kontext der zu verarbeitenden Daten ergeben, berücksichtigt werden.

Der fertige Anforderungskatalog SOLLTE mit allen betroffenen Fachabteilungen abgestimmt werden.

APP.6.A3 Sichere Beschaffung von Software [Beschaffungsstelle] (B)

Wenn Software beschafft wird, MUSS auf Basis des Anforderungskatalog eine geeignete Software ausgewählt werden. Die ausgewählte Software MUSS aus vertrauenswürdigen Quellen beschafft werden. Die vertrauenswürdige Quelle SOLLTE eine Möglichkeit bereitstellen, die Software auf Integrität zu überprüfen.

Darüber hinaus SOLLTE die Software mit einem geeigneten Wartungsvertrag oder einer vergleichbaren Zusage des Herstellers oder Software-Anbieters beschafft werden. Diese Verträge oder Zusagen SOLLTEN insbesondere garantieren, dass auftretende Sicherheitslücken und Schwachstellen der Software während des gesamten Nutzungszeitraums zeitnah behoben werden.

APP.6.A4 Regelung für die Installation und Konfiguration von Software [Fachverantwortliche] (B)

Die Installation und Konfiguration der Software MUSS durch den IT-Betrieb so geregelt werden, dass

- die Software nur mit dem geringsten notwendigen Funktionsumfang installiert und ausgeführt wird,
- die Software mit den geringsten möglichen Berechtigungen ausgeführt wird,
- die datensparsamsten Einstellungen (in Bezug auf die Verarbeitung von personenbezogenen Daten) konfiguriert werden sowie
- alle relevanten Sicherheitsupdates und -patches installiert sind, bevor die Software produktiv eingesetzt wird.

Hierbei MÜSSEN auch abhängige Komponenten (u. a. Laufzeitumgebungen, Bibliotheken, Schnittstellen sowie weitere Programme) mitbetrachtet werden. Der IT-Betrieb MUSS in Abstimmung mit dem Fachverantwortlichen festlegen, wer die Software wie installieren darf. Idealerweise SOLLTE Software immer zentral durch den IT-Betrieb installiert werden. Ist es erforderlich, dass die Software (teilweise) manuell installiert wird, dann MUSS der IT-Betrieb eine Installationsanweisung erstellen, in der klar geregelt wird, welche Zwischenschritte zur Installation durchzuführen und welche Konfigurationen vorzunehmen sind.

Darüber hinaus MUSS der IT-Betrieb regeln, wie die Integrität der Installationsdateien überprüft wird. Falls zu einem Installationspaket digitale Signaturen oder Prüfsummen verfügbar sind, MÜSSEN mit diesen die Integrität überprüft werden.

Sofern erforderlich, SOLLTE der IT-Betrieb eine sichere Standardkonfiguration der Software festlegen, mit der die Software konfiguriert wird. Die Standardkonfiguration SOLLTE dokumentiert werden.

APP.6.A5 Sichere Installation von Software (B)

Software MUSS entsprechend der Regelung für die Installation auf den IT-Systemen installiert werden. Dabei MÜSSEN ausschließlich unveränderte Versionen der freigegebenen Software verwendet werden.

Wird von diesen Anweisungen abgewichen, MUSS dies durch den Vorgesetzten und den IT-Betrieb genehmigt werden und entsprechend dokumentiert werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein APP.6 *Allgemeine Software*. Sie SOLLTEN grundsätzlich erfüllt werden.

APP.6.A6 Berücksichtigung empfohlener Sicherheitsanforderungen (S)

Die Institution SOLLTE die nachfolgenden Sicherheitsanforderungen im Anforderungskatalog für die Software berücksichtigen:

- Die Software SOLLTE generelle Sicherheitsfunktionen wie Protokollierung und Authentifizierung umfassen, die im Anwendungskontext erforderlich sind.
- Die Software SOLLTE es ermöglichen, die Härtungsfunktionen der Einsatzumgebung zu nutzen. Hierbei SOLLTEN insbesondere die Härtungsfunktionen des geplanten Betriebssystems und der geplanten Ausführungsumgebung berücksichtigt werden.
- Wenn durch die Software Informationen über ungesicherte, öffentliche Netze übertragen werden, dann SOLLTE die Software sichere Verschlüsselungsfunktionen einsetzen, die dem Stand der Technik entsprechen. Darüber hinaus SOLLTEN die übertragenen Daten auf Integrität überprüft werden, indem Prüfsummen oder digitale Signaturen eingesetzt werden.
- Verwendet die Software Zertifikate, dann SOLLTE sie die Möglichkeit bieten, die Zertifikate transparent darzustellen. Zudem SOLLTE es möglich sein, Zertifikate zu sperren, ihnen das Vertrauen zu entziehen oder eigene Zertifikate zu ergänzen.

Die sich aus den Sicherheitsanforderungen ergebenden Funktionen der Software SOLLTEN im Betrieb verwendet werden.

APP.6.A7 Auswahl und Bewertung potentieller Software [Fachverantwortliche, Beschaffungsstelle] (S)

Anhand des Anforderungskatalogs SOLLTEN die am Markt erhältlichen Produkte gesichtet werden. Sie SOLLTEN mithilfe einer Bewertungsskala miteinander verglichen werden. Danach SOLLTE untersucht werden, ob die Produkte aus der engeren Wahl die Anforderungen der Institution erfüllen. Gibt es mehrere Alternativen für Produkte, SOLLTEN auch die Nutzerakzeptanz und der zusätzliche Aufwand für z. B. Schulungen oder die Migration berücksichtigt werden. Die Fachverantwortlichen SOLLTEN gemeinsam mit dem IT-Betrieb anhand der Bewertungen und Testergebnisse ein geeignetes Softwareprodukt auswählen.

APP.6.A8 Regelung zur Verfügbarkeit der Installationsdateien (S)

Der IT-Betrieb SOLLTE die Verfügbarkeit der Installationsdateien sicherstellen, um die Installation reproduzieren zu können. Hierzu SOLLTE er

- die Installationsdateien geeignet sichern oder
- die Verfügbarkeit der Installationsdateien durch die Bezugsquelle (z. B. App-Store) sicherstellen.

Diese Regelung SOLLTE im Datensicherungskonzept der Institution integriert werden.

APP.6.A9 Inventarisierung von Software (S)

Software SOLLTE inventarisiert werden. In einem Bestandsverzeichnis SOLLTE dokumentiert werden, auf welchen Systemen die Software unter welcher Lizenz eingesetzt wird. Bei Bedarf SOLLTEN zusätzlich die sicherheitsrelevanten Einstellungen mit erfasst werden. Software SOLLTE nur mit Lizenzen eingesetzt werden, die dem Einsatzzweck und den vertraglichen Bestimmungen entsprechen. Die Lizenz SOLLTE den gesamten vorgesehenen Nutzungszeitraum der Software abdecken.

Wird von einer Standardkonfiguration abgewichen, SOLLTE dies dokumentiert werden. Das Bestandsverzeichnis SOLLTE anlassbezogen durch den IT-Betrieb aktualisiert werden, insbesondere wenn Software installiert wird.

Das Bestandsverzeichnis SOLLTE so aufgebaut sein, dass bei Sicherheitsvorfällen eine schnelle Gesamtübersicht mit den notwendigen Details ermöglicht wird.

APP.6.A10 Erstellung einer Sicherheitsrichtlinie für den Einsatz der Software (S)

Die Institution SOLLTE die Regelungen, die festlegen, wie die Software eingesetzt und betrieben wird, in einer Sicherheitsrichtlinie zusammenfassen. Die Richtlinie SOLLTE allen relevanten Verantwortlichen, Zuständigen und Mitarbeitern der Institution bekannt sein und die Grundlage für ihre Arbeit und ihr Handeln bilden. Inhaltlich SOLLTE die Richtlinie auch ein Benutzer-Handbuch umfassen, dass erläutert, wie die Software zu benutzen und zu administrieren ist.

Es SOLLTE regelmäßig und stichprobenartig überprüft werden, ob die Mitarbeiter sich an die Richtlinie halten. Die Richtlinie SOLLTE regelmäßig aktualisiert werden.

APP.6.A11 Verwendung von Plug-ins und Erweiterungen (S)

Es SOLLTEN nur unbedingt notwendige Plug-ins und Erweiterungen installiert werden. Werden Erweiterungen eingesetzt, SOLLTE die Software die Möglichkeit bieten, Erweiterungen zu konfigurieren und abzuschalten.

APP.6.A12 Geregelte Außerbetriebnahme von Software [Fachverantwortliche] (S)

Wenn Software außer Betrieb genommen wird, SOLLTE der IT-Betrieb mit den Fachverantwortlichen regeln, wie dies im Detail durchzuführen ist. Ebenfalls SOLLTE geregelt werden, wie die Benutzer hierüber zu informieren sind. Hierbei SOLLTE geklärt werden, ob die funktionalen Anforderungen fortbestehen (z. B. zur Bearbeitung von Fachaufgaben). Ist dies der Fall, dann SOLLTE geregelt werden, wie die benötigten Funktionen der betroffenen Software weiter verfügbar sein werden.

APP.6.A13 Deinstallation von Software (S)

Wird Software deinstalliert, SOLLTEN alle angelegten und nicht mehr benötigten Dateien entfernt werden. Alle Einträge in Systemdateien, die für das Produkt vorgenommen wurden und nicht länger benötigt werden, SOLLTEN rückgängig gemacht werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein APP.6 *Allgemeine Software* 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.

APP.6.A14 Nutzung zertifizierter Software (H)

Bei der Beschaffung von Software SOLLTE festgelegt werden, ob Zusicherungen des Herstellers, Vertreibers und Anbieters über implementierte Sicherheitsfunktionen als ausreichend vertrauenswürdig anerkannt werden kann. Ist dies nicht der Fall, SOLLTE eine Zertifizierung der Anwendung z. B. nach Common Criteria als Entscheidungskriterium herangezogen werden. Stehen mehrere Produkte zur Auswahl, SOLLTEN insbesondere dann Sicherheitszertifikate berücksichtigt werden, wenn der evaluierte Funktionsumfang die Mindestfunktionalität (weitestgehend) umfasst und die Mechanismenstärke dem Schutzbedarf entspricht.

Anhang G – SYS.1.1 Allgemeiner Server

wenn sie nicht mehr aktualisiert werden. Sind die installierten Anwendungen und Dienste unbekannt, ist der Institution gar nicht bewusst, dass diese ebenfalls aktualisiert werden müssen. Auf diese Weise können sie leicht zum Einfallstor für Angreifer werden.

2.4 Überlastung von Servern

Wenn Server nicht ausreichend dimensioniert sind, ist irgendwann der Punkt erreicht, an dem sie den Anforderungen der Institution nicht mehr gerecht werden. Je nach Art der betroffenen Systeme kann dies eine Vielzahl von negativen Auswirkungen haben. So können die Server oder Dienste beispielsweise vorübergehend nicht verfügbar sein oder es können Datenverluste auftreten. Die Überlastung eines einzelnen Servers kann bei komplexen IT-Landschaften außerdem dazu führen, dass bei weiteren Servern Probleme oder Ausfälle auftreten.

Auslöser für die Überlastung von Informationssystemen kann sein, dass

- installierte Dienste oder Anwendungen falsch konfiguriert sind und so unnötig viel Speicher beanspruchen,
- vorhandene Speicherplatzkapazitäten überschritten werden,
- zahlreiche Anfragen zur gleichen Zeit ein System überbeanspruchen,
- zu viel Rechenleistung von den Diensten beansprucht wird oder
- eine zu große Anzahl an Nachrichten zur gleichen Zeit versendet wird.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.1.1 *Allgemeiner Server* aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der 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 Erfüllung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Haustechnik

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein SYS.1.1 *Allgemeiner Server* vorrangig erfüllt werden:

SYS.1.1.A1 Geeignete Aufstellung (B)

Server MÜSSEN an Orten betrieben werden, zu denen nur berechtigte Personen Zutritt haben. Server MÜSSEN daher in Rechenzentren, Rechnerräumen oder abschließbaren Serverschränken aufgestellt beziehungsweise eingebaut werden (siehe hierzu die entsprechenden Bausteine der Schicht INF *Infrastruktur*). Server DÜRFEN NICHT als Arbeitsplatzrechner genutzt werden. Als Arbeitsplatz genutzte IT-Systeme DÜRFEN NICHT als Server genutzt werden.

SYS.1.1.A2 Benutzerauthentisierung an Servern (B)

Für die Anmeldung von Benutzern und Diensten am Server MÜSSEN Authentisierungsverfahren eingesetzt werden, die dem Schutzbedarf der Server angemessen sind. Dies SOLLTE in besonderem Maße für administrative Zugänge berücksichtigt werden. Soweit möglich, SOLLTE dabei auf zentrale,

netzbasierte Authentisierungsdienste zurückgegriffen werden.

SYS.1.1.A3 ENTFALLEN (B)
Diese Anforderung ist entfallen.

SYS.1.1.A4 ENTFALLEN (B)
Diese Anforderung ist entfallen.

SYS.1.1.A5 Schutz von Schnittstellen (B)
Es MUSS gewährleistet werden, dass nur dafür vorgesehene Wechselspeicher und sonstige Geräte an die Server angeschlossen werden können. Alle Schnittstellen, die nicht verwendet werden, MÜSSEN deaktiviert werden.

SYS.1.1.A6 Deaktivierung nicht benötigter Dienste (B)
Alle nicht benötigten Dienste und Anwendungen MÜSSEN deaktiviert oder deinstalliert werden, vor allem Netzdienste. Auch alle nicht benötigten Funktionen in der Firmware MÜSSEN deaktiviert werden. Auf Servern SOLLTE der Speicherplatz für die einzelnen Benutzer, aber auch für Anwendungen, geeignet beschränkt werden.

Die getroffenen Entscheidungen SOLLTEN so dokumentiert werden, dass nachvollzogen werden kann, welche Konfiguration und Softwareausstattung für die Server gewählt wurden.

SYS.1.1.A7 ENTFALLEN (B)
Diese Anforderung ist entfallen.

SYS.1.1.A8 ENTFALLEN (B)
Diese Anforderung ist entfallen.

SYS.1.1.A9 Einsatz von Virenschutz-Programmen auf Servern (B)
Abhängig vom installierten Betriebssystem, den bereitgestellten Diensten und von anderen vorhandenen Schutzmechanismen des Servers MUSS geprüft werden, ob Viren-Schutzprogramme eingesetzt werden sollen und können. Soweit vorhanden, MÜSSEN konkrete Aussagen, ob ein Virenschutz notwendig ist, aus den betreffenden Betriebssystem-Bausteinen des IT-Grundschutz-Kompendiums berücksichtigt werden.

SYS.1.1.A10 Protokollierung (B)
Generell MÜSSEN alle sicherheitsrelevanten Systemereignisse protokolliert werden, dazu gehören mindestens:

- Systemstarts und Reboots,
- erfolgreiche und erfolglose Anmeldungen am System (Betriebssystem und Anwendungssoftware),
- fehlgeschlagene Berechtigungsprüfungen,
- blockierte Datenströme (Verstöße gegen ACLs oder Firewallregeln),
- Einrichtung oder Änderungen von Benutzern, Gruppen und Berechtigungen,
- sicherheitsrelevante Fehlermeldungen (z. B. Hardwaredefekte, Überschreitung von Kapazitätsgrenzen) sowie
- Warnmeldungen von Sicherheitssystemen (z. B. Virenschutz).

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein SYS.1.1 *Allgemeiner Server*. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.1.1.A11 Festlegung einer Sicherheitsrichtlinie für Server (S)
Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution SOLLTEN die Anforderungen an

Server in einer separaten Sicherheitsrichtlinie konkretisiert werden. Diese Richtlinie SOLLTE allen Administratoren und anderen Personen, die an der Beschaffung und dem Betrieb der Server beteiligt sind, bekannt und Grundlage für deren Arbeit sein. Die Umsetzung der in der Richtlinie geforderten Inhalte SOLLTE regelmäßig überprüft werden. Die Ergebnisse SOLLTEN sinnvoll dokumentiert werden.

SYS.1.1.A12 Planung des Server-Einsatzes (S)

Jedes Server-System SOLLTE geeignet geplant werden. Dabei SOLLTEN mindestens folgende Punkte berücksichtigt werden:

- Auswahl der Hardwareplattform, des Betriebssystems und der Anwendungssoftware,
- Dimensionierung der Hardware (Leistung, Speicher, Bandbreite etc.),
- Art und Anzahl der Kommunikationsschnittstellen,
- Leistungsaufnahme, Wärmelast, Platzbedarf und Bauform,
- Realisierung administrativer Zugänge (siehe SYS.1.1.A5 *Schutz der Administrationsschnittstellen*),
- Zugriffe von Benutzern,
- Realisierung der Protokollierung (siehe SYS.1.1.A10 *Protokollierung*),
- Realisierung der Systemaktualisierung (siehe SYS.1.1.A7 *Updates und Patches für Betriebssystem und Anwendungen*) sowie
- Einbindung ins System- und Netzmanagement, in die Datensicherung und die Schutzsysteme (Virenschutz, IDS etc.).

Alle Entscheidungen, die in der Planungsphase getroffen wurden, SOLLTEN so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können.

SYS.1.1.A13 Beschaffung von Servern (S)

Bevor ein oder mehrere Server beschafft werden, SOLLTE eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden.

SYS.1.1.A14 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.1.1.A15 Unterbrechungsfreie und stabile Stromversorgung [Haustechnik] (S)

Jeder Server SOLLTE an eine unterbrechungsfreie Stromversorgung (USV) angeschlossen werden.

SYS.1.1.A16 Sichere Grundkonfiguration von Servern (S)

Die Grundeinstellungen von Servern SOLLTEN überprüft und falls erforderlich entsprechend den Vorgaben der Sicherheitsrichtlinie angepasst werden. Erst nachdem die Installation und die Konfiguration abgeschlossen sind, SOLLTE der Server mit dem Internet verbunden werden.

SYS.1.1.A17 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.1.1.A18 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.1.1.A19 Einrichtung lokaler Paketfilter (S)

Vorhandene lokale Paketfilter SOLLTEN über ein Regelwerk so ausgestaltet werden, dass die eingehende und ausgehende Kommunikation auf die erforderlichen Kommunikationspartner, Kommunikationsprotokolle bzw. Ports und Schnittstellen beschränkt wird. Die Identität von Remote-Systemen und die Integrität der Verbindungen mit diesen SOLLTE kryptografisch abgesichert sein.

SYS.1.1.A20 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.1.1.A21 Betriebsdokumentation für Server (S)
Betriebliche Aufgaben, die an einem Server durchgeführt werden, SOLLTEN nachvollziehbar dokumentiert werden (Wer?, Wann?, Was?). Aus der Dokumentation SOLLTEN insbesondere Konfigurationsänderungen nachvollziehbar sein. Sicherheitsrelevante Aufgaben, z. B. wer befugt ist, neue Festplatten einzubauen, SOLLTEN dokumentiert werden. Alles, was automatisch dokumentiert werden kann, SOLLTE auch automatisch dokumentiert werden. Die Dokumentation SOLLTE gegen unbefugten Zugriff und Verlust geschützt werden.

SYS.1.1.A22 Einbindung in die Notfallplanung (S)
Der Server SOLLTE im Notfallmanagementprozess berücksichtigt werden. Dazu SOLLTEN die Notfallanforderungen an das System ermittelt und geeignete Notfallmaßnahmen umgesetzt werden, z. B. indem Wiederanlaufpläne erstellt oder Passwörter und kryptografische Schlüssel sicher hinterlegt werden.

SYS.1.1.A23 Systemüberwachung und Monitoring von Servern (S)
Das Server-System SOLLTE in ein geeignetes Systemüberwachungs- bzw. Monitoringkonzept eingebunden werden. Hierbei SOLLTEN der Systemzustand und die Funktionsfähigkeit des Systems und der darauf betriebenen Dienste laufend überwacht werden. Fehlerzustände sowie die Überschreitung definierter Grenzwerte SOLLTEN hierüber an das Betriebspersonal meldet werden.

SYS.1.1.A24 Sicherheitsprüfungen für Server (S)
Server SOLLTEN regelmäßigen Sicherheitstests unterzogen werden, die überprüfen, ob alle Sicherheitsvorgaben eingehalten werden und ggf. vorhandene Schwachstellen identifizieren. Diese Sicherheitsprüfungen SOLLTEN insbesondere auf Servern mit externen Schnittstellen durchgeführt werden. Um mittelbare Angriffe über infizierte Systeme im eigenen Netz zu vermeiden, SOLLTEN jedoch auch interne Server in festgelegten Zyklen entsprechend überprüft werden. Es SOLLTE geprüft werden, ob die Sicherheitsprüfungen automatisiert, z. B. mittels geeigneter Skripte, realisiert werden können.

SYS.1.1.A25 Geregelte Außerbetriebnahme eines Servers (S)
Bei der Außerbetriebnahme eines Servers SOLLTE sichergestellt werden, dass keine wichtigen Daten, die eventuell auf den verbauten Datenträgern gespeichert sind, verloren gehen und dass keine schutzbedürftigen Daten zurückbleiben. Es SOLLTE einen Überblick darüber geben, welche Daten wo auf dem Server gespeichert sind. Es SOLLTE außerdem sichergestellt sein, dass vom Server angebotene Dienste durch einen anderen Server übernommen werden, wenn dies erforderlich ist.

Es SOLLTE eine Checkliste erstellt werden, die bei der Außerbetriebnahme eines Servers abgearbeitet werden kann. Diese Checkliste SOLLTE mindestens Aspekte zur Datensicherung, Migration von Diensten und dem anschließenden sicheren Löschen aller Daten umfassen.

SYS.1.1.A35 Erstellung und Pflege eines Betriebshandbuchs (S)
Es SOLLTE ein Betriebshandbuch erstellt werden. Darin SOLLTEN alle erforderlichen Regelungen, Anforderungen und Einstellungen dokumentiert werden, die erforderlich sind, um Server zu betreiben. Für jede Art von Server SOLLTE es ein spezifisches Betriebshandbuch geben. Das Betriebshandbuch SOLLTE regelmäßig aktualisiert werden. Das Betriebshandbuch SOLLTE vor unberechtigtem Zugriff geschützt werden. Das Betriebshandbuch SOLLTE in Notfällen zur Verfügung stehen.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein SYS.1.1 *Allgemeiner Server* 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.

SYS.1.1.A26 ENTFALLEN (H)
Diese Anforderung ist entfallen.

SYS.1.1.A27 Hostbasierte Angriffserkennung (H)

Hostbasierte Angriffserkennungssysteme (Host-based Intrusion Detection Systems, IDS bzw. Intrusion Prevention Systems, IPS) SOLLTEN eingesetzt werden, um das Systemverhalten auf Anomalien und Missbrauch hin zu überwachen. Die eingesetzten IDS/IPS-Mechanismen SOLLTEN geeignet ausgewählt, konfiguriert und ausführlich getestet werden. Im Falle einer Angriffserkennung SOLLTE das Betriebspersonal in geeigneter Weise alarmiert werden.

Über Betriebssystem-Mechanismen oder geeignete Zusatzprodukte SOLLTEN Veränderungen an Systemdateien und Konfigurationseinstellungen überprüft, eingeschränkt und gemeldet werden.

SYS.1.1.A28 Steigerung der Verfügbarkeit durch Redundanz (H)

Server mit hohen Verfügbarkeitsanforderungen SOLLTEN gegen Ausfälle in geeigneter Weise geschützt sein. Hierzu SOLLTEN mindestens geeignete Redundanzen verfügbar sein sowie Wartungsverträge mit den Lieferanten abgeschlossen werden. Es SOLLTE geprüft werden, ob bei sehr hohen Anforderungen Hochverfügbarkeitsarchitekturen mit automatischem Failover, gegebenenfalls über verschiedene Standorte hinweg, erforderlich sind.

SYS.1.1.A29 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.1.1.A30 Ein Dienst pro Server (H)

Abhängig von der Bedrohungslage und dem Schutzbedarf der Dienste SOLLTE auf jedem Server jeweils nur ein Dienst betrieben werden.

SYS.1.1.A31 Application Whitelisting (H)

Es SOLLTE bei erhöhtem Schutzbedarf über Application Whitelisting sichergestellt werden, dass nur erlaubte Programme ausgeführt werden. Zum einen SOLLTEN vollständige Pfade bzw. Verzeichnisse festgelegt werden, aus denen diese Programme ausgeführt werden dürfen. Zum anderen SOLLTE alternativ einzelnen Anwendungen explizit die Ausführung gestattet werden.

SYS.1.1.A32 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.1.1.A33 Aktive Verwaltung der Wurzelzertifikate (H)

Im Zuge der Beschaffung und Installation des Servers SOLLTE dokumentiert werden, welche Wurzelzertifikate für den Betrieb des Servers notwendig sind. Auf dem Server SOLLTEN lediglich die für den Betrieb notwendigen und vorab dokumentierten Wurzelzertifikate enthalten sein. Es SOLLTE regelmäßig überprüft werden, ob die vorhandenen Wurzelzertifikate noch den Vorgaben der Institution entsprechen. Es SOLLTEN alle auf dem IT-System vorhandenen Zertifikatsspeicher in die Prüfung einbezogen werden.

SYS.1.1.A34 Festplattenverschlüsselung (H)

Bei erhöhtem Schutzbedarf sollten die Datenträger des Servers mit einem als sicher geltenden Produkt bzw. Verfahren verschlüsselt werden. Dies SOLLTE auch für virtuelle Maschinen mit produktiven Daten gelten. Es SOLLTE nicht nur ein TPM allein als Schlüsselschutz dienen. Das Wiederherstellungspasswort SOLLTE an einem geeigneten sicheren Ort gespeichert werden. Bei sehr hohen Anforderungen z. B. an die Vertraulichkeit SOLLTE eine Full Volume oder Full Disk Encryption erfolgen.

SYS.1.1.A36 Absicherung des Bootvorgangs (H)

Bootloader und Betriebssystem-Kern SOLLTEN durch selbstkontrolliertes Schlüsselmaterial signiert beim Systemstart in einer vertrauenswürdigen Kette geprüft werden (Secure Boot). Nicht benötigtes Schlüsselmaterial SOLLTE entfernt werden.

Anhang H – SYS.2.1 Allgemeiner Client

Angreifer gelingt, die Zugangsdaten auszuspähen oder zu erraten. Wird keine Bildschirmsperre aktiviert, kann der Client auch bei kurzzeitiger Abwesenheit unberechtigt genutzt werden.

2.5 Installation nicht benötigter Betriebssystemkomponenten und Applikationen

Bei der Installation eines Betriebssystems besteht in der Regel die Möglichkeit, optionale Software zu installieren. Auch im laufenden Betrieb wird regelmäßig Software installiert und getestet. Mit jeder weiteren Anwendung steigen nicht nur Rechen- und Speicherlast eines Clients an, sondern auch die Wahrscheinlichkeit für darin verborgene Schwachstellen. Nicht benötigte Software unterliegt außerdem häufig keinem regelmäßigen Patch-Management, sodass auch bekannte Sicherheitslücken nicht zeitnah geschlossen werden. Dadurch können Angreifer auch solche Schwachstellen ausnutzen, die schon lange bekannt sind.

2.6 Abhören von Räumen mittels Mikrofon und Kamera

Viele Clients verfügen über ein Mikrofon und eine Kamera. Diese können prinzipiell von jedem aktiviert und verwendet werden, der über entsprechende Zugriffsrechte verfügt, bei vernetzten Systemen auch von Externen. Werden diese Rechte nicht sorgfältig vergeben, können Unbefugte Mikrofon oder Kamera dazu missbrauchen, um über das Internet Räume abzuhören oder unbemerkt Besprechungen aufzuzeichnen. Hierzu gehören auch Intelligente Persönliche Assistenten (IPA) oder Sprachassistenten, die die Umgebung permanent abhören und nach Nennung eines geräteabhängigen Aktivierungsworts bestimmte Funktionen ausführen, wie Musik abspielen, Kontakte anrufen, die Beleuchtung steuern oder das Raumklima verändern. Werden die Gespräche z. B. von IPAs an Dritte übermittelt, könnten diese unter Umständen von Unbefugten abgehört werden. Die aufgezeichneten Gespräche könnten auch bei den Betreibern des IPA längerfristig abgespeichert und weiterverarbeitet werden.

2.7 Fehlerhafte Administration oder Nutzung von Geräten und Systemen

Moderne Client-Betriebssysteme sind sehr komplex. Daher können insbesondere Fehlkonfiguration von Komponenten die Sicherheit beeinträchtigen, sodass das IT-System fehlerhaft funktioniert oder kompromittiert werden kann. Grundsätzlich beinhaltet jede Schnittstelle an einem IT-System nicht nur die Möglichkeit, darüber bestimmte Dienste des IT-Systems berechtigt zu nutzen, sondern auch das Risiko, dass Unbefugte auf das IT-System zugreifen. Wenn etwa durch Fehlkonfiguration der Authentisierungsmechanismen Benutzerkennungen und zugehörige Passwörter ausgespäht werden können, ist eine unberechtigte Nutzung der damit geschützten Anwendungen oder IT-Systeme denkbar.

Auch eine fehlerhafte oder nicht ordnungsgemäße Nutzung von Geräten, Systemen und Anwendungen kann die Sicherheit beeinträchtigen, vor allem, wenn vorhandene Sicherheitsmaßnahmen missachtet oder umgangen werden. So können beispielsweise zu großzügig vergebene Rechte, leicht zu erratende Passwörter, nicht ausreichend geschützte Datenträger mit Sicherungskopien oder bei vorübergehender Abwesenheit nicht gesperrte Arbeitsplätze zu Sicherheitsvorfällen führen. Eine weitere Folge der fehlerhaften Bedienung von IT-Systemen oder Anwendungen kann das versehentlich Löschen oder Verändern von Daten sein. Dabei ist es ebenfalls möglich, dass vertrauliche Informationen in die Hände Dritter gelangen, beispielsweise wenn Zugriffsrechte falsch gesetzt werden.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.2.1 *Allgemeiner Client* aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der 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 Erfüllung von Anforderungen haben. Diese sind dann jeweils explizit in

eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Benutzer, Haustechnik

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein SYS.2.1 *Allgemeiner Client* vorrangig erfüllt werden:

SYS.2.1.A1 Sichere Benutzerauthentisierung (B)
Um den Client zu nutzen, MÜSSEN sich die Benutzer gegenüber dem IT-System authentisieren. Benutzer MÜSSEN eine Bildschirmsperre verwenden, wenn sie den Client unbeaufsichtigt betreiben. Die Bildschirmsperre SOLLTE automatisch aktiviert werden, wenn für eine festgelegte Zeitspanne keine Aktion durch den Benutzer durchgeführt wurde. Die Bildschirmsperre DARF NUR durch eine erfolgreiche Benutzerauthentisierung deaktiviert werden können. Die Benutzer SOLLTEN verpflichtet werden, sich nach Aufgabenerfüllung vom IT-System bzw. von der IT-Anwendung abzumelden.

SYS.2.1.A2 ENTFALLEN (B)
Diese Anforderung ist entfallen.

SYS.2.1.A3 Aktivieren von Autoupdate-Mechanismen (B)
Automatische Update-Mechanismen (Autoupdate) MÜSSEN aktiviert werden, sofern nicht andere Mechanismen wie regelmäßige manuelle Wartung oder ein zentrales Softwareverteilungssystem für Updates eingesetzt werden. Wenn für Autoupdate-Mechanismen ein Zeitintervall vorgegeben werden kann, SOLLTE mindestens täglich automatisch nach Updates gesucht und diese installiert werden.

SYS.2.1.A4 ENTFALLEN (B)
Diese Anforderung ist entfallen.

SYS.2.1.A5 ENTFALLEN (B)
Diese Anforderung ist entfallen.

SYS.2.1.A6 Einsatz von Schutzprogrammen gegen Schadsoftware (B)
Abhängig vom installierten Betriebssystem und von anderen vorhandenen Schutzmechanismen des Clients MUSS geprüft werden, ob Schutzprogramme gegen Schadsoftware eingesetzt werden sollen. Soweit vorhanden, MÜSSEN konkrete Aussagen, ob ein solcher Schutz notwendig ist, aus den Betriebssystem-Bausteinen des IT-Grundschutz-Kompendiums berücksichtigt werden.

Schutzprogramme auf den Clients MÜSSEN so konfiguriert sein, dass die Benutzer weder sicherheitsrelevante Änderungen an den Einstellungen vornehmen noch die Schutzprogramme deaktivieren können.

Das Schutzprogramm MUSS nach Schadsoftware suchen, wenn Dateien ausgetauscht oder übertragen werden. Der gesamte Datenbestand eines Clients MUSS regelmäßig auf Schadsoftware geprüft werden. Wenn ein Client infiziert ist, MUSS im Offlinebetrieb untersucht werden, ob ein gefundenes Schadprogramm bereits vertrauliche Daten gesammelt, Schutzfunktionen deaktiviert oder Code aus dem Internet nachgeladen hat.

SYS.2.1.A7 ENTFALLEN (B)
Diese Anforderung ist entfallen.

SYS.2.1.A8 Absicherung des Bootvorgangs (B)
Der Startvorgang des IT-Systems („Booten“) MUSS gegen Manipulation abgesichert werden. Es MUSS

festgelegt werden, von welchen Medien gebootet werden darf. Es SOLLTE entschieden werden, ob und wie der Bootvorgang kryptografisch geschützt werden soll. Es MUSS sichergestellt werden, dass nur Administratoren die Clients von einem anderen als den voreingestellten Laufwerken oder externen Speichermedien booten können. NUR Administratoren DÜRFEN von wechselbaren oder externen Speichermedien booten können. Die Konfigurationseinstellungen des Bootvorgangs DÜRFEN NUR durch Administratoren verändert werden können. Alle nicht benötigten Funktionen in der Firmware MÜSSEN deaktiviert werden.

SYS.2.1.A42 Nutzung von Cloud- und Online-Funktionen [Benutzer] (B)

Es DÜRFEN NUR zwingend notwendige Cloud- und Online-Funktionen des Betriebssystems genutzt werden. Die notwendigen Cloud- und Online-Funktionen SOLLTEN dokumentiert werden. Die entsprechenden Einstellungen des Betriebssystems MÜSSEN auf Konformität mit den organisatorischen Datenschutz- und Sicherheitsvorgaben überprüft und restriktiv konfiguriert bzw. die Funktionen deaktiviert werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein SYS.2.1 *Allgemeiner Client*. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.2.1.A9 Festlegung einer Sicherheitsrichtlinie für Clients (S)

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution SOLLTEN die Anforderungen an allgemeine Clients konkretisiert werden. Die Richtlinie SOLLTE allen Benutzern sowie allen Personen, die an der Beschaffung und dem Betrieb der Clients beteiligt sind, bekannt und Grundlage für deren Arbeit sein. Die Umsetzung der in der Richtlinie geforderten Inhalte SOLLTE regelmäßig überprüft werden. Die Ergebnisse SOLLTEN nachvollziehbar dokumentiert werden.

SYS.2.1.A10 Planung des Einsatzes von Clients (S)

Es SOLLTE im Vorfeld geplant werden, wo und wie Clients eingesetzt werden sollen. Die Planung SOLLTE dabei nicht nur Aspekte betreffen, die typischerweise direkt mit den Begriffen IT- oder Informationssicherheit in Verbindung gebracht werden, sondern auch betriebliche Aspekte, die Anforderungen im Bereich der Sicherheit nach sich ziehen. Alle Entscheidungen, die in der Planungsphase getroffen wurden, SOLLTEN so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können.

SYS.2.1.A11 Beschaffung von Clients (S)

Bevor Clients beschafft werden, SOLLTE eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden. Die jeweiligen Hersteller von IT- und Betriebssystem SOLLTEN für den gesamten geplanten Nutzungszeitraum Patches für Schwachstellen zeitnah zur Verfügung stellen. Die zu beschaffenden Systeme SOLLTEN über eine Firmware-Konfigurationsoberfläche für UEFI SecureBoot und, sofern vorhanden, für das TPM verfügen, die eine Kontrolle durch den Eigentümer (Institution) gewährleistet und so den selbstverwalteten Betrieb von SecureBoot und des TPM ermöglicht.

SYS.2.1.A12 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.2.1.A13 Zugriff auf Ausführungsumgebungen mit unbeobachtbarer Codeausführung (S)

Der Zugriff auf Ausführungsumgebungen mit unbeobachtbarer Codeausführung (z. B. durch das Betriebssystem speziell abgesicherte Speicherbereiche, Firmwarebereiche etc.) SOLLTE nur durch Benutzer mit administrativen Berechtigungen möglich sein. Die entsprechenden Einstellungen im BIOS bzw. der UEFI-Firmware SOLLTEN durch ein Passwort vor unberechtigten Veränderungen geschützt werden. Wird die Kontrolle über die Funktionen an das Betriebssystem delegiert, SOLLTEN auch dort nur Benutzer mit administrativen Berechtigungen auf die Funktionen zugreifen dürfen.

SYS.2.1.A14 Updates und Patches für Firmware, Betriebssystem und Anwendungen (S)

Auf Betriebssysteme, die über ein Rolling-Release-Modell aktualisiert werden, SOLLTE verzichtet werden. Es SOLLTEN NUR Anwendungsprogramme ausgewählt und installiert werden, für die Support angeboten wird. Betriebssysteme, Anwendungsprogramme und Firmware, für die keine regelmäßigen Sicherheitsupdates angeboten werden, DÜRFEN NICHT eingesetzt werden.

SYS.2.1.A15 Sichere Installation und Konfiguration von Clients (S)

Es SOLLTE festgelegt werden, welche Komponenten des Betriebssystems, welche Fachanwendungen und welche weiteren Tools installiert werden sollen. Die Installation und Konfiguration der IT-Systeme SOLLTE nur von autorisierten Personen (Administratoren oder vertraglich gebundenen Dienstleistern) nach einem definierten Prozess in einer Installationsumgebung durchgeführt werden. Nachdem die Installation und die Konfiguration abgeschlossen sind, SOLLTEN die Grundeinstellungen überprüft werden. Sofern die Installation und Konfiguration den Vorgaben aus der Sicherheitsrichtlinie entsprechen, SOLLTEN die Clients im Anschluss in der Produktivumgebung in Betrieb genommen werden. Alle Installations- und Konfigurationsschritte SOLLTEN so dokumentiert werden, dass diese durch einen sachkundigen Dritten nachvollzogen und wiederholt werden können.

SYS.2.1.A16 Deaktivierung und Deinstallation nicht benötigter Komponenten und Kennungen (S)

Nach der Installation SOLLTE überprüft werden, welche Komponenten der Firmware sowie des Betriebssystems und welche Anwendungen und weiteren Tools auf den Clients installiert und aktiviert sind. Nicht benötigte Module, Programme, Dienste, Aufgaben und Firmwarefunktionen (wie Fernwartung) SOLLTEN deaktiviert oder ganz deinstalliert werden. Nicht benötigte Laufzeitumgebungen, Interpretersprachen und Compiler SOLLTEN deinstalliert werden. Nicht benötigte Benutzerkennungen SOLLTEN deaktiviert oder gelöscht werden. Nicht benötigte Schnittstellen und Hardware des IT-Systemes (wie Webcams) SOLLTEN deaktiviert werden. Es SOLLTE verhindert werden, dass diese Komponenten wieder reaktiviert werden können. Die getroffenen Entscheidungen SOLLTEN nachvollziehbar dokumentiert werden.

SYS.2.1.A17 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.2.1.A18 Nutzung von verschlüsselten Kommunikationsverbindungen (S)

Kommunikationsverbindungen SOLLTEN, soweit möglich, durch Verschlüsselung geschützt werden.

Die Clients SOLLTEN kryptografische Algorithmen und Schlüssellängen verwenden, die dem Stand der Technik und den Sicherheitsanforderungen der Institution entsprechen.

Neue Zertifikate von Zertifikatsaustellern SOLLTEN erst nach Überprüfung des Fingerprints aktiviert werden.

SYS.2.1.A19 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.2.1.A20 Schutz der Administrationsverfahren bei Clients (S)

Abhängig davon, ob Clients lokal oder über das Netz administriert werden, SOLLTEN geeignete Sicherheitsvorkehrungen getroffen werden. Die zur Administration verwendeten Verfahren SOLLTEN über die in der Sicherheitsrichtlinie festgelegten Vorgaben erfolgen.

SYS.2.1.A21 Verhinderung der unautorisierten Nutzung von Rechnermikrofonen und Kameras (S)

Der Zugriff auf Mikrofon und Kamera eines Clients SOLLTE nur durch den Benutzer selbst möglich sein, solange er lokal am IT-System arbeitet. Wenn vorhandene Mikrofone oder Kameras nicht genutzt und deren Missbrauch verhindert werden soll, SOLLTEN diese, wenn möglich, ausgeschaltet, abgedeckt (nur Kamera), deaktiviert oder physisch vom Gerät getrennt werden. Es SOLLTE geregelt werden, wie

Kameras und Mikrofone in Clients genutzt und wie die Rechte vergeben werden.

SYS.2.1.A22 ENTFALLEN (S)
Diese Anforderung ist entfallen.

SYS.2.1.A23 Bevorzugung von Client-Server-Diensten (S)
Wenn möglich, SOLLTEN zum Informationsaustausch dedizierte Serverdienste genutzt und direkte Verbindungen zwischen Clients vermieden werden. Falls dies nicht möglich ist, SOLLTE festgelegt werden, welche Client-zu-Client-Dienste (oft auch als „Peer-to-Peer" bezeichnet) genutzt und welche Informationen darüber ausgetauscht werden dürfen. Falls erforderlich, SOLLTEN die Benutzer für die Nutzung solcher Dienste geschult werden. Direkte Verbindungen zwischen Clients SOLLTEN sich nur auf das LAN beschränken. Auto-Discovery-Protokolle SOLLTEN auf das notwendige Maß beschränkt werden.

SYS.2.1.A24 Umgang mit externen Medien und Wechseldatenträgern (S)
Auf externe Schnittstellen SOLLTE NUR restriktiv zugegriffen werden können. Es SOLLTE untersagt werden, dass nicht zugelassene Geräte oder Wechseldatenträger mit den Clients verbunden werden. Es SOLLTE verhindert werden, dass von den Clients auf Wechseldatenträger aus nicht vertrauenswürdigen Quellen zugegriffen werden kann. Die unerlaubte Ausführung von Programmen auf bzw. von externen Datenträgern SOLLTE technisch unterbunden werden. Es SOLLTE verhindert werden, dass über Wechsellaufwerke oder externe Schnittstellen unberechtigt Daten von den Clients kopiert werden können.

SYS.2.1.A25 ENTFALLEN (S)
Diese Anforderung ist entfallen.

SYS.2.1.A26 Schutz vor Ausnutzung von Schwachstellen in Anwendungen (S)
Um die Ausnutzung von Schwachstellen in Anwendungen zu erschweren, SOLLTEN ASLR und DEP/NX im Betriebssystem aktiviert und von den Anwendungen genutzt werden. Sicherheitsfunktionen des Kernels und der Standardbibliotheken wie z. B. Heap- und Stackschutz SOLLTEN aktiviert werden.

SYS.2.1.A27 Geregelte Außerbetriebnahme eines Clients (S)
Bei der Außerbetriebnahme eines Clients SOLLTE sichergestellt werden, dass keine Daten verloren gehen und dass keine schutzbedürftigen Daten zurückbleiben. Es SOLLTE einen Überblick darüber geben, welche Daten wo auf den IT-Systemen gespeichert sind. Es SOLLTE eine Checkliste erstellt werden, die bei der Außerbetriebnahme eines IT-Systems abgearbeitet werden kann. Diese Checkliste SOLLTE mindestens Aspekte zur Datensicherung weiterhin benötigter Daten und dem anschließenden sicheren Löschen aller Daten umfassen.

SYS.2.1.A43 Lokale Sicherheitsrichtlinien für Clients (S)
Alle sicherheitsrelevanten Einstellungen SOLLTEN bedarfsgerecht konfiguriert, getestet und regelmäßig überprüft werden. Dafür SOLLTEN Sicherheitsrichtlinien, unter Berücksichtigung der Empfehlungen des Betriebssystemherstellers und des voreingestellten Standardverhaltens, konfiguriert werden, sofern das Standardverhalten nicht anderen Anforderungen aus dem IT-Grundschutz oder der Organisation widerspricht. Die Entscheidungen SOLLTEN dokumentiert und begründet werden. Sicherheitsrichtlinien SOLLTEN in jedem Fall gesetzt werden, auch dann, wenn das voreingestellte Standardverhalten dadurch nicht verändert wird.

SYS.2.1.A44 Verwaltung der Sicherheitsrichtlinien von Clients (S)
Alle Einstellungen der Clients SOLLTEN durch Nutzung eines Managementsystems verwaltet und entsprechend dem ermittelten Schutzbedarf sowie auf den internen Richtlinien basierend konfiguriert sein. Konfigurationsänderungen SOLLTEN dokumentiert, begründet und mit dem Sicherheitsmanagement abgestimmt werden, sodass der Stand der Sicherheitskonfiguration jederzeit nachvollziehbar ist und Konfigurationsänderungen schnell durchgeführt und zentralisiert verteilt werden können.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein SYS.2.1 *Allgemeiner Client* 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.

SYS.2.1.A28 Verschlüsselung der Clients (H)

Wenn vertrauliche Informationen auf den Clients gespeichert werden, SOLLTEN mindestens die schutzbedürftigen Dateien sowie ausgewählte Dateisystembereiche oder besser die gesamten Datenträger verschlüsselt werden. Hierfür SOLLTE ein eigenes Konzept erstellt und die Details der Konfiguration besonders sorgfältig dokumentiert werden. In diesem Zusammenhang SOLLTEN die Authentisierung (z. B. Passwort, PIN, Token), die Ablage der Wiederherstellungsinformationen, die zu verschlüsselnden Laufwerke und die Schreibrechte auf unverschlüsselte Datenträger geregelt werden. Der Zugriff auf das genutzte Schlüsselmaterial MUSS angemessen geschützt sein.

Benutzer SOLLTEN darüber aufgeklärt werden, wie sie sich bei Verlust eines Authentisierungsmittels zu verhalten haben.

SYS.2.1.A29 Systemüberwachung und Monitoring der Clients (H)

Die Clients SOLLTEN in ein geeignetes Systemüberwachungs- bzw. Monitoringkonzept eingebunden werden, das den Systemzustand und die Funktionsfähigkeit der Clients laufend überwacht und Fehlerzustände sowie die Über- bzw. Unterschreitung definierter Grenzwerte an das Betriebspersonal meldet.

SYS.2.1.A30 Einrichten einer Referenzumgebung für Clients (H)

Für Clients SOLLTE eine Referenzinstallation erstellt werden, in der die Grundkonfiguration und alle Konfigurationsänderungen, Updates und Patches vor dem Einspielen auf den Client vorab getestet werden können. Für verschiedene, typische und häufig wiederkehrende Testfälle SOLLTEN Checklisten erstellt werden, die beim Testlauf möglichst automatisiert abgearbeitet werden sollten. Die Testfälle SOLLTEN sowohl die Anwendersicht als auch die Betriebsperspektive berücksichtigen. Zusätzlich SOLLTEN alle Tests so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können.

SYS.2.1.A31 Einrichtung lokaler Paketfilter (H)

Auf jedem Client SOLLTEN, zusätzlich zu den eingesetzten zentralen Sicherheitsgateways, lokale Paketfilter eingesetzt werden. Als Strategie zur Paketfilter-Implementierung SOLLTE eine Whitelist-Strategie gewählt werden, die auf Basis der benötigten Netzkommunikation erfolgt.

SYS.2.1.A32 Einsatz zusätzlicher Maßnahmen zum Schutz vor Exploits (H)

Auf den Clients SOLLTEN zusätzliche Maßnahmen zum expliziten Schutz vor Exploits (Angriffe, um Systemlücken auszunutzen) getroffen werden. Wenn notwendige Schutzmaßnahmen nicht über Funktionen des Betriebssystems umgesetzt werden können, SOLLTEN zusätzliche geeignete Sicherheitsmaßnahmen umgesetzt werden. Sollte es nicht möglich sein, nachhaltige Maßnahmen umzusetzen, SOLLTEN andere geeignete (in der Regel organisatorische) Sicherheitsmaßnahmen ergriffen werden.

SYS.2.1.A33 Application Whitelisting (H)

Es SOLLTE über Application Whitelisting sichergestellt werden, dass nur explizit erlaubte Programme und Skripte ausgeführt werden können. Die Regeln SOLLTEN so eng wie möglich gefasst werden. Falls Pfade und Hashes nicht explizit angegeben werden können, SOLLTEN alternativ auch zertifikatsbasierte oder Pfad-Regeln genutzt werden.

SYS.2.1.A34 Kapselung von sicherheitskritischen Anwendungen und Betriebssystemkomponenten (H)

Um sowohl den Zugriff eines Angreifers auf das Betriebssystem oder andere Anwendungen als auch

den Zugriff vom Betriebssystem auf besonders schützenswerte Dateien zu verhindern, SOLLTEN Anwendungen und Betriebssystemkomponenten (wie beispielsweise Authentisierung oder Zertifikatsüberprüfung) besonders gekapselt bzw. anderen Anwendungen und Betriebssystemkomponenten gegenüber isoliert werden. Dabei SOLLTEN insbesondere sicherheitskritische Anwendungen berücksichtigt werden, die mit Daten aus unsicheren Quellen arbeiten (z.B. Webbrowser und Bürokommunikations-Anwendungen).

SYS.2.1.A35 Aktive Verwaltung der Wurzelzertifikate (H)

Im Zuge der Beschaffung und Installation des Clients SOLLTE dokumentiert werden, welche Wurzelzertifikate für den Betrieb des Clients notwendig sind. Auf dem Client SOLLTEN lediglich die für den Betrieb notwendigen und vorab dokumentierten Wurzelzertifikate enthalten sein. Es SOLLTE regelmäßig überprüft werden, ob die vorhandenen Wurzelzertifikate noch den Vorgaben der Institution entsprechen. Es SOLLTEN alle auf dem IT-System vorhandenen Zertifikatsspeicher in die Prüfung einbezogen werden (z. B. UEFI-Zertifikatsspeicher, Zertifikatsspeicher von Web-Browsern etc.).

SYS.2.1.A36 Selbstverwalteter Einsatz von SecureBoot und TPM (H)

Auf UEFI-kompatiblen Systemen SOLLTEN Bootloader, Kernel sowie alle benötigten Firmware-Komponenten durch selbstkontrolliertes Schlüsselmaterial signiert und nicht benötigtes Schlüsselmaterial SOLLTE entfernt werden. Sofern das Trusted Platform Module (TPM) nicht benötigt wird, SOLLTE es deaktiviert werden.

SYS.2.1.A37 Verwendung von Mehr-Faktor-Authentisierung (H)

Es SOLLTE eine sichere Mehr-Faktor-Authentisierung unter Einbeziehung unterschiedlicher Faktoren (Wissen, Besitz, Eigenschaft) für die lokale Anmeldung am Client eingerichtet werden, z. B. Passwort mit Chipkarte oder Token.

SYS.2.1.A38 Einbindung in die Notfallplanung (H)

Die Clients SOLLTEN im Notfallmanagementprozess berücksichtigt werden. Die Clients SOLLTEN hinsichtlich der Geschäftsprozesse oder Fachaufgaben, für die sie benötigt werden, für den Wiederanlauf priorisiert werden. Es SOLLTEN geeignete Notfallmaßnahmen vorgesehen werden, indem mindestens Wiederanlaufpläne erstellt, Bootmedien zur Systemwiederherstellung generiert sowie Passwörter und kryptografische Schlüssel sicher hinterlegt werden.

SYS.2.1.A39 Unterbrechungsfreie und stabile Stromversorgung [Haustechnik] (H)

Clients SOLLTEN an eine unterbrechungsfreie Stromversorgung (USV) angeschlossen werden. Die USV SOLLTE hinsichtlich Leistung und Stützzeit ausreichend dimensioniert sein. Clients SOLLTEN vor Überspannung geschützt werden.

SYS.2.1.A40 Betriebsdokumentation (H)

Die Durchführung betrieblicher Aufgaben an Clients bzw. Clientgruppen SOLLTE nachvollziehbar anhand der Fragen „Wer?“, „Wann?“ und „Was?“ dokumentiert werden. Aus der Dokumentation SOLLTEN insbesondere Konfigurationsänderungen nachvollziehbar sein. Auch sicherheitsrelevante Aufgaben (z. B. wer befugt ist, neue Festplatten einzubauen) SOLLTEN dokumentiert werden. Alles, was automatisch dokumentiert werden kann, SOLLTE auch automatisch dokumentiert werden. Die Dokumentation SOLLTE vor unbefugtem Zugriff und Verlust geschützt werden. Sicherheitsrelevante Aspekte SOLLTEN nachvollziehbar erläutert und hervorgehoben werden.

SYS.2.1.A41 Verwendung von Quotas für lokale Datenträger (H)

Es SOLLTE überlegt werden, Quotas einzurichten, die den verwendeten Speicherplatz auf der lokalen Festplatte begrenzen. Alternativ SOLLTEN Mechanismen des verwendeten Datei- oder Betriebssystems genutzt werden, die den Benutzer bei einem bestimmten Füllstand der Festplatte warnen oder nur noch dem Systemadministrator Schreibrechte einräumen.

SYS.2.1.A45 Erweiterte Protokollierung (H)

Es SOLLTE auch Client-Verhalten, das nicht mit der Sicherheit direkt in Verbindung steht, protokolliert

Anhang I – NET.1.1 Netzarchitektur und - design

mindestens ein zustandsbehafteter Paketfilter eingesetzt werden.

In der zweistufigen Firewall-Architektur MUSS jeder ein- und ausgehende Datenverkehr durch den äußeren Paketfilter bzw. den internen Paketfilter kontrolliert und gefiltert werden.

Eine P-A-P-Struktur, die aus Paketfilter, Application-Layer-Gateway bzw. Sicherheits-Proxies und Paketfilter besteht, MUSS immer realisiert werden, wenn die Sicherheitsrichtlinie oder die Anforderungsspezifikation dies fordern.

NET.1.1.A5 Client-Server-Segmentierung (B)

Clients und Server MÜSSEN in unterschiedlichen Netzsegmenten platziert werden. Die Kommunikation zwischen diesen Netzsegmenten MUSS mindestens durch einen zustandsbehafteten Paketfilter kontrolliert werden.

Es SOLLTE beachtet werden, dass mögliche Ausnahmen, die es erlauben, Clients und Server in einem gemeinsamen Netzsegment zu positionieren, in den entsprechenden anwendungs- und systemspezifischen Bausteinen geregelt werden.

Für Gastzugänge und für Netzbereiche, in denen keine ausreichende interne Kontrolle über die Endgeräte gegeben ist, MÜSSEN dedizierte Netzsegmente eingerichtet werden.

NET.1.1.A6 Endgeräte-Segmentierung im internen Netz (B)

Es DÜRFEN NUR Endgeräte in einem Netzsegment positioniert werden, die einem ähnlichen Sicherheitsniveau entsprechen.

NET.1.1.A7 Absicherung von schützenswerten Informationen (B)

Schützenswerte Informationen MÜSSEN über nach dem derzeitigen Stand der Technik sichere Protokolle übertragen werden, falls nicht über vertrauenswürdige dedizierte Netzsegmente (z. B. innerhalb des Managementnetzes) kommuniziert wird. Können solche Protokolle nicht genutzt werden, MUSS nach Stand der Technik angemessen verschlüsselt und authentisiert werden (siehe NET.3.3 *VPN).*

NET.1.1.A8 Grundlegende Absicherung des Internetzugangs (B)

Der Internetverkehr MUSS über die Firewall-Struktur geführt werden (siehe NET.1.1.A4 *Netztrennung in Zonen*). Die Datenflüsse MÜSSEN durch die Firewall-Struktur auf die benötigten Protokolle und Kommunikationsbeziehungen eingeschränkt werden.

NET.1.1.A9 Grundlegende Absicherung der Kommunikation mit nicht vertrauenswürdigen Netzen (B)

Für jedes Netz MUSS festgelegt werden, inwieweit es als vertrauenswürdig einzustufen ist. Netze, die nicht vertrauenswürdig sind, MÜSSEN wie das Internet behandelt und entsprechend abgesichert werden.

NET.1.1.A10 DMZ-Segmentierung für Zugriffe aus dem Internet (B)

Die Firewall-Strukur MUSS für alle Dienste bzw. Anwendungen, die aus dem Internet erreichbar sind, um eine sogenannte externe DMZ ergänzt werden. Es SOLLTE ein Konzept zur DMZ-Segmentierung erstellt werden, das die Sicherheitsrichtlinie und die Anforderungsspezifikation nachvollziehbar umsetzt. Abhängig vom Sicherheitsniveau der IT-Systeme MÜSSEN die DMZ-Segmente weitergehend unterteilt werden. Eine externe DMZ MUSS am äußeren Paketfilter angeschlossen werden.

NET.1.1.A11 Absicherung eingehender Kommunikation vom Internet in das interne Netz (B)

Ein IP-basierter Zugriff auf das interne Netz MUSS über einen sicheren Kommunikationskanal erfolgen. Der Zugriff MUSS auf vertrauenswürdige IT-Systeme und Benutzer beschränkt werden (siehe NET.3.3 *VPN*). Derartige VPN-Gateways SOLLTEN in einer externen DMZ platziert werden. Es SOLLTE beachtet werden, dass hinreichend gehärtete VPN-Gateways direkt aus dem Internet erreichbar sein können. Die über das VPN-Gateway authentisierten Zugriffe ins interne Netz MÜSSEN mindestens die

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Planer
Weitere Zuständigkeiten	IT-Betrieb

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein NET.1.1 *Netzarchitektur und -design* vorrangig erfüllt werden:

NET.1.1.A1 Sicherheitsrichtlinie für das Netz [IT-Betrieb] (B)

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution MUSS eine spezifische Sicherheitsrichtlinie für das Netz erstellt werden. Darin MÜSSEN nachvollziehbar Anforderungen und Vorgaben beschrieben werden, wie Netze sicher konzipiert und aufgebaut werden. In der Richtlinie MUSS unter anderem festgelegt werden,

- in welchen Fällen die Zonen zu segmentieren sind und in welchen Fällen Benutzergruppen bzw. Mandanten logisch oder sogar physisch zu trennen sind,
- welche Kommunikationsbeziehungen und welche Netz- und Anwendungsprotokolle jeweils zugelassen werden,
- wie der Datenverkehr für Administration und Überwachung netztechnisch zu trennen ist,
- welche institutionsinterne, standortübergreifende Kommunikation (WAN, Funknetze) erlaubt und welche Verschlüsselung im WAN, LAN oder auf Funkstrecken erforderlich ist sowie
- welche institutionsübergreifende Kommunikation zugelassen ist.

Die Richtlinie MUSS allen im Bereich Netzdesign zuständigen Mitarbeitern bekannt sein. Sie MUSS zudem grundlegend für ihre Arbeit sein. Wird die Richtlinie verändert oder wird von den Anforderungen abgewichen, MUSS dies dokumentiert und mit dem verantwortlichen ISB abgestimmt werden. Es MUSS regelmäßig überprüft werden, ob die Richtlinie noch korrekt umgesetzt ist. Die Ergebnisse MÜSSEN sinnvoll dokumentiert werden.

NET.1.1.A2 Dokumentation des Netzes [IT-Betrieb] (B)

Es MUSS eine vollständige Dokumentation des Netzes erstellt werden. Sie MUSS einen Netzplan beinhalten. Die Dokumentation MUSS nachhaltig gepflegt werden. Die initiale Ist-Aufnahme, einschließlich der Netzperformance, sowie alle durchgeführten Änderungen im Netz MÜSSEN in der Dokumentation enthalten sein. Die logische Struktur des Netzes MUSS dokumentiert werden, insbesondere, wie die Subnetze zugeordnet und wie das Netz zoniert und segmentiert wird.

NET.1.1.A3 Anforderungsspezifikation für das Netz (B)

Ausgehend von der Sicherheitsrichtlinie für das Netz MUSS eine Anforderungsspezifikation erstellt werden. Diese MUSS nachhaltig gepflegt werden. Aus den Anforderungen MÜSSEN sich alle wesentlichen Elemente für Netzarchitektur und -design ableiten lassen.

NET.1.1.A4 Netztrennung in Zonen (B)

Das Gesamtnetz MUSS mindestens in folgende drei Zonen physisch separiert sein: internes Netz, demilitarisierte Zone (DMZ) und Außenanbindungen (inklusive Internetanbindung sowie Anbindung an andere nicht vertrauenswürdige Netze). Die Zonenübergänge MÜSSEN durch eine Firewall abgesichert werden. Diese Kontrolle MUSS dem Prinzip der lokalen Kommunikation folgen, sodass von Firewalls ausschließlich erlaubte Kommunikation weitergeleitet wird (Whitelisting).

Nicht vertrauenswürdige Netze (z. B. Internet) und vertrauenswürdige Netze (z. B. Intranet) MÜSSEN mindestens durch eine zweistufige Firewall-Struktur, bestehend aus zustandsbehafteten Paketfiltern (Firewall), getrennt werden. Um Internet und externe DMZ netztechnisch zu trennen, MUSS

mindestens ein zustandsbehafteter Paketfilter eingesetzt werden.

In der zweistufigen Firewall-Architektur MUSS jeder ein- und ausgehende Datenverkehr durch den äußeren Paketfilter bzw. den internen Paketfilter kontrolliert und gefiltert werden.

Eine P-A-P-Struktur, die aus Paketfilter, Application-Layer-Gateway bzw. Sicherheits-Proxies und Paketfilter besteht, MUSS immer realisiert werden, wenn die Sicherheitsrichtlinie oder die Anforderungsspezifikation dies fordern.

NET.1.1.A5 Client-Server-Segmentierung (B)

Clients und Server MÜSSEN in unterschiedlichen Netzsegmenten platziert werden. Die Kommunikation zwischen diesen Netzsegmenten MUSS mindestens durch einen zustandsbehafteten Paketfilter kontrolliert werden.

Es SOLLTE beachtet werden, dass mögliche Ausnahmen, die es erlauben, Clients und Server in einem gemeinsamen Netzsegment zu positionieren, in den entsprechenden anwendungs- und systemspezifischen Bausteinen geregelt werden.

Für Gastzugänge und für Netzbereiche, in denen keine ausreichende interne Kontrolle über die Endgeräte gegeben ist, MÜSSEN dedizierte Netzsegmente eingerichtet werden.

NET.1.1.A6 Endgeräte-Segmentierung im internen Netz (B)

Es DÜRFEN NUR Endgeräte in einem Netzsegment positioniert werden, die einem ähnlichen Sicherheitsniveau entsprechen.

NET.1.1.A7 Absicherung von schützenswerten Informationen (B)

Schützenswerte Informationen MÜSSEN über nach dem derzeitigen Stand der Technik sichere Protokolle übertragen werden, falls nicht über vertrauenswürdige dedizierte Netzsegmente (z. B. innerhalb des Managementnetzes) kommuniziert wird. Können solche Protokolle nicht genutzt werden, MUSS nach Stand der Technik angemessen verschlüsselt und authentisiert werden (siehe NET.3.3 *VPN).*

NET.1.1.A8 Grundlegende Absicherung des Internetzugangs (B)

Der Internetverkehr MUSS über die Firewall-Struktur geführt werden (siehe NET.1.1.A4 *Netztrennung in Zonen*). Die Datenflüsse MÜSSEN durch die Firewall-Struktur auf die benötigten Protokolle und Kommunikationsbeziehungen eingeschränkt werden.

NET.1.1.A9 Grundlegende Absicherung der Kommunikation mit nicht vertrauenswürdigen Netzen (B)

Für jedes Netz MUSS festgelegt werden, inwieweit es als vertrauenswürdig einzustufen ist. Netze, die nicht vertrauenswürdig sind, MÜSSEN wie das Internet behandelt und entsprechend abgesichert werden.

NET.1.1.A10 DMZ-Segmentierung für Zugriffe aus dem Internet (B)

Die Firewall-Strukur MUSS für alle Dienste bzw. Anwendungen, die aus dem Internet erreichbar sind, um eine sogenannte externe DMZ ergänzt werden. Es SOLLTE ein Konzept zur DMZ-Segmentierung erstellt werden, das die Sicherheitsrichtlinie und die Anforderungsspezifikation nachvollziehbar umsetzt. Abhängig vom Sicherheitsniveau der IT-Systeme MÜSSEN die DMZ-Segmente weitergehend unterteilt werden. Eine externe DMZ MUSS am äußeren Paketfilter angeschlossen werden.

NET.1.1.A11 Absicherung eingehender Kommunikation vom Internet in das interne Netz (B)

Ein IP-basierter Zugriff auf das interne Netz MUSS über einen sicheren Kommunikationskanal erfolgen. Der Zugriff MUSS auf vertrauenswürdige IT-Systeme und Benutzer beschränkt werden (siehe NET.3.3 *VPN*). Derartige VPN-Gateways SOLLTEN in einer externen DMZ platziert werden. Es SOLLTE beachtet werden, dass hinreichend gehärtete VPN-Gateways direkt aus dem Internet erreichbar sein können. Die über das VPN-Gateway authentisierten Zugriffe ins interne Netz MÜSSEN mindestens die

interne Firewall durchlaufen.

IT-Systeme DÜRFEN NICHT via Internet oder externer DMZ auf das interne Netz zugreifen. Es SOLLTE beachtet werden, dass etwaige Ausnahmen zu dieser Anforderung in den entsprechenden anwendungs- und systemspezifischen Bausteinen geregelt werden.

NET.1.1.A12 Absicherung ausgehender interner Kommunikation zum Internet (B)

Ausgehende Kommunikation aus dem internen Netz zum Internet MUSS an einem Sicherheits-Proxy entkoppelt werden. Die Entkoppelung MUSS außerhalb des internen Netzes erfolgen. Wird eine P-A-P-Struktur eingesetzt, SOLLTE die ausgehende Kommunikation immer durch die Sicherheits-Proxies der P-A-P-Struktur entkoppelt werden.

NET.1.1.A13 Netzplanung (B)

Jede Netzimplementierung MUSS geeignet, vollständig und nachvollziehbar geplant werden. Dabei MÜSSEN die Sicherheitsrichtlinie sowie die Anforderungsspezifikation beachtet werden. Darüber hinaus MÜSSEN in der Planung mindestens die folgenden Punkte bedarfsgerecht berücksichtigt werden:

- Anbindung von Internet und, sofern vorhanden, Standortnetz und Extranet,
- Topologie des Gesamtnetzes und der Netzbereiche, d. h. Zonen und Netzsegmente,
- Dimensionierung und Redundanz der Netz- und Sicherheitskomponenten, Übertragungsstrecken und Außenanbindungen,
- zu nutzende Protokolle und deren grundsätzliche Konfiguration und Adressierung, insbesondere IPv4/IPv6-Subnetze von Endgerätegruppen sowie
- Administration und Überwachung (siehe NET.1.2 *Netzmanagement*).

Die Netzplanung MUSS regelmäßig überprüft werden.

NET.1.1.A14 Umsetzung der Netzplanung (B)

Das geplante Netz MUSS fachgerecht umgesetzt werden. Dies MUSS während der Abnahme geprüft werden.

NET.1.1.A15 Regelmäßiger Soll-Ist-Vergleich (B)

Es MUSS regelmäßig geprüft werden, ob das bestehende Netz dem Soll-Zustand entspricht. Dabei MUSS mindestens geprüft werden, inwieweit es die Sicherheitsrichtlinie und Anforderungsspezifikation erfüllt. Es MUSS auch geprüft werden, inwiefern die umgesetzte Netzstruktur dem aktuellen Stand der Netzplanung entspricht. Dafür MÜSSEN zuständige Personen sowie Prüfkriterien bzw. Vorgaben festgelegt werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein NET.1.1 *Netzarchitektur und -design*. Sie SOLLTEN grundsätzlich erfüllt werden.

NET.1.1.A16 Spezifikation der Netzarchitektur (S)

Auf Basis der Sicherheitsrichtlinie und der Anforderungsspezifikation SOLLTE eine Architektur für die Zonen inklusive internem Netz, DMZ-Bereich und Außenanbindungen entwickelt und nachhaltig gepflegt werden. Dabei SOLLTEN je nach spezifischer Situation der Institution alle relevanten Architekturelemente betrachtet werden, mindestens jedoch:

- Netzarchitektur des internen Netzes mit Festlegungen dazu, wie Netzvirtualisierungstechniken, Layer-2- und Layer-3-Kommunikation sowie Redundanzverfahren einzusetzen sind,
- Netzarchitektur für Außenanbindungen, inklusive Firewall-Architekturen, sowie DMZ- und Extranet-Design und Vorgaben an die Standortkopplung,

- Festlegung, an welchen Stellen des Netzes welche Sicherheitskomponenten wie Firewalls oder IDS/IPS zu platzieren sind und welche Sicherheitsfunktionen diese realisieren müssen,
- Vorgaben für die Netzanbindung der verschiedenen IT-Systeme,
- Netzarchitektur in Virtualisierungs-Hosts, wobei insbesondere Network Virtualization Overlay (NVO) und die Architektur in Vertikal integrierten Systemen (ViS) zu berücksichtigen sind,
- Festlegungen der grundsätzlichen Architektur-Elemente für eine Private Cloud sowie Absicherung der Anbindungen zu Virtual Private Clouds, Hybrid Clouds und Public Clouds sowie
- Architektur zur sicheren Administration und Überwachung der IT-Infrastruktur.

NET.1.1.A17 Spezifikation des Netzdesigns (S)

Basierend auf der Netzarchitektur SOLLTE das Netzdesign für die Zonen inklusive internem Netz, DMZ-Bereich und Außenanbindungen entwickelt und nachhaltig gepflegt werden. Dafür SOLLTEN die relevanten Architekturelemente detailliert betrachtet werden, mindestens jedoch:

- zulässige Formen von Netzkomponenten inklusive virtualisierter Netzkomponenten,
- Festlegungen darüber, wie WAN- und Funkverbindungen abzusichern sind,
- Anbindung von Endgeräten an Switching-Komponenten, Verbindungen zwischen Netzelementen sowie Verwendung von Kommunikationsprotokollen,
- Redundanzmechanismen für alle Netzelemente,
- Adresskonzept für IPv4 und IPv6 sowie zugehörige Routing- und Switching-Konzepte,
- virtualisierte Netze in Virtualisierungs-Hosts inklusive NVO,
- Aufbau, Anbindung und Absicherung von Private Clouds sowie sichere Anbindung von Virtual Private Clouds, Hybrid Clouds und Public Clouds sowie
- Festlegungen zum Netzdesign für die sichere Administration und Überwachung der IT-Infrastruktur.

NET.1.1.A18 P-A-P-Struktur für die Internet-Anbindung (S)

Das Netz der Institution SOLLTE über eine Firewall mit P-A-P-Struktur an das Internet angeschlossen werden (siehe NET.1.1.A4 *Netztrennung in Zonen*).

Zwischen den beiden Firewall-Stufen MUSS ein proxy-basiertes Application-Layer-Gateway (ALG) realisiert werden. Das ALG MUSS über ein eigenes Transfernetz (dual-homed) sowohl zum äußeren Paketfilter als auch zum internen Paketfilter angebunden werden. Das Transfernetz DARF NICHT mit anderen Aufgaben als denjenigen für das ALG belegt sein.

Falls kein ALG eingesetzt wird, dann MÜSSEN entsprechende Sicherheits-Proxies realisiert werden. Die Sicherheits-Proxies MÜSSEN über ein eigenes Transfernetz (dual-homed) angebunden werden. Das Transfernetz DARF NICHT mit anderen Aufgaben als denjenigen für die Sicherheits-Proxies belegt sein. Es MUSS geprüft werden, ob über die Sicherheits-Proxies gegenseitige Angriffe möglich sind. Ist dies der Fall, MUSS das Transfernetz geeignet segmentiert werden.

Jeglicher Datenverkehr MUSS über das ALG oder entsprechende Sicherheits-Proxies entkoppelt werden. Ein Transfernetz, das beide Firewall-Stufen direkt miteinander verbindet, DARF NICHT konfiguriert werden. Die interne Firewall MUSS zudem die Angriffsfläche des ALGs oder der Sicherheits-Proxies gegenüber Innentätern oder IT-Systemen im internen Netz reduzieren.

Authentisierte und vertrauenswürdige Netzzugriffe vom VPN-Gateway ins interne Netz SOLLTEN NICHT das ALG oder die Sicherheits-Proxies der P-A-P-Struktur durchlaufen.

NET.1.1.A19 Separierung der Infrastrukturdienste (S)

Server, die grundlegende Dienste für die IT-Infrastruktur bereitstellen, SOLLTEN in einem dedizierten Netzsegment positioniert werden. Die Kommunikation mit ihnen SOLLTE durch einen

zustandsbehafteten Paketfilter (Firewall) kontrolliert werden.

NET.1.1.A20 Zuweisung dedizierter Subnetze für IPv4/IPv6-Endgerätegruppen (S)
Unterschiedliche IPv4-/IPv6- Endgeräte SOLLTEN je nach verwendetem Protokoll (IPv4-/IPv6- oder IPv4/IPv6-DualStack) dedizierten Subnetzen zugeordnet werden.

NET.1.1.A21 Separierung des Management-Bereichs (S)
Um die Infrastruktur zu managen, SOLLTE durchgängig ein Out-of-Band-Management genutzt werden. Dabei SOLLTEN alle Endgeräte, die für das Management der IT-Infrastruktur benötigt werden, in dedizierten Netzsegmenten positioniert werden. Die Kommunikation mit diesen Endgeräten SOLLTE durch einen zustandsbehafteten Paketfilter kontrolliert werden. Die Kommunikation von und zu diesen Management-Netzsegmenten SOLLTE auf die notwendigen Management-Protokolle mit definierten Kommunikations-Endpunkten beschränkt werden.

Der Management-Bereich SOLLTE mindestens die folgenden Netzsegmente umfassen. Diese SOLLTEN abhängig von der Sicherheitsrichtlinie und der Anforderungsspezifikation weiter unterteilt werden in

- Netzsegment(e) für IT-Systeme, die für die Authentisierung und Autorisierung der administrativen Kommunikation zuständig sind,
- Netzsegment(e) für die Administration der IT-Systeme,
- Netzsegment(e) für die Überwachung und das Monitoring,
- Netzsegment(e), die die zentrale Protokollierung inklusive Syslog-Server und SIEM-Server enthalten,
- Netzsegment(e) für IT-Systeme, die für grundlegende Dienste des Management-Bereichs benötigt werden sowie
- Netzsegment(e) für die Management-Interfaces der zu administrierenden IT-Systeme.

Die verschiedenen Management-Interfaces der IT-Systeme MÜSSEN nach ihrem Einsatzzweck und ihrer Netzplatzierung über einen zustandsbehafteten Paketfilter getrennt werden. Dabei SOLLTEN die IT-Systeme (Management-Interfaces) zusätzlich bei folgender Zugehörigkeit über dedizierte Firewalls getrennt werden:

- IT-Systeme, die aus dem Internet erreichbar sind,
- IT-Systeme im internen Netz sowie
- Sicherheitskomponenten, die sich zwischen den aus dem Internet erreichbaren IT-Systemen und dem internen Netz befinden.

Es MUSS sichergestellt werden, dass die Segmentierung nicht durch die Management-Kommunikation unterlaufen werden kann. Eine Überbrückung von Netzsegmenten MUSS ausgeschlossen werden.

NET.1.1.A22 Spezifikation des Segmentierungskonzepts (S)
Auf Basis der Spezifikationen von Netzarchitektur und Netzdesign SOLLTE ein umfassendes Segmentierungskonzept für das interne Netz erstellt werden. Dieses Segmentierungskonzept SOLLTE eventuell vorhandene virtualisierte Netze in Virtualisierungs-Hosts beinhalten. Das Segmentierunskonzept SOLLTE geplant, umgesetzt, betrieben und nachhaltig gepflegt werden. Das Konzept SOLLTE mindestens die folgenden Punkte umfassen, soweit diese in der Zielumgebung vorgesehen sind:

- Initial anzulegende Netzsegmente und Vorgaben dazu, wie neue Netzsegmente zu schaffen sind und wie Endgeräte in den Netzsegmenten zu positionieren sind,
- Festlegung für die Segmentierung von Entwicklungs- und Testsystemen (Staging),
- Netzzugangskontrolle für Netzsegmente mit Clients,
- Anbindung von Netzbereichen, die über Funktechniken oder Standleitung an die Netzsegmente

angebunden sind,

- Anbindung der Virtualisierungs-Hosts und von virtuellen Maschinen auf den Hosts an die Netzsegmente,
- Rechenzentrumsautomatisierung sowie
- Festlegungen dazu, wie Endgeräte einzubinden sind, die mehrere Netzsegmente versorgen, z. B. Load Balancer, und Speicher- sowie Datensicherungslösungen.

Abhängig von der Sicherheitsrichtlinie und der Anforderungsspezifikation SOLLTE für jedes Netzsegment konzipiert werden, wie es netztechnisch realisiert werden soll. Darüber hinaus SOLLTE festgelegt werden, welche Sicherheitsfunktionen die Koppelelemente zwischen den Netzsegmenten bereitstellen müssen (z. B. Firewall als zustandsbehafteter Paketfilter oder IDS/IPS).

NET.1.1.A23 Trennung von Netzsegmenten (S)

IT-Systeme mit unterschiedlichem Schutzbedarf SOLLTEN in verschiedenen Netzsegmenten platziert werden. Ist dies nicht möglich, SOLLTE sich der Schutzbedarf nach dem höchsten vorkommenden Schutzbedarf im Netzsegment richten. Darüber hinaus SOLLTEN die Netzsegmente abhängig von ihrer Größe und den Anforderungen des Segmentierungskonzepts weiter unterteilt werden. Es MUSS sichergestellt werden, dass keine Überbrückung von Netzsegmenten oder gar Zonen möglich ist.

Gehören die virtuellen LANs (VLANs) an einem Switch unterschiedlichen Institutionen an, SOLLTE die Trennung physisch erfolgen. Alternativ SOLLTEN Daten verschlüsselt werden, um die übertragenen Informationen vor unbefugtem Zugriff zu schützen.

NET.1.1.A24 Sichere logische Trennung mittels VLAN (S)

Falls VLANs eingesetzt werden, dann DARF dadurch KEINE Verbindung geschaffen werden zwischen dem internen Netz und einer Zone vor dem ALG oder den Sicherheits-Proxies.

Generell MUSS sichergestellt werden, dass VLANs nicht überwunden werden können.

NET.1.1.A25 Fein- und Umsetzungsplanung von Netzarchitektur und -design (S)

Eine Fein- und Umsetzungsplanung für die Netzarchitektur und das Netzdesign SOLLTE durchgeführt, dokumentiert, geprüft und nachhaltig gepflegt werden.

NET.1.1.A26 Spezifikation von Betriebsprozessen für das Netz (S)

Betriebsprozesse SOLLTEN bedarfsgerecht erzeugt oder angepasst und dokumentiert werden. Dabei SOLLTE insbesondere berücksichtigt werden, wie sich die Zonierung sowie das Segmentierungskonzept auf den IT-Betrieb auswirken.

NET.1.1.A27 Einbindung der Netzarchitektur in die Notfallplanung [IT-Betrieb] (S)

Es SOLLTE initial und in regelmäßigen Abständen nachvollziehbar analysiert werden, wie sich die Netzarchitektur und die abgeleiteten Konzepte auf die Notfallplanung auswirken.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein NET.1.1 *Netzarchitektur und -design* 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.

NET.1.1.A28 Hochverfügbare Netz- und Sicherheitskomponenten (H)

Zentrale Bereiche des internen Netzes sowie die Sicherheitskomponenten SOLLTEN hochverfügbar ausgelegt sein. Dazu SOLLTEN die Komponenten redundant ausgelegt und auch intern hochverfügbar realisiert werden.

NET.1.1.A29 Hochverfügbare Realisierung von Netzanbindungen (H)

Die Netzanbindungen, wie z. B. Internet-Anbindung und WAN-Verbindungen, SOLLTEN vollständig

redundant gestaltet werden. Je nach Verfügbarkeitsanforderung SOLLTEN redundante Anbindungen an einen oder verschiedene Anbieter bedarfsabhängig mit unterschiedlicher Technik und Performance bedarfsgerecht umgesetzt werden. Auch SOLLTE Wegeredundanz innerhalb und außerhalb der eigenen Zuständigkeit bedarfsgerecht umgesetzt werden. Dabei SOLLTEN mögliche Single Points of Failures (SPoF) und störende Umgebungsbedingungen berücksichtigt werden.

NET.1.1.A30 Schutz vor Distributed-Denial-of-Service (H)

Um DDoS-Angriffe abzuwehren, SOLLTE per Bandbreitenmanagement die verfügbare Bandbreite gezielt zwischen verschiedenen Kommunikationspartnern und Protokollen aufgeteilt werden.

Um DDoS-Angriffe mit sehr hohen Datenraten abwehren zu können, SOLLTEN Mitigation-Dienste über größere Internet Service Provider (ISPs) eingekauft werden. Deren Nutzung SOLLTE in Verträgen geregelt werden.

NET.1.1.A31 Physische Trennung von Netzsegmenten (H)

Abhängig von Sicherheitsrichtlinie und Anforderungsspezifikation SOLLTEN Netzsegmente physisch durch separate Switches getrennt werden.

NET.1.1.A32 Physische Trennung von Management-Netzsegmenten (H)

Abhängig von Sicherheitsrichtlinie und Anforderungsspezifikation SOLLTEN Netzsegmente des Management-Bereichs physisch voneinander getrennt werden.

NET.1.1.A33 Mikrosegmentierung des Netzes (H)

Das Netz SOLLTE in kleine Netzsegmente mit sehr ähnlichem Anforderungsprofil und selbem Schutzbedarf unterteilt werden. Insbesondere SOLLTE dies für die DMZ-Segmente berücksichtigt werden.

NET.1.1.A34 Einsatz kryptografischer Verfahren auf Netzebene (H)

Die Netzsegmente SOLLTEN im internen Netz, im Extranet und im DMZ-Bereich mittels kryptografischer Techniken bereits auf Netzebene realisiert werden. Dafür SOLLTEN VPN-Techniken oder IEEE 802.1AE eingesetzt werden.

Wenn innerhalb von internem Netz, Extranet oder DMZ über Verbindungsstrecken kommuniziert wird, die für einen erhöhten Schutzbedarf nicht ausreichend sicher sind, SOLLTE die Kommunikation angemessen auf Netzebene verschlüsselt werden.

NET.1.1.A35 Einsatz von netzbasiertem DLP (H)

Auf Netzebene SOLLTEN Systeme zur Data Lost Prevention (DLP) eingesetzt werden.

NET.1.1.A36 Trennung mittels VLAN bei sehr hohem Schutzbedarf (H)

Bei sehr hohem Schutzbedarf SOLLTEN KEINE VLANs eingesetzt werden.

4 Weiterführende Informationen

4.1 Wissenswertes

Das BSI hat folgende weiterführende Dokumente zum Themenfeld Netze veröffentlicht:

- Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA)
- Technische Leitlinie für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf: BSI-TL-02103 - Version 2.0

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27033 „Information technology – Security techniques — Network security — Part 1: Overview and concepts bis Part 3: Reference networking scenarios – Threats, design techniques and control issues“ Vorgaben für die Absicherung von Netzen.

Anhang J – INF.7 Büroarbeitsplatz

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	Mitarbeiter, Zentrale Verwaltung, Haustechnik, Vorgesetzte

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein INF.7 *Büroarbeitsplatz* vorrangig erfüllt werden:

INF.7.A1 Geeignete Auswahl und Nutzung eines Büroraumes [Vorgesetzte] (B)
Es DÜRFEN NUR geeignete Räume als Büroräume genutzt werden. Die Büroräume MÜSSEN für den Schutzbedarf bzw. das Schutzniveau der dort verarbeiteten Informationen angemessen ausgewählt und ausgestattet sein. Büroräume mit Publikumsverkehr DÜRFEN NICHT in sicherheitsrelevanten Bereichen liegen. Für den Arbeitsplatz und für die Einrichtung eines Büroraumes MUSS die Arbeitsstättenverordnung umgesetzt werden.

INF.7.A2 Geschlossene Fenster und abgeschlossene Türen [Mitarbeiter, Haustechnik] (B)
Wenn Mitarbeiter ihre Büroräume verlassen, SOLLTEN alle Fenster geschlossen werden. Befinden sich vertrauliche Informationen in dem Büroraum, MÜSSEN beim Verlassen die Türen abgeschlossen werden. Dies SOLLTE insbesondere in Bereichen mit Publikumsverkehr beachtet werden. Die entsprechenden Vorgaben SOLLTEN in einer geeigneten Anweisung festgehalten werden. Alle Mitarbeiter SOLLTEN dazu verpflichtet werden, der Anweisung nachzukommen. Zusätzlich MUSS regelmäßig geprüft werden, ob beim Verlassen des Büroraums die Fenster geschlossen und, wenn notwendig, die Türen abgeschlossen werden. Ebenso MUSS darauf geachtet werden, dass Brand- und Rauchschutztüren tatsächlich geschlossen werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein INF.7 *Büroarbeitsplatz*. Sie SOLLTEN grundsätzlich erfüllt werden.

INF.7.A3 Fliegende Verkabelung (S)
Die Stromanschlüsse und Zugänge zum Datennetz im Büroraum SOLLTEN sich dort befinden, wo die IT-Geräte aufgestellt sind. Verkabelungen, die über den Boden verlaufen, SOLLTEN geeignet abgedeckt werden.

INF.7.A4 ENTFALLEN (S)
Diese Anforderung ist entfallen.

INF.7.A5 Ergonomischer Arbeitsplatz [Zentrale Verwaltung, Vorgesetzte] (S)
Die Arbeitsplätze aller Mitarbeiter SOLLTEN ergonomisch eingerichtet sein. Vor allem die Bildschirme SOLLTEN so aufgestellt werden, dass ein ergonomisches und ungestörtes Arbeiten möglich ist. Dabei SOLLTE beachtet werden, dass Bildschirme nicht durch Unbefugte eingesehen werden können. Die Bildschirmarbeitsschutzverordnung (BildscharbV) SOLLTE umgesetzt werden. Alle Arbeitsplätze SOLLTEN für eine möglichst fehlerfreie Bedienung der IT individuell verstellbar sein.

INF.7.A6 Aufgeräumter Arbeitsplatz [Mitarbeiter, Vorgesetzte] (S)
Jeder Mitarbeiter SOLLTE dazu angehalten werden, seinen Arbeitsplatz aufgeräumt zu hinterlassen. Die

Mitarbeiter SOLLTEN dafür sorgen, dass Unbefugte keine vertraulichen Informationen einsehen können. Alle Mitarbeiter SOLLTEN ihre Arbeitsplätze sorgfältig überprüfen und sicherstellen, dass keine vertraulichen Informationen frei zugänglich sind. Vorgesetzte SOLLTEN Arbeitsplätze sporadisch daraufhin überprüfen, ob dort schutzbedürftige Informationen offen zugreifbar sind.

INF.7.A7 Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger [Mitarbeiter, Haustechnik] (S)

Die Mitarbeiter SOLLTEN angewiesen werden, vertrauliche Dokumente und Datenträger verschlossen aufzubewahren, wenn sie nicht verwendet werden. Dafür SOLLTEN geeignete Behältnisse in den Büroräumen oder in deren Umfeld aufgestellt werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein INF.7 *Büroarbeitsplatz* 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.

INF.7.A8 Einsatz von Diebstahlsicherungen [Mitarbeiter] (H)

Wenn der Zutritt zu den Räumen nicht geeignet beschränkt werden kann, SOLLTEN für alle IT-Systeme Diebstahlsicherungen eingesetzt werden. In Bereichen mit Publikumsverkehr SOLLTEN Diebstahlsicherungen benutzt werden.

4 Weiterführende Informationen

4.1 Wissenswertes

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ im Kapitel CF19 Vorgaben zur physischen Sicherheit und Umgebungssicherheit von Gebäuden und Räumen.

Das Deutsche Institut für Normung macht in seiner Norm „DIN EN 1627:2011-09“ Vorgaben zur physischen Sicherheit von Gebäuden und Räumen.

Das Bundesministerium für Arbeit und Soziales macht in seiner Arbeitsstättenverordnung Vorgaben zum Einrichten und Betreiben von Arbeitsstätten in Bezug auf die Sicherheit und den Schutz der Gesundheit von Beschäftigten.

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 INF.7 *Büroarbeitsplatz* von Bedeutung.

G 0.2	Ungünstige klimatische Bedingungen
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

Selbständigkeitserklärung

„Ich erkläre hiermit, dass ich diese Thesis selbständig verfasst und keine andern als die angegebenen Quellen benutzt habe. Alle Stellen, die wörtlich oder sinngemäss aus Quellen entnommen wurden, habe ich als solche kenntlich gemacht. Ich versichere zudem, dass ich bisher noch keine wissenschaftliche Arbeit mit gleichem oder ähnlichem Inhalt an der Fernfachhochschule Schweiz oder an einer anderen Hochschule eingereicht habe. Mir ist bekannt, dass andernfalls die Fernfachhochschule Schweiz zum Entzug des aufgrund dieser Thesis verliehenen Titels berechtigt ist.“

Ort, Datum, Unterschrift