Bundesamt
für Sicherheit in der
Informationstechnik

OPS.1.1.1 Allgemeiner IT-Betrieb

1. Beschreibung

1.1. Einleitung

Der IT-Betrieb (engl. IT Operations) stellt eine Organisationseinheit und den zugehörigen Geschäftsprozess innerhalb der Informationstechnik dar. Der Prozess beschreibt die Aufgaben mit allen Tätigkeiten, die durch die Organisationseinheit IT-Betrieb umgesetzt werden. Die IT umfasst alle IT-Komponenten einer Institution, insbesondere IT-Systeme, -Dienste, -Anwendungen, -Plattformen und Netze. Zum IT-Betrieb zählen unter anderem die folgenden Aufgaben:

- die Verwaltung, inklusive Inventarisierung und Dokumentation
- die Mitwirkung bei der Beschaffung
- die In- und Außerbetriebnahme, inklusive Austausch von IT
- die IT-Administration
- das IT-Monitoring
- das IT Incident Management

Die ordnungsgemäße, sichere und korrekte Ausführung des IT-Betriebs ist unabdingbar, um die Funktionsfähigkeit der IT zu gewährleisten. Hierzu legt der IT-Betrieb Rahmenbedingungen beispielsweise für die Prozessgestaltung fest und stellt sicher, dass diese eingehalten werden.

Außerdem muss der IT-Betrieb auch die eigenen verwendeten Betriebsmittel, also die spezifischen IT-Komponenten, die für betriebliche Zwecke des IT-Betriebs eingesetzt werden, in angemessenem Umfang zur Verfügung stellen und deren Funktionsfähigkeit gewährleisten. Die betriebene IT umfasst also immer auch die Betriebsmittel des IT-Betriebs selbst. Diesen Betriebsmitteln kommt aus Sicherheitsperspektive eine besondere Bedeutung zu. Auf ihnen werden viele für die IT-Komponenten und deren Funktionsfähigkeit wichtige Informationen vorgehalten, die ein attraktives Ziel für einen Angriff bieten und daher geschützt werden müssen. Außerdem ist ihre Verfügbarkeit für den IT-Betrieb wesentlich.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, die Informationssicherheit als integralen Bestandteil bei allen allgemein gültigen Aspekten des IT-Betriebs zu etablieren. Mit der Umsetzung dieses Bausteins sorgt die Institution dafür, dass die Tätigkeiten des allgemeinen IT-Betriebs, durch die die Funktionsfähigkeit der IT sichergestellt wird, ordnungsgemäß und systematisch durchgeführt werden.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.1.1.1 *Allgemeiner IT-Betrieb* ist einmal auf den gesamten Informationsverbund anzuwenden.

Um ein IT-Grundschutz-Modell für einen konkreten Informationsverbund zu erstellen, muss grundsätzlich die Gesamtheit aller Bausteine betrachtet werden. In der Regel sind mehrere Bausteine auf das Thema bzw. Zielobjekt anzuwenden.

Dieser Baustein behandelt übergreifende Aspekte des IT-Betriebs. In größeren Institutionen ist es sinnvoll, darüber hinaus den IT-Betrieb in das Service-Management der Institution einzubetten. Hierzu können Standardwerke, wie z. B. die „Information Technology Infrastructure Library" (ITIL), herangezogen werden. Ein solches Service Management ist nicht auf die IT beschränkt (IT-Service-Management), sondern adressiert auch Geschäftsprozesse und Fachaufgaben wie „Portfolio Management".

Folgende Inhalte sind ebenfalls von Bedeutung und werden an anderer Stelle behandelt:

- spezielle Aspekte des IT-Betriebs aus weiteren Bausteinen der Schicht OPS.1.1 *Kern-IT-Betrieb,* insbesondere die Durchführung der Administration (siehe OPS.1.1.2 *Ordnungsgemäße IT-Administration*) und Tätigkeiten im Patch- und Änderungsmanagement (siehe OPS.1.1.3 *Patch- und Änderungsmanagement*)
- Aspekte des Netz- und Systemmanagements (siehe NET.1.2 *Netzmanagement* und OPS.1.1.7 *Systemmanagement*)
- die ordnungsgemäße Verwaltung von Benutzenden und Rechten (siehe ORP.4 *Identitäts- und Berechtigungsmanagement*)
- Aspekte der Datensicherung und Archivierung (siehe CON.3 *Datensicherungskonzept* und OPS.1.2.2 *Archivierung*)
- Aspekte, die sich nicht auf den Regelbetrieb, sondern auf Ausnahmesituationen beziehen, insbesondere auf einen IT-Angriff und die Kompromittierung von IT-Systemen (Incident Management, siehe Baustein DER.1 *Detektion von sicherheitsrelevanten Ereignissen* sowie Bausteine aus dem Bereich DER.2 *Security Incident Management* und Baustein DER.4 *Notfallmanagement*)
- besondere Anforderungen für den Fall, dass der IT-Betrieb durch Dritte erfolgt (siehe OPS.2.3 *Nutzung von Outsourcing* und OPS.3.2 *Anbieten von Outsourcing*)

Dieser Baustein behandelt **nicht**

- den Teil des Betriebs von IT-Komponenten, für den nicht der IT-Betrieb, sondern z. B. eine Fachabteilung zuständig ist,
- spezielle Aspekte von DevOps,
- Aspekte, die kennzeichnend für den IT-Service sind, beispielsweise die Schnittstelle zu Benutzenden oder die Bereitstellung einer Hotline, sowie
- die Umsetzung von IT-Projekten.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.1.1.1 *Allgemeiner IT-Betrieb* von besonderer Bedeutung.

2.1. Unzureichende Personalkapazitäten

Das Betriebspersonal ist dafür zuständig, dass die gesamte IT funktionsfähig ist, ohne die Institutionen häufig nicht mehr operabel sind. Die IT ist besonders gefährdet, falls der IT-Betrieb nicht über ausreichende Kapazitäten verfügt.

Herrscht Personalmangel, z. B. aufgrund fehlerhafter oder unzureichender Personalplanung, können Prozesse des IT-Betriebs nicht ordnungsgemäß ausgeführt werden. Dabei können neben der Verfügbarkeit auch die Vertraulichkeit und Integrität des Informationsverbundes eingeschränkt werden, z. B. wenn aufgrund von Personalmangel kein geeignetes IT-Monitoring oder Security Monitoring erfolgt.

Ist das benötigte Know-how beim Betriebspersonal nicht ausreichend redundant verfügbar, da weiteres Personal beispielsweise nur unzureichend geschult wurde, kann die Abhängigkeit von einzelnen Personen dazu führen, dass die Verfügbarkeit des IT-Betriebs nicht mehr vollständig gewährleistet ist.

2.2. Verlust betriebsrelevanter Informationen

Prozesse, die durch den IT-Betrieb unzureichend ausgeführt werden, können dazu führen, dass betriebsrelevante Informationen veraltet sind oder gar verloren gehen.

Führt der IT-Betrieb Tätigkeiten aus, die auf einer unzureichenden oder manipulierten Dokumentation basieren, kann dies zu Störungen der IT-Funktionalität führen. Sind darüber hinaus die Informationen, die benötigt werden um einen Störfall zu beheben, nur unzureichend vorhanden, können diese Störungen nicht oder nur fehlerhaft behoben werden. Als Folge unzureichender Dokumentation kann sowohl die Verfügbarkeit der IT-Komponenten als auch die Vertraulichkeit der Informationen beeinträchtigt werden.

Werden die betriebsrelevanten Informationen unzureichend abgesichert, z. B. indem sie offengelegt oder leicht zugänglich sind, ist deren Vertraulichkeit nicht mehr gewährleistet.

Eine Ursache für den Verlust betriebsrelevanter Informationen kann z. B. eine unzureichende Abstimmung mit den beauftragten Dienstleistenden über die zu liefernde Dokumentation sein, was in den oben genannten Konsequenzen resultieren kann.

2.3. Eingeschränkte Verfügbarkeit von Betriebsmitteln

Betriebsmittel, worunter sämtliche IT-Komponenten zusammengefasst werden, mit denen die Tätigkeiten des IT-Betriebs erbracht werden, haben einen erheblichen Einfluss darauf, dass IT-Betriebsprozesse effizient durchgeführt werden können.

Sind die Betriebsmittel unzureichend redundant ausgelegt, nur eingeschränkt gehärtet oder überlastet, kann hierdurch die Verfügbarkeit eingeschränkt sein. Falls Betriebsmittel nicht ausreichend verfügbar sind, können z. B. aufgetretene Fehler an betriebenen IT-Komponenten nicht behoben werden, wodurch die Verfügbarkeit, Integrität oder Vertraulichkeit der betriebenen IT-Komponenten gefährdet wird.

2.4. Missbrauch betriebsrelevanter Informationen und privilegierter Rechte durch berechtigte Personen

Privilegierte Rechte des Betriebspersonals ermöglichen weitreichende Auswirkungen auf die gesamte IT. Werden betriebsrelevante Informationen und privilegierte Rechte durch berechtigte Personen missbraucht, um zu sabotieren, zu manipulieren oder Informationen auszuspähen, sind alle Schutzziele der Informationssicherheit für die betriebenen IT-Komponenten und für die Informationen der Institution gefährdet. Diese Ausgangslage kann mehrere Ursachen haben.

Verfügt das Betriebspersonal über zu weit gefasste privilegierte Rechte, können diese Berechtigungen für Angriffe missbraucht werden. Auch kann durch Nötigung, Phishing oder Social Engineering erzwungen werden, dass weitreichende Rechte freigegeben oder betriebsrelevante Informationen preisgegeben werden.

Wenn internes oder externes Betriebspersonal ausscheidet und die entsprechenden Prozesse unzureichend ausgeführt werden, können solche Personen weiterhin die privilegierten Rechte nutzen. Ebenso können Sammel-Accounts bewirken, dass z. B. beim Wechsel des Arbeitsfeldes weiterhin Zugang zu betriebsrelevanten Informationen und Betriebsmitteln gewährt wird.

Betriebsrelevante Informationen können auch durch menschliche Fehler preisgegeben werden, indem beispielsweise Regelungen nicht umgesetzt werden, die Ausspähung oder Diebstahl verhindern.

2.5. Erreichbarkeit oder Ausspähen von Betriebsmitteln und betriebsrelevanten Informationen durch Unbefugte

Besteht kein ausreichender Schutz gegen unbefugte Zutritte zu Räumlichkeiten, in denen Betriebsmittel positioniert sind, kann dies als Ausgangspunkt für jede Art von Angriffen bzw. Missbrauch ausgenutzt werden. Folglich können alle Schutzziele der Informationssicherheit beeinträchtigt werden.

Schnittstellen bzw. Zugänge des IT-Betriebs, die unzureichend abgesichert werden, können begünstigen, dass unbefugte Personen Betriebsmittel und betriebsrelevante Informationen erreichen oder ausspähen können.

2.6. Fehlleiten des IT-Betriebs

Spiegeln interne oder externe Personen dem IT-Betrieb bewusst falsche Tatsachen vor, indem sich diese z. B. fälschlicherweise als andere Person ausgeben, kann der IT-Betrieb zu falschen Reaktionen verleitet werden. Dabei können z. B. Phishing E-Mails, die an den IT-Betrieb gesendet werden, inkorrekte Tätigkeiten auslösen. Abhängig davon, wie der IT-Betrieb fehlgeleitet wird, können alle Schutzziele der Informationssicherheit erheblich gefährdet werden. Die Verfügbarkeit kann eingeschränkt werden, wenn zum Beispiel die Administrierenden dazu verleitet werden, IT-Systeme auszuschalten.

2.7. Verhinderung von Betriebsprozessen

Werden die Tätigkeiten des IT-Betriebs blockiert und somit nicht ordnungsgemäß ausgeführt, kann hierdurch die Verfügbarkeit und die Integrität der gesamten IT beeinträchtigt werden.

Eine mögliche Ursache kann eine unzureichende Konzeptionierung und Beschaffung von IT-Komponenten sein, indem z. B. nicht berücksichtigt wurde, ob die Anwendungen gut betrieben werden können. Ebenso kann die Fehlplanung von Prozessen, z. B. durch unklare Schnittstellen oder Zuständigkeiten, dazu führen, dass der IT-Betrieb nur unzureichend ausgeführt wird.

Auch inkorrekt ausgeführte Tätigkeiten des Betriebspersonals, die z. B. auf unzureichendes Know-how über Betriebsprozesse zurückzuführen sind, können bewirken, dass Betriebsprozesse verhindert werden und dadurch die gesamte IT nur noch eingeschränkt verfügbar bzw. funktionstüchtig ist.

Ebenso kann das Verhalten des Betriebspersonals oder die Tätigkeiten von verschiedenen Dienstleistenden mit nicht klar abgegrenzten Schnittstellen verhindern, dass Betriebsprozesse korrekt ausgeführt werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.1.1.1 *Allgemeiner IT-Betrieb* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Keine

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

OPS.1.1.1.A1 Festlegung der Aufgaben und Zuständigkeiten des IT-Betriebs (B)

Für alle betriebenen IT-Komponenten MUSS festgelegt werden, welche Aufgaben für den IT-Betrieb anfallen und wer dafür zuständig ist. Hierfür MÜSSEN die entsprechenden Rechte, Pflichten, Aufgaben mit den hierfür erforderlichen Tätigkeiten, Befugnisse und zugehörigen Prozesse geregelt werden. Weiterhin MÜSSEN die Schnittstellen und Meldewege sowie das Eskalationsmanagement zwischen verschiedenen Betriebseinheiten und gegenüber anderen organisatorischen Einheiten der Institution festgelegt werden.

OPS.1.1.1.A2 Festlegung von Rollen und Berechtigungen für den IT-Betrieb (B)

Für alle betriebenen IT-Komponenten MUSS das jeweilige Rollen- und Berechtigungskonzept auch Rollen und zugehörige Berechtigungen für den IT-Betrieb festlegen. Für die Betriebsmittel MUSS ebenfalls ein Rollen- und Berechtigungskonzept erstellt werden.

Das Rollen- und Berechtigungskonzept für den IT-Betrieb MUSS die IT-Nutzung von IT-Betriebsaufgaben trennen. Administrationsaufgaben und sonstige Betriebsaufgaben MÜSSEN durch unterschiedliche Rollen getrennt werden. Grundsätzlich SOLLTE der IT-Betrieb für unterschiedliche Betriebstätigkeiten unterschiedliche Rollen festlegen, die für die jeweiligen Tätigkeiten die erforderlichen Berechtigungen besitzen. Sammel-Accounts DÜRFEN NUR in begründeten Ausnahmefällen eingerichtet werden.

Die Rollen und Berechtigungen MÜSSEN regelmäßig geprüft und auf die aktuellen Gegebenheiten angepasst werden. Insbesondere MÜSSEN die Berechtigungen von ausgeschiedenem Personal auf den IT-Komponenten entfernt werden. Ebenso MÜSSEN die Rollen und Berechtigungen gelöscht werden, wenn IT-Komponenten außer Betrieb genommenen werden.

3.2. Standard-Anforderungen

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

OPS.1.1.1.A3 Erstellen von Betriebshandbüchern für die betriebene IT (S)

Für alle betriebenen IT-Komponenten SOLLTEN die Betriebsaufgaben geplant und in Betriebshandbüchern erfasst werden. Die Betriebshandbücher SOLLTEN stets verfügbar sein und mindestens die folgenden Themen adressieren:

- relevante System- und Kontaktinformationen
- erforderliche und zulässige Betriebsmittel
- allgemeine Konfigurationsvorgaben
- Konfigurationsvorgaben zur Härtung von Spezialsystemen
- Rollen- und Berechtigungen
- IT-Monitoring, Protokollierung und Alarmierung
- Datensicherung und Notfallkonzepte
- IT Incident Management
- Vorgaben für alle regelmäßigen und außerplanmäßigen Tätigkeiten

Die Betriebshandbücher SOLLTEN regelmäßig und anlassbezogen geprüft und angepasst werden.

OPS.1.1.1.A4 Bereitstellen ausreichender Personal- und Sachressourcen (S)

Der IT-Betrieb SOLLTE über ausreichende Personal-Ressourcen verfügen, um einen ordnungsgemäßen IT-Betrieb gewährleisten zu können. Hierfür SOLLTE der Aufwand für alle Tätigkeiten des IT-Betriebs ermittelt werden. Die Personal-Ressourcen SOLLTEN mit angemessenen Redundanzen und Reserven geplant werden und auch kurzfristige Personalausfälle sowie temporär erhöhte Personalbedarfe berücksichtigen.

Ebenfalls SOLLTEN geeignete Sach-Ressourcen bereitstehen. Hierfür SOLLTE für jede Tätigkeit des IT-Betriebs identifiziert werden, welche Betriebsmittel erforderlich sind.

Die Ressourcenplanung SOLLTE regelmäßig und anlassbezogen überprüft und an die aktuellen Erfordernisse angepasst werden.

OPS.1.1.1.A5 Festlegen von gehärteten Standardkonfigurationen (S)

Der IT-Betrieb SOLLTE die betriebenen IT-Komponenten kategorisieren und für diese Kategorien gehärtete Standardkonfigurationen festlegen und bereitstellen.

Für IT-Plattformen wie Virtualisierungshosts, auf denen weitere IT-Komponenten bereitgestellt und betrieben werden, SOLLTE eine abgestimmte Härtung entwickelt und umgesetzt werden, die alle Elemente der IT-Komponenten berücksichtigt. Hierbei SOLLTEN verschiedene Ausprägungen der IT-Komponenten berücksichtigt und erlaubte Abweichungen spezifiziert werden.

Die Konfigurationsvorgaben SOLLTEN die Sicherheitsanforderungen der Institution umsetzen und die Empfehlungen der jeweiligen Herstellenden berücksichtigen. Die gehärteten Standard-Konfigurationen SOLLTEN in den jeweiligen Betriebshandbüchern dokumentiert werden.

Jede Standardkonfiguration SOLLTE vor Bereitstellung getestet werden. Die gehärteten Standardkonfigurationen SOLLTEN regelmäßig und anlassbezogen geprüft und gemäß der verfügbaren Informationen an den aktuellen Stand der Technik angepasst werden.

Der IT-Betrieb SOLLTE gewährleisten, dass die aktuellen Konfigurationsvorgaben stets verfügbar sind und über eine Versionierung und eine Beschreibung identifizierbar sind.

OPS.1.1.1.A6 Durchführung des IT-Asset-Managements (S)

Der IT-Betrieb SOLLTE eine Übersicht aller vorhandenen IT-Assets erstellen, regelmäßig prüfen und aktuell halten.

Im IT-Asset-Management (ITAM) SOLLTEN alle produktiven IT-Komponenten, Test-Instanzen und IT-Komponenten der Reservevorhaltung erfasst werden. Auch vorhandene, aber nicht mehr genutzte IT-Assets SOLLTEN erfasst werden.

Es SOLLTEN ITAM-Tools eingesetzt werden, die eine zentrale Verwaltung der IT-Assets ermöglichen.

OPS.1.1.1.A7 Sicherstellung eines ordnungsgemäßen IT-Betriebs (S)

Der IT-Betrieb SOLLTE für alle IT-Komponenten Betriebskonzepte entwickeln. Diese Betriebskonzepte SOLLTEN regelmäßig geprüft und angepasst werden.

Die sicherheitsrelevanten Vorgaben zur Konfiguration SOLLTEN umgesetzt werden. Dafür SOLLTEN die gehärteten Standard-Konfigurationen genutzt werden.

Der IT-Betrieb SOLLTE für alle Tätigkeiten Prüfkriterien festlegen, die in ihrer Gesamtheit als Leitfaden für den ordnungsgemäßen IT-Betrieb dienen. Die Freigabe von installierten oder geänderten IT-Komponenten in den produktiven Betrieb SOLLTE über diese Prüfkriterien nachgewiesen werden.

Bei Inbetriebnahme und nach Updates oder Umstrukturierungen SOLLTEN Systemtests für die IT-Komponenten durchgeführt werden. Der IT-Betrieb SOLLTE festlegen, in welcher Umgebung die jeweiligen Systemtests mit welcher Testabdeckung und Testtiefe durchgeführt werden.

Der IT-Betrieb SOLLTE Vorkehrungen für die Ersatzbeschaffung von IT-Komponenten treffen. Hierfür SOLLTEN eine Reservevorhaltung oder Lieferverträge vorgesehen werden.

Alle Tätigkeiten des IT-Betriebs SOLLTEN umfassend und nachvollziehbar erfasst werden. Hierfür SOLLTE der IT-Betrieb ein geeignetes Werkzeug wie ein Ticketsystem nutzen.

Der IT-Betrieb SOLLTE insbesondere die Qualität der Betriebsprozesse, die Einhaltung von SLAs und die Zufriedenheit der Benutzenden systematisch erfassen. Es SOLLTEN regelmäßig Reports erstellt werden, die dem Nachweis eines ordnungsgemäßen IT-Betriebs dienen.

OPS.1.1.1.A8 Regelmäßiger Soll-Ist-Vergleich (S)

Der IT-Betrieb SOLLTE regelmäßig und anlassbezogen für alle betriebenen IT-Komponenten sowie für die Betriebsmittel prüfen, ob die aktuelle Konfiguration dem Sollzustand entspricht. Darüber hinaus SOLLTE geprüft werden, ob die gelebten Prozesse die festgelegten Prozesse des IT-Betriebs umsetzen.

OPS.1.1.1.A9 Durchführung von IT-Monitoring (S)

Alle IT-Komponenten SOLLTEN in ein einheitliches IT-Monitoring eingebunden werden, das alle relevanten Parameter der IT-Komponenten beinhaltet. Das IT-Monitoring SOLLTE mit dem übergeordneten Service-Management abgestimmt werden.

Der IT-Betrieb SOLLTE das IT-Monitoring entsprechend eines vorher festgelegten Monitoring-Plans durchführen. Je IT-Komponente SOLLTEN angemessene Schwellwerte ermittelt werden, die eine Meldung oder einen Alarm auslösen.

Der IT-Betrieb SOLLTE für das IT-Monitoring spezifizieren, welche Meldewege genutzt werden und welche Konsequenzen aus den Meldungen oder Alarmen gezogen werden. Auf Basis von Monitoring-Ergebnissen SOLLTE überprüft werden, ob die Infrastruktur erweitert oder angepasst wird. Über die gewonnenen Erkenntnisse SOLLTEN regelmäßig Reports erstellt werden, die das aktuelle Lagebild der betriebenen IT und die zeitliche Entwicklung sowie Trends darstellen.

Die Konzeption des IT-Monitorings SOLLTE regelmäßig und anlassbezogen geprüft und aktualisiert werden, um dem aktuellen Stand der Technik und der betriebenen Infrastruktur zu entsprechen.

Die Monitoring-Daten SOLLTEN nur über sichere Kommunikationswege übertragen werden.

OPS.1.1.1.A10 Führen eines Schwachstelleninventars (S)

Der IT-Betrieb SOLLTE ein Schwachstelleninventar führen, in dem die Schwachstellen aller betriebenen IT-Komponenten und der Umgang mit diesen zentral erfasst und gepflegt werden.

Der IT-Betrieb SOLLTE die Behandlung der Schwachstellen initiieren, nachhalten und sicherstellen. Es SOLLTE ein Prozess definiert werden, der den Umgang mit den Schwachstellen festlegt. Mindestens SOLLTE spezifiziert werden,

- bis wann ein verfügbares Update, in dem die Schwachstelle behoben ist, zu installieren ist,
- in welchen Fällen und bis wann IT-Komponenten mit Schwachstellen außer Betrieb genommen oder ersetzt werden und
- ob und wie solche IT-Komponenten separiert werden, falls weder ein Ersatz noch ein Update möglich ist.

OPS.1.1.1.A11 Festlegung und Einhaltung von SLAs (S)

Für alle IT-Komponenten und alle Tätigkeiten SOLLTE der IT-Betrieb Service Level Agreements (SLAs) definieren und überwachen, die dem Schutzbedarf der IT-Komponenten entsprechen und innerhalb der Institution abgestimmt sind. Die festgelegten SLAs SOLLTEN die Rollen und Berechtigungen sowie eventuelle Abhängigkeiten der jeweiligen Tätigkeit von anderen Organisationseinheiten berücksichtigen.

OPS.1.1.1.A12 Spezifikation und Umsetzung klarer Betriebsprozesse (S)

Der IT-Betrieb SOLLTE für alle Aufgaben Betriebsprozesse spezifizieren, die für die jeweilige Aufgabe alle Tätigkeiten und Abhängigkeiten umfassen und gewährleisten, dass die Tätigkeiten des IT-Betriebs nachvollziehbar sind.

Es SOLLTE für jeden Prozess festgelegt werden, wer den Prozess initiieren darf und wer diesen umsetzt. Für jeden Prozess SOLLTEN die organisatorischen Schnittstellen zu anderen Gruppen des IT-Betriebs oder anderen Organisationseinheiten spezifiziert werden.

Das Personal des IT-Betriebs SOLLTE für die relevanten Betriebsprozesse eingewiesen werden.

Wenn Prozesse durchlaufen wurden, SOLLTE dies protokolliert werden. Das Ergebnis des Durchlaufs SOLLTE protokolliert werden. Für jeden Prozessschritt SOLLTE festgelegt werden, ob dokumentiert werden muss, dass er bearbeitet wurde. Darüber hinaus SOLLTE festgelegt werden, wann der Prozess erfolgreich abgeschlossen ist.

Der IT-Betrieb SOLLTE einen Prozess spezifizieren, der grundsätzlich beschreibt, wie mit Situationen umzugehen ist, die nicht in den regulären Betriebsprozessen enthalten sind. Mindestens SOLLTEN Fallback-Prozesse definiert sein und beschrieben werden, wie bei fehlerhaftem oder manipuliertem Betrieb vorzugehen ist.

OPS.1.1.1.A13 Absicherung der Betriebsmittel und der Dokumentation (S)

Auf die Betriebsmittel, die Dokumentation und die Betriebshandbücher SOLLTEN nur berechtigte Personen des IT-Betriebs zugreifen können. Der IT-Betrieb SOLLTE sicherstellen, dass die Betriebsmittel und die Dokumentation zu jeder Zeit verfügbar sind.

Falls die IT-Systeme und -Anwendungen der Betriebsmittel über die produktive Infrastruktur kommunizieren, SOLLTEN sichere Protokolle verwendet werden. Vertrauliche Daten SOLLTEN ausschließlich über sichere Protokolle übertragen werden.

Die Betriebsmittel SOLLTEN in das Schwachstellenmanagement und das IT-Monitoring eingebunden werden.

OPS.1.1.1.A14 Berücksichtigung der Betreibbarkeit bei Konzeption und Beschaffung (S)

Für die IT-Komponenten SOLLTEN Anforderungen für einen effizienten und sicheren Betrieb bereits bei der Konzeption und der Beschaffung berücksichtigt werden. Hierfür SOLLTEN die Anforderungen des IT-Betriebs erhoben und berücksichtigt werden. Der IT-Betrieb SOLLTE dabei auch die Komplexität der IT berücksichtigen.

OPS.1.1.1.A15 Planung und Einsatz von Betriebsmitteln (S)

Der IT-Betrieb SOLLTE für alle IT-Komponenten die Betriebsmittel bedarfsgerecht planen, beschaffen und einsetzen. Der IT-Betrieb SOLLTE die Anforderungen an die jeweiligen Betriebsmittel ermitteln und diese mit den anderen betroffenen Organisationseinheiten der Institution abstimmen.

Die Netze, in denen die Betriebsmittel positioniert sind, SOLLTEN von den sonstigen Netzen der Institution mindestens logisch getrennt werden (siehe Baustein NET.1.1 *Netzarchitektur und -design*). Das Netz für die Betriebsmittel SOLLTE abhängig von Sicherheitsrichtlinie und Funktionsabhängigkeiten weiter unterteilt werden. Als Basis für die weitere Segmentierung SOLLTEN die unterschiedlichen Betriebsgruppen und Zielsysteme verwendet werden.

OPS.1.1.1.A16 Schulung des Betriebspersonals (S)

Für den IT-Betrieb SOLLTE durch einen Schulungsplan sichergestellt werden, dass für alle IT-Komponenten und Betriebsmittel jeweils mehrere Personen die erforderlichen Fähigkeiten und Qualifikationen besitzen. In den Schulungsmaßnahmen SOLLTEN insbesondere die folgenden Themen adressiert werden:

- Härtung und Standard-Konfigurationen
- spezifische Sicherheitseinstellungen für die betriebenen IT-Komponenten und eingesetzten Betriebsmittel
- mögliche Interferenzen zwischen den genutzten Betriebsmitteln
- Abhängigkeiten und Schnittstellen der Prozesse des IT-Betriebs

Wenn neue IT-Komponenten beschafft werden, SOLLTE ein Budget für entsprechende Schulungsmaßnahmen des IT-Betriebs eingeplant werden.

OPS.1.1.1.A17 Planung des IT-Betriebs unter besonderer Berücksichtigung von Mangel- und Notsituationen (S)

Der IT-Betrieb SOLLTE für die betriebenen IT-Komponenten definieren, wann eine Mangel- oder eine Notsituation vorliegt. Für diese Situationen SOLLTE nach den Vorgaben des allgemeinen Notfallmanagements festgelegt werden, welche IT-Komponenten vorrangig betrieben werden oder für einen Mindestbetrieb benötigt werden. Die Notfallplanung SOLLTE die folgenden Punkte beinhalten:

- Disaster-Recovery-Plan
- Notfallhandbuch für die IT-Komponenten unter Einbeziehung der gesamten Infrastruktur
- Umgang mit kritischen und längerfristigen betriebsbehindernden Störungen

OPS.1.1.1.A18 Planung des Einsatzes von Dienstleistenden (S)

Der IT-Betrieb SOLLTE den Einsatz von Dienstleistenden koordinieren und diese unter anderem über SLAs so steuern, dass die Dienstleistung in ausreichendem Maße erbracht wird. Der Einsatz von verschiedenen Dienstleistenden SOLLTE aufeinander abgestimmt werden, insbesondere falls diese für den gleichen Tätigkeitsbereich vorgesehen sind. Für solche Situationen SOLLTE jeweils eine eindeutige Kommunikationsschnittstelle festgelegt werden.

Der IT-Betrieb SOLLTE die Festlegungen zum Dienstleistendenmanagement sowie die für die Dienstleistenden vorgesehenen Tätigkeiten festhalten, regelmäßig prüfen und anpassen.

OPS.1.1.1.A19 Regelungen für Wartungs- und Reparaturarbeiten (S)

IT-Komponenten SOLLTEN regelmäßig gewartet werden. Es SOLLTE geregelt sein, welche Sicherheitsaspekte bei Wartungs- und Reparaturarbeiten zu beachten sind. Es SOLLTE festgelegt werden, wer für die Wartung oder Reparatur von IT-Komponenten zuständig ist. Durchgeführte Wartungs- und Reparaturarbeiten SOLLTEN dokumentiert werden.

Es SOLLTE sichergestellt werden, dass Wartungs- und Reparaturarbeiten, die durch Dritte ausgeführt werden, mit den Beteiligten abgestimmt sind. Es SOLLTEN interne Mitarbeitende des IT-Betriebs bestimmt werden, die solche Arbeiten autorisieren, gegebenenfalls beobachten oder unterstützen und abnehmen.

OPS.1.1.1.A20 Prüfen auf Schwachstellen (S)

Der IT-Betrieb SOLLTE regelmäßig Informationen über bekannt gewordene Schwachstellen bezüglich der IT-Plattformen, Firmware, Betriebssysteme, eingesetzter IT-Anwendungen und Dienste einholen, diese für die konkreten Gegebenheiten analysieren und berücksichtigen.

Die IT-Komponenten SOLLTEN regelmäßig und anlassbezogen auf Schwachstellen getestet werden. Für jede IT-Komponente SOLLTEN die angemessene Test-Abdeckung, -Tiefe und -Methode festgelegt werden.

Die Tests und identifizierten Schwachstellen SOLLTEN nachvollziehbar erfasst werden. Die Schwachstellen SOLLTEN so schnell wie möglich behoben werden. Solange keine entsprechenden Patches zur Verfügung stehen, MÜSSEN für schwerwiegende Schwachstellen und Bedrohungen andere Maßnahmen zum Schutz der IT-Komponente getroffen werden. Falls dies für eine IT-Komponente nicht möglich ist, SOLLTE diese nicht weiter betrieben werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

OPS.1.1.1.A21 Einbinden der Betriebsmittel in das Sicherheitsmonitoring (H)

Die IT-Systeme und -Anwendungen, die als Betriebsmittel genutzt werden, SOLLTEN in ein Sicherheitsmonitoring eingebunden werden.

Falls die Institution ein System zur zentralen Detektion und automatisierten Echtzeitüberprüfung von Ereignismeldungen einsetzt, SOLLTEN die Betriebsmittel darin eingebunden werden. Betriebsmittel wie IT-Management- und IT-Monitoring-Systeme SOLLTEN als Datenquelle für das Sicherheitsmonitoring genutzt werden.

OPS.1.1.1.A22 Automatisierte Tests auf Schwachstellen (H)

Alle IT-Komponenten SOLLTEN regelmäßig und automatisiert auf Schwachstellen getestet werden. Die Ergebnisse der Tests SOLLTEN automatisiert protokolliert und anderen Werkzeugen im Sicherheitsmonitoring bereitgestellt werden.

Bei kritischen Schwachstellen SOLLTE eine automatisierte Alarmierung erfolgen.

OPS.1.1.1.A23 Durchführung von Penetrationstests (H)

Für alle IT-Komponenten SOLLTEN Penetrationstests durchgeführt werden. Hierfür SOLLTE ein Konzept erstellt und umgesetzt werden, das neben den zu verwendenden Testmethoden und Testtiefen auch die Erfolgskriterien festlegt.

OPS.1.1.1.A24 Umfassendes Protokollieren der Prozessschritte im IT-Betrieb (H)

Für die Betriebsprozesse SOLLTE jeder Prozessschritt nachvollziehbar protokolliert werden.

OPS.1.1.1.A25 Sicherstellen von autark funktionierenden Betriebsmitteln (H)

Für die Betriebsmittel SOLLTE sichergestellt werden, dass diese auch bei äußeren Störungen genutzt werden können. Insbesondere SOLLTE eine ausgefallende Internet-Anbindung nicht zu einer Störung der Betriebsmittel führen.

Die Betriebsmittel SOLLTEN so konfiguriert und verortet werden, dass die Abhängigkeiten zwischen den verschiedenen Betriebsmitteln minimiert wird. Es SOLLTE verhindert werden, dass der Ausfall eines Betriebsmittels zu einer betriebsverhindernden Störung eines anderen Betriebsmittels führt.

OPS.1.1.1.A26 Proaktive Instandhaltung im IT-Betrieb (H)

Für die IT-Systeme SOLLTE eine proaktive Instandhaltung durchgeführt werden, in der in festgelegten Intervallen vorbeugende Instandhaltungsmaßnahmen durchgeführt werden.

Ergänzend zu der regelmäßigen Wartung und der proaktiven Instandhaltung SOLLTE je IT-Komponente abgewogen werden, ob eine vorausschauende Instandhaltung (engl. Predictive Maintenance) genutzt wird.

4. Weiterführende Informationen

4.1. Abgrenzung betriebsspezifischer Begriffe

Betriebshandbuch

Ein Betriebshandbuch (BHB) beschreibt je IT-Komponente alle relevanten Maßnahmen und Daten, die für den Betrieb der IT-Komponente notwendig sind. Ein BHB basiert auf dem entsprechenden Betriebskonzept und ist als lebendes Dokument zu betrachten, das fortwährender Aktualisierung und Ergänzung unterliegt.

Betriebskonzept

Ein Betriebskonzept beschreibt für eine gleichartige Gruppe von IT-Komponenten die Betriebsorganisation und die Betriebsprozesse. Das Betriebskonzept bildet die Grundlage für das Betriebshandbuch.

Betriebsprozesse

Ein Betriebsprozess spezifiziert die Tätigkeiten, die zur Erfüllung einer Betriebsaufgabe notwendig sind. Komponentenspezifische Betriebsprozesse können auch als Teil des Betriebshandbuchs definiert werden.

4.2. Wissenswertes

Die Information Technology Infrastructure Library (ITIL) gibt Hinweise (Best Practices) zur Einrichtung und Umsetzung des Service Management einer Institution.

Die International Organization for Standardization (ISO) spezifiziert in der Norm ISO/IEC 20000 die Mindestanforderungen an Prozesse des IT Service Management, um einen messbaren Qualitätsstandard der IT-Services zu gewährleisten. Die Norm ISO/IEC 20000 ist an ITIL ausgerichtet und ergänzt deren Best Practices.

Bundesamt
für Sicherheit in der
Informationstechnik

OPS.1.1.2 Ordnungsgemäße IT-Administration

1. Beschreibung

1.1. Einleitung

Unter IT-Administration werden Tätigkeiten hauptsächlich innerhalb des IT-Betriebs verstanden, für die administrative Rechte benötigt werden und die die Konfiguration von IT-Komponenten verändern. Administrierende sorgen nicht nur dafür, dass die IT-Komponenten verfügbar bleiben, sondern setzen auch Maßnahmen für die Informationssicherheit um und überprüfen, ob diese wirksam sind.

Zu den Tätigkeitsbereichen der Administrierenden gehört es unter anderem, die IT einer Institution einzurichten, zu konfigurieren, zu überprüfen und bestehende IT zu ändern. Hierzu zählt ebenfalls die Fachadministration, also die IT-Administration von Anwendungen, für deren Betrieb der entsprechende Fachbereich statt der Organisationseinheit IT-Betrieb zuständig ist.

Administrative Rechte für IT-Komponenten (also insbesondere für IT-Systeme, IT-Dienste, Anwendungen, IT-Plattformen und Netze) sind privilegierte Rechte, die neben den Zugängen auch Zugriffe über das Netz sowie physikalische Zutritte umfassen können. Daher sind sowohl die administrativen Rechte auf organisatorischer Ebene als auch die Administrationswerkzeuge selber ein attraktives Ziel für Angreifer. Wesentlich für die Sicherheit der IT-Administration sind die ordnungsgemäße und nachvollziehbare Durchführung aller administrativen Tätigkeiten und die Absicherung der dafür benötigten Hilfsmittel.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, die Informationssicherheit als integralen Bestandteil bei der ordnungsgemäßen IT-Administration zu etablieren. Mit der Umsetzung dieses Bausteins sorgt die Institution einerseits dafür, dass die für die Sicherheit des Informationsverbunds erforderlichen Tätigkeiten der IT-Administration ordnungsgemäß und systematisch durchgeführt werden. Andererseits reagiert die Institution damit auch auf die besonderen Gefährdungen, die sich aus dem Umgang mit privilegierten Rechten und aus dem Zugang zu schützenswerten Bereichen der Institution zwangsläufig ergeben.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.1.1.2 *Ordnungsgemäße IT-Administration* ist einmal auf den gesamten Informationsverbund anzuwenden.

Um ein IT-Grundschutz-Modell für einen konkreten Informationsverbund zu erstellen, muss grundsätzlich die Gesamtheit aller Bausteine betrachtet werden. In der Regel sind mehrere Bausteine auf das Thema bzw. Zielobjekt anzuwenden.

Dieser Baustein behandelt

- übergreifende Anforderungen an den Administrationsprozess, sowohl für den IT-Betrieb als auch in der Fachadministration,
- Anforderungen an administrative Tätigkeiten sowie
- Anforderungen an den Umgang mit administrativen Berechtigungen, also privilegierten Zutritten, Zugängen und Zugriffen.

Folgende Inhalte sind ebenfalls von Bedeutung und werden an anderer Stelle behandelt:

- Fernadministration von IT-Systemen über externe Schnittstellen sowie Fernwartung von Geräten und Komponenten durch die Herstellungs- oder Zulieferunternehmen (siehe OPS.1.2.5 *Fernwartung*)
- Patch- und Änderungsmanagement (siehe OPS.1.1.3 *Patch- und Änderungsmanagement*)
- die Absicherung von Administrationswerkzeugen (siehe NET.1.2 *Netzmanagement* und OPS.1.1.7 *Systemmanagement*)
- die ordnungsgemäße Verwaltung von Benutzenden und Berechtigungen (siehe ORP.4 *Identitäts- und Berechtigungsmanagement*)
- besondere Anforderungen für den Fall, dass die IT-Administration durch Dritte erfolgt (siehe OPS.2.3 *Nutzung von Outsourcing* und OPS.3.2 *Anbieten von Outsourcing*)
- Aspekte für die IT-Administration von industrieller IT (siehe Bausteine aus dem Bereich IND *Industrielle IT*)

Dieser Baustein behandelt **nicht**

- die allgemeinen Aspekte des IT-Betriebs wie Inventarisierung, In- und Außerbetriebnahme von IT-Komponenten sowie die grundsätzlichen Rahmenbedingungen für Administrierende (siehe OPS.1.1.1 *Allgemeiner IT-Betrieb*)
- die Einweisung des Personals in einzuhaltende allgemeine Sicherheitsbestimmungen der IT (siehe ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit*)
- die kontinuierliche Schulung des Personals sowie die damit einhergehende Sensibilisierung für Gefährdungen und Sicherheitsmaßnahmen (siehe ORP.2 *Personal* und ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit*)

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.1.1.2 *Ordnungsgemäße IT-Administration* von besonderer Bedeutung.

2.1. Unzureichend geregelte Zuständigkeiten

Die IT-Administration umfasst diverse Aufgaben auf verschiedensten Komponenten unterschiedlicher Bereiche. Fehlen Regelungen über Zuständigkeiten oder Prozesse oder sind die Regelungen und Prozesse den Zuständigen nicht bekannt, kann dies verschiedene mögliche Folgen haben. Gegebenenfalls werden erforderliche Administrationsaufgaben gar nicht oder durch den falschen Bereich erledigt, der gegebenenfalls nicht alle zu beachtenden Einzelheiten kennt. Womöglich werden auch gegenwirkende Maßnahmen von verschiedenen Bereichen durchgeführt. Dies kann bewirken, dass IT-Systeme nur eingeschränkt oder gar nicht mehr verfügbar sind.

Wird bei der Festlegung von Zuständigkeiten nicht beachtet, dass verschiedene IT-Administrationstätigkeiten, z. B. zwischen Applikationsbetrieb und Systembetrieb, untrennbar miteinander verbunden sind, können zusammengehörende Aufgaben gegebenenfalls nicht ordnungsgemäß durchgeführt werden.

Erhalten Administrierende zu viele Rechte, weil Zuständigkeiten nicht geregelt sind, können sie eventuell vertrauliche Informationen einsehen, die sie nicht einsehen dürfen. Dies ist insbesondere der Fall, wenn aus Bequemlichkeit zu viele administrative Konten mit zu weitreichenden Rechten eingerichtet sind, im schlimmsten Fall sogar über Organisationseinheiten hinweg.

Außerdem kann eine zu hohe Anzahl Administrierender zu einem Kontrollverlust führen, wenn nicht klar geregelt ist, wer für welche Aufgaben zuständig ist. In diesem Fall sind alle Schutzziele der Informationssicherheit gefährdet.

2.2. Unzureichende Dokumentation

Die Dokumentation kann unzureichend sein, wenn Informationen über IT-Komponenten (z. B. über Konfiguration oder Zugriffsrechte) nicht oder nur unvollständig erfasst wurden. Auch wenn die Dokumentation im Rahmen von IT-Administrationstätigkeiten nicht aktualisiert wird, ist die Dokumentation unzureichend, weil sie nicht mehr dem Ist-Zustand entspricht.

Unzureichende Dokumentation kann zu Fehlkonfigurationen oder allgemein fehlerhafter IT-Administration führen. Dadurch können alle Schutzziele der Informationssicherheit erheblich gefährdet werden.

Außerdem kann auch das Notfallmanagement erheblich beeinträchtigt werden, weil für zeitkritische Aufgaben erst Informationen gesammelt werden müssen oder die Aufgaben aufgrund der Diskrepanz zwischen Dokumentation und Ist-Zustand nicht wie geplant durchgeführt werden können. Dies kann dazu führen, dass ein Notfall nicht schnell genug behandelt und die Verfügbarkeit von IT-Komponenten länger beeinträchtigt wird.

2.3. Missbrauch von privilegierten Berechtigungen durch Administrierende

Zu weit gefasste administrative Berechtigungen können genutzt werden, um zu sabotieren oder Informationen auszuspähen, die als Ausgangspunkt für Angriffe verwendet werden können. Dadurch werden alle Schutzziele der Informationssicherheit gefährdet.

Privilegierte Zutritte, Zugänge und Zugriffe können auch missbraucht werden, wenn die Prozesse beim Ausscheiden von internen oder externen Administrierenden unzureichend sind und dadurch ausgeschiedene Personen weiterhin auf IT-Komponenten zugreifen können. Auch in diesem Fall sind alle Schutzziele der Informationssicherheit gefährdet.

2.4. Preisgabe von schützenswerten Informationen an unberechtigte Personen

Über Zugänge der IT-Administration kann auf schützenswerte Informationen zugegriffen werden, z. B. auf die Dokumentation, die für die IT-Administration benötigt wird, oder auf die Konfigurationen von IT-Systemen. Werden die Zugänge der IT-Administration unzureichend abgesichert, können auch unberechtigte Personen an schützenswerte Informationen gelangen. Über den Verlust der Vertraulichkeit hinaus können diese Informationen auch manipuliert oder für weitergehende Angriffe genutzt werden, wodurch alle Schutzziele der Informationssicherheit erheblich gefährdet sind.

2.5. Personalausfall von Kernkompetenzträgern

Sind die benötigten Kenntnisse bei den Administrierenden nicht auf allen Gebieten redundant vorhanden, könnte eine entsprechende IT-Administrationstätigkeit nicht durchgeführt werden, wenn Kernkompetenztragende ausfallen. Wenn zusätzlich die Dokumentation für durchzuführende Arbeitsschritte unzureichend ist, kann die IT-Administrationstätigkeit nicht von anderen Administrierenden ohne weitere Risiken durchgeführt werden. Dies kann dazu führen, dass Fehlfunktionen nicht behoben werden können. In der Folge ist die Verfügbarkeit von IT-Systemen nicht (ausreichend) gewährleistet und Schwachstellen können nicht behoben werden, wodurch Angriffe begünstigt werden.

Diese Situation kann auch dadurch entstehen, dass es für IT-Administrationstätigkeiten keine festgelegten Vertretenden mit entsprechenden Berechtigungen gibt oder dass festgelegte Vertretende oder sogar der Notfallzugang nicht über die erforderlichen administrativen Berechtigungen verfügen.

2.6. Unzureichende Verfügbarkeit von Administrierenden

Herrscht bei den Administrierenden Personalmangel, z. B. durch unzureichende Personalplanung, Überbuchung oder Pandemie, können gegebenenfalls erforderliche Administrationsaufgaben nicht durchgeführt werden, falls dazu keine Zeit ist. Unter Umständen werden aufgrund von Zeitmangel auch Fehler bei der IT-Administration gemacht. Beides kann zu unzureichender Verfügbarkeit von IT-Systemen oder zu einer erhöhten Angriffsfläche und damit zur Gefährdung aller Schutzziele der Informationssicherheit führen.

Personalmangel kann zusätzlich zur Folge haben, dass Administrierende aus Zeitmangel für ihre Aufgaben unzureichend geschult werden, was ebenfalls dazu führen kann, dass im Bedarfsfall bzw. im Notfall bestimmte IT-Administrationstätigkeiten nicht korrekt durchgeführt werden.

2.7. Unzureichende Absicherung von Administrationswerkzeugen

Administrationswerkzeuge ermöglichen einen weitreichenden Zugriff auf die IT einer Institution. Werden diese Werkzeuge unzureichend abgesichert, kann das dazu führen, dass die Administrationswerkzeuge als solche bezüglich aller Schutzziele der Informationssicherheit gefährdet sind. Über sie kann die IT-Administration sabotiert werden oder es kann eine unberechtigte IT-Administration ermöglicht werden.

Wird bei einem Angriff Zugriff auf Administrationswerkzeuge erlangt, können weitreichende Berechtigungen erhalten werden. Diese Berechtigungen können für Angriffe aller Art missbraucht werden, wodurch ebenfalls alle Schutzziele der Informationssicherheit gefährdet sind.

Eine Ursache für die unzureichende Absicherung von Administrationswerkzeugen kann z. B. dadurch entstehen, dass sie unzureichend von anderen Anwendungen getrennt sind. Diese unzureichende Trennung ist auf allen Ebenen möglich. Sie kann z. B. dadurch entstehen, dass Texteditoren oder SSH-Clients zur IT-Administration genutzt werden, die auch im nicht-administrativen Kontext verwendet werden.

2.8. Ausfall der Administrationsmöglichkeit

Wenn Administrationsmöglichkeiten ausfallen und es aufgrund von Fehlplanungen keine Redundanz oder andere Alternativen gibt, können IT-Administrationstätigkeiten dieser Art nicht durchgeführt werden, bis der Ausfall behoben ist. Dadurch ist im schlimmsten Fall die gesamte IT eingeschränkt oder nicht verfügbar bzw. funktionstüchtig.

Administrationswerkzeuge können auch durch die Administration des Werkzeuges selbst ausfallen, z. B. durch eine Fehladministration, durch einen eingespielten Patch oder eine Änderung, die durch eine IT-Administrationstätigkeit herbeigeführt wird.

2.9. Fehlgeleitete Administration

Wird die IT-Administration fehlgeleitet, indem z. B. falsche Informationen eingeschleust werden, kann die IT-Administration zu falschen Reaktionen verleitet werden. Beispielsweise können Administrierende außerhalb des geregelten Prozesses fälschlicherweise darüber informiert werden, dass ein IT-System ausgefallen ist, was sie zu einem Neustart verleitet. Hierdurch können Informationen, Hard- oder Software manipuliert werden, wodurch deren Verfügbarkeit und Integrität nicht mehr gewährleistet ist. Zudem können auf diese Weise auch schützenswerte Informationen offengelegt werden.

2.10. Fehlerhafte Administration

Menschliche Fehler können nie ausgeschlossen werden und können bei der IT-Administration weitreichende Folgen haben. Zusätzlich werden sie durch einige der bisher genannten Gefährdungen begünstigt.

Die in der IT-Administration verwendeten Werkzeuge erlauben mit wenig Aufwand sehr weitreichende Änderungen an IT-Komponenten. Je nach Fehler können damit alle Schutzziele der Informationssicherheit erheblich gefährdet sein. Fehler werden insbesondere durch parallele Arbeiten an unterschiedlichen Themen begünstigt, bei denen beispielsweise unterschiedliche Eingabefenster oder Konsolenausgaben verwechselt werden können.

2.11. Störung der IT durch IT-Administrationstätigkeiten

Selbst wenn IT-Administrationstätigkeiten fehlerfrei durchgeführt werden, kann dabei trotzdem die IT der Institution gestört werden. Werden z. B. vorgegebene Wartungsfenster für IT-Administrationstätigkeiten nicht eingehalten, kann die Verfügbarkeit der administrierten IT gestört werden. Zudem können auch korrekt im Wartungsfenster durchgeführte IT-Administrationstätigkeiten später zu Störungen führen, z. B. wenn die Administrierbarkeit der entsprechenden Komponenten durch nicht vorhergesehene Wechselwirkungen beeinträchtigt wird.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.1.1.2 *Ordnungsgemäße IT-Administration* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

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

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

OPS.1.1.2.A1 ENTFALLEN (B)

Diese Anforderung ist entfallen.

OPS.1.1.2.A2 Vertretungsregelungen (B)

Für jede Administrationsaufgabe MUSS eine Vertretung benannt werden. Die Vertretung MUSS über die notwendigen administrativen Berechtigungen (organisatorisch und technisch) verfügen, um die Tätigkeit durchführen zu können. Eine benannte Vertretung MUSS über die im Kontext der Administrationsaufgabe notwendigen Kenntnisse verfügen.

Die Regelung der Vertretung MUSS Mangel- und Notfallsituationen berücksichtigen.

OPS.1.1.2.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

OPS.1.1.2.A4 Beendigung der Tätigkeit in der IT-Administration (B)

Falls eine Person von Administrationsaufgaben entbunden wird, MÜSSEN ihr alle damit zusammenhängenden privilegierten Berechtigungen auf organisatorischer und technischer Ebene entzogen werden. Insbesondere MÜSSEN persönliche administrative Konten gesperrt und Passwörter aller administrativer Konten geändert werden, die der Person bekannt sind. Weiterhin MÜSSEN alle betroffenen Parteien darauf hingewiesen werden, dass diese Person von den entsprechenden Aufgaben entbunden ist und daher keine administrativen Berechtigungen mehr haben darf.

Es MUSS geregelt werden unter welchen Rahmenbedingungen geprüft wird, ob sich zusätzliche nicht dokumentierte administrative Rechte verschafft wurden. Diese Prüfung SOLLTE insbesondere erfolgen, falls die Entscheidung eine Person von Administrationsaufgaben zu entbinden nicht im Einvernehmen mit der entsprechenden Person getroffen wurde. Falls solche administrativen Rechte gefunden wurden, MÜSSEN diese wieder entzogen werden.

OPS.1.1.2.A5 Nachweisbarkeit von administrativen Tätigkeiten (B)

Administrative Tätigkeiten MÜSSEN nachweisbar sein. Dafür MUSS mindestens festgehalten werden,

- welche Änderung bei einer Tätigkeit durchgeführt wurde,
- wer eine Tätigkeit durchgeführt hat und
- wann eine Tätigkeit durchgeführt wurde.

Die Institution MUSS jederzeit nachweisen können, welche Person welche administrativen Tätigkeiten durchgeführt hat. Dazu SOLLTEN alle Administrierenden über eine eigene Zugangskennung verfügen. Auch Vertretungen von Administrierenden SOLLTEN eigene Zugangskennungen erhalten. Jeder Anmeldevorgang (Login) über eine Administrationskennung MUSS protokolliert werden.

OPS.1.1.2.A6 Schutz administrativer Tätigkeiten (B)

Administrative Schnittstellen und Funktionen DÜRFEN NUR berechtigten Personen zur Verfügung stehen. Für diese Schnittstellen und Funktionen MÜSSEN geeignete Verfahren zur Authentisierung

festgelegt werden. Es MUSS sichergestellt sein, dass IT-Administrationstätigkeiten nur durchgeführt werden können, falls vorher eine dementsprechende Authentisierung erfolgt ist.

Es MUSS festgelegt werden, welche Protokolle für Administrationsschnittstellen verwendet werden dürfen, so dass die bei der Administration stattfindende Kommunikation abgesichert ist.

OPS.1.1.2.A21 Regelung der IT-Administrationsrollen (B)

Es MÜSSEN Rollen definiert werden, die ausschließlich zur IT-Administration vergeben werden. Administrationsrollen MÜSSEN aufgrund des tatsächlichen Bedarfs im Aufgabenbereich der IT-Administration nachvollziehbar vergeben werden. Alle notwendigen IT-Administrationstätigkeiten MÜSSEN durch Berechtigungen in den Administrationsrollen nach dem Minimalprinzip abgedeckt sein.

Die IT-Administration unterschiedlicher Ebenen der IT-Komponenten, z. B. die Trennung von Betriebssystem- und Anwendungsadministration, MUSS bei der Konzeption der Administrationsrollen berücksichtigt werden.

OPS.1.1.2.A22 Trennung von administrativen und anderen Tätigkeiten (B)

Die durchführende Person MUSS wissen, bei welchem Teil ihrer Aufgabe es sich um administrative Tätigkeiten handelt. Aufgaben, die keine Administrationsrechte benötigen, DÜRFEN NICHT mit Administrationsrechten ausgeführt werden.

Es MUSS sichergestellt werden, dass Administrationswerkzeuge klar als solche erkennbar sind. Wenn eine Anwendung zur Erfüllung einer Administrationsaufgabe benutzt wird, DARF NICHT dieselbe Instanz dieser Anwendung für andere Aufgaben verwendet werden. Dies SOLLTE auf technischer Ebene sichergestellt werden. Die Zugangskennungen, die zur IT-Administration genutzt werden, SOLLTEN sich von Zugangskennungen unterscheiden, die in anderem Kontext genutzt werden.

3.2. Standard-Anforderungen

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

OPS.1.1.2.A7 Regelung der IT-Administrationstätigkeit (S)

Jede IT-Administrationstätigkeit SOLLTE einer klar definierten Aufgabe zugeordnet sein. Für diese Aufgaben SOLLTE geregelt werden,

- durch wen diese Aufgabe ausgeführt werden darf und
- durch wen diese Aufgabe beauftragt werden darf.

Es SOLLTE nachvollziehbar sein, in welchen Prozessen sich Administrationsaufgaben einfügen. IT-Administrationstätigkeiten SOLLTEN nur mit denjenigen Berechtigungen durchgeführt werden, die zur Erfüllung der entsprechenden Aufgabe notwendig sind. Es SOLLTE festgelegt werden, wie IT-Administrationstätigkeiten auszuführen sind.

Die Regelungen für IT-Administrationstätigkeiten SOLLTEN regelmäßig und anlassbezogen überprüft und aktualisiert werden.

Für jede IT-Administrationstätigkeit SOLLTE sichergestellt werden, dass diese bei Bedarf auch im Notfall ausgeführt werden kann.

OPS.1.1.2.A8 Administration von Fachanwendungen (S)

Es SOLLTE geregelt und dokumentiert werden, welche Administrationsaufgaben für Fachanwendungen vom IT-Betrieb und welche durch die Fachadministration durchgeführt werden.

Für Fachanwendungen SOLLTE identifiziert werden, welche Zugriffe der IT-Betrieb auf Systemebene benötigt.

Alle Schnittstellen und Abhängigkeiten zwischen der Fachadministration und der Administration durch den IT-Betrieb SOLLTEN identifiziert werden. Immer wenn Administrationsprozesse erstellt und gepflegt werden, SOLLTEN die Zuständigkeiten und Abhängigkeiten dieser Schnittstellen berücksichtigt werden.

OPS.1.1.2.A9 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.1.2.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.1.2.A11 Dokumentation von IT-Administrationstätigkeiten (S)

Durchgeführte IT-Administrationstätigkeiten SOLLTEN nachvollziehbar dokumentiert werden. Es SOLLTE geprüft werden, welche grundsätzlichen Anforderungen an die Dokumentation der IT-Administrationstätigkeiten existieren. Es SOLLTE identifiziert werden, welche Ziele mit der Dokumentation erreicht werden sollen. Aufgrund dieser Anforderungen und Ziele SOLLTE verbindlich festgelegt werden, welche Schritte in welchem Detailierungsgrad dokumentiert werden. Aus der Dokumentation SOLLTE mindestens hervorgehen,

- welche Änderungen erfolgten,
- wann die Änderungen erfolgten,
- wer die Änderungen durchgeführt hat,
- auf welcher Grundlage bzw. aus welchem Anlass die Änderungen erfolgt sind und
- inwiefern und aus welchem Grund gegebenenfalls von vorgegebenen Standards oder Konfigurationen abgewichen wurde.

Dokumentation im Kontext einer IT-Administrationstätigkeit SOLLTE in Standard-Arbeitsabläufen enthalten sein. Es SOLLTE geregelt werden, welche Möglichkeiten zu nutzen sind, falls IT-Administrationstätigkeiten außerplanmäßig durchgeführt werden.

Es SOLLTE identifiziert werden, unter welchen Umständen ein Zugriff auf die Dokumentation notwendig ist. Der Zugriff SOLLTE dementsprechend gewährleistet sein.

OPS.1.1.2.A12 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.1.2.A13 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.1.2.A16 Erweiterte Sicherheitsmaßnahmen für Administrationszugänge (S)

Der Zugang zu administrativen Oberflächen und Schnittstellen SOLLTE auf IT-Systeme, die zur IT-Administration verwendet werden, beschränkt sein. Daher SOLLTEN Netze, die zur IT-Administration verwendet werden, durch Filter- und Segmentierungsmaßnahmen von produktiven Netzen zu administrierender Komponenten getrennt werden (Out-of-Band-Management). Wo kein Out-of-Band-Management möglich ist, SOLLTEN Software-Schnittstellen und physische Schnittstellen zur IT-Administration durch zusätzliche Maßnahmen abgesichert werden und nur für Personen erreichbar sein, die für deren Nutzung berechtigt sind. Hierzu SOLLTE eine Zwei-Faktor-Authentisierung verwendet werden.

OPS.1.1.2.A20 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.1.2.A23 Rollen- und Berechtigungskonzept für administrative Zugriffe (S)

Es SOLLTE ein angemessenes Rollen- und Berechtigungskonzept für administrative Zugriffe existieren. Darin SOLLTEN grundsätzliche Vorgaben gemacht werden, mindestens darüber,

- wie Administrationsrollen beantragt und zugewiesen werden,
- welche Arten von Administrationsrollen existieren,
- welche Arten von Berechtigungen im Kontext der Administrationsrollen vergeben werden,
- wie für die IT-Administration notwendige Berechtigungen vergeben werden.

OPS.1.1.2.A24 Prüfen von IT-Administrationstätigkeiten (S)

Bevor eine IT-Administrationstätigkeit durchgeführt wird, SOLLTE geprüft werden, ob der Anlass und die Art der Tätigkeit im Kontext der zugrundeliegenden Aufgabe plausibel sind. Nachdem eine IT-Administrationstätigkeit an einer Komponente durchgeführt wurde, SOLLTE geprüft werden, ob die Konfiguration und der Status der Komponente dem gewünschten Zielzustand entspricht.

Falls eine zusätzliche Qualitätssicherung der ausgeführten Administrationsaufgabe notwendig ist, SOLLTE diese nicht durch dieselbe Person durchgeführt werden, die die entsprechenden Tätigkeiten durchgeführt hat.

Für IT-Administrationstätigkeiten mit potenziell weitreichenden Folgen SOLLTE geprüft werden, ob diese Tätigkeiten die Verfügbarkeit der IT-Administration selbst einschränken könnten. In diesem Fall SOLLTEN entsprechende Vorkehrungen getroffen werden, um einen Rollback der IT-Administrationstätigkeiten zu ermöglichen.

OPS.1.1.2.A25 Zeitfenster für schwerwiegende IT-Administrationstätigkeiten (S)

Für IT-Administrationstätigkeiten mit potenziell weitreichenden Folgen SOLLTEN durch den IT-Betrieb Wartungsfenster abgestimmt werden. Falls der IT-Betrieb für IT-Administrationstätigkeiten Vorgaben zu Zeitfenstern macht, MÜSSEN diese eingehalten werden.

OPS.1.1.2.A26 Backup der Konfiguration (S)

Alle Konfigurationen SOLLTEN durch regelmäßige Backups auf Anwendungsebene und auf IT-Systemebene gesichert werden. Vor IT-Administrationstätigkeiten mit potenziell weitreichenden Folgen SOLLTE ein zusätzliches Backup gemacht werden. Für Backups SOLLTE gewährleistet sein, dass sie im Fehlerfall wieder eingespielt werden können.

OPS.1.1.2.A27 Ersatz für zentrale IT-Administrationswerkzeuge (S)

Für zentrale IT-Administrationswerkzeuge SOLLTEN Alternativen zur Verfügung stehen, mit denen im Bedarfsfall administriert werden kann. Hierzu SOLLTEN Sprungsysteme mit Zugriff auf entsprechende Administrationsnetze zur Verfügung stehen. Falls solche Alternativen nicht zur Verfügung stehen, SOLLTE zur IT-Administration der Zugang und der direkte Zugriff auf die zu administrierende IT möglich sein.

OPS.1.1.2.A28 Protokollierung administrativer Tätigkeiten (S)

Administrative Tätigkeiten SOLLTEN protokolliert werden. Die Protokolldateien SOLLTEN für eine angemessene Zeitdauer geschützt aufbewahrt werden. Die ausführenden Administrierenden SOLLTEN keine Möglichkeiten haben, die aufgezeichneten Protokolldateien zu verändern oder zu löschen. Protokolldaten SOLLTEN regelmäßig geprüft werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

OPS.1.1.2.A14 ENTFALLEN (H)

Diese Anforderung ist entfallen.

OPS.1.1.2.A15 ENTFALLEN (H)

Diese Anforderung ist entfallen.

OPS.1.1.2.A17 IT-Administration im Vier-Augen-Prinzip (H)

Es SOLLTE geregelt werden, welche Administrationsaufgaben eine zusätzliche Person erfordern, die die Ausführung überwacht. Diese Person SOLLTE im Kontext der durchzuführenden IT-Administrationstätigkeiten auch über die zur Ausführung notwendigen Qualifikationen verfügen.

OPS.1.1.2.A18 Durchgängige Protokollierung administrativer Tätigkeiten (H)

Bei IT-Komponenten mit hohem Schutzbedarf SOLLTEN alle administrativen Tätigkeiten in sämtlichen Bereichen protokolliert werden. Dabei SOLLTE jede administrative Aktion vollständig nachvollzogen werden. Die ausführenden Administrierenden SOLLTEN keinen Einfluss auf Art und Umfang der Protokollierung nehmen können.

OPS.1.1.2.A19 Nutzung hochverfügbarer IT-Administrationswerkzeuge (H)

Administrationswerkzeuge SOLLTEN redundant ausgelegt werden. Es SOLLTE sichergestellt werden, dass im Störungsfall weiterhin alle Administrationsaufgaben ohne wesentliche Einschränkungen ausgeführt werden können.

OPS.1.1.2.A29 Monitoring der IT-Administrationswerkzeuge (H)

Für IT-Administrationswerkzeuge SOLLTEN Kenngrößen zur Verfügbarkeit identifiziert werden. Diese Kenngrößen SOLLTEN kontinuierlich überwacht werden. Es SOLLTEN tolerierbare Grenzwerte dieser Kenngrößen festgelegt werden. Werden diese nicht eingehalten, SOLLTEN die zuständigen Teams automatisch benachrichtigt werden.

OPS.1.1.2.A30 Sicherheitsmonitoring administrativer Tätigkeiten (H)

Falls ein IT-System zur zentralen Detektion und automatisierten Echtzeitüberprüfung von Ereignismeldungen genutzt wird, SOLLTEN dort Ereignisdaten zu administrativen Tätigkeiten ausgewertet werden. Hierzu SOLLTEN bestehende Monitoring-Systeme der IT sowie kritische Administrationswerkzeuge in dieses IT-System eingebunden werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) stellt in Anhang A der Norm ISO/IEC 27001:2013 unter anderem im Kontext der Themen Zugangssteuerung (A.9) und IT-Betrieb (A.12) Anforderungen an die ordnungsgemäße IT-Administration.

Das BSI spezifiziert unter anderem für den Bereich der sicheren Administration Anforderungen im Dokument „Konkretisierung der Anforderungen an die gemäß § 8a Absatz 1 BSIG umzusetzenden Maßnahmen“.

Bundesamt
für Sicherheit in der
Informationstechnik

OPS.1.1.3 Patch- und Änderungsmanagement

1. Beschreibung

1.1. Einleitung

Es ist eine große Herausforderung, die in einer Institution eingesetzten Komponenten der Informationstechnik korrekt und zeitnah zu aktualisieren. So zeigt sich in der Praxis, dass vorhandene Sicherheitslücken oder Betriebsstörungen häufig auf mangelhafte oder fehlende Patches und Änderungen zurückzuführen sind. Ein fehlendes oder vernachlässigtes Patch- und Änderungsmanagement führt daher schnell zu möglichen Angriffspunkten.

Aufgabe des Patch- und Änderungsmanagements ist es allgemein, verändernde Eingriffe in Anwendungen, Infrastruktur, Dokumentationen, Prozesse und Verfahren steuer- und kontrollierbar zu gestalten.

1.2. Zielsetzung

In diesem Baustein wird aufgezeigt, wie ein funktionierendes Patchmanagement in einer Institution aufgebaut und wie der entsprechende Prozess kontrolliert und optimiert werden kann.

Über das Patchmanagement hinaus beinhaltet der Baustein jedoch auch einige Kernaspekte eines Änderungsmanagements, die für die Informationssicherheit relevant sind. Mit Änderungsmanagement wird die Aufgabe bezeichnet, Änderungen zu planen und zu steuern.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.1.1.3 *Patch- und Änderungsmanagement* ist für den gesamten Informationsverbund anzuwenden.

Die Beschreibungen in diesem Baustein konzentrieren sich auf den IT-Betrieb, und dort insbesondere auf das Patchmanagement, mit dem Software aktualisiert wird (z. B. durch Sicherheitskorrekturen, Service Packs und Hot Fixes). In den einzelnen Bausteinen der Schichten SYS *IT-Systeme* und APP *Anwendungen* finden sich gegebenenfalls spezifischere Anforderungen bezüglich des Patch- und Änderungsmanagements.

Dieser Baustein beinhaltet kein vollständiges Änderungsmanagement, sondern lediglich die Kernaspekte zur Informationssicherheit. In größeren Institutionen ist es sinnvoll, darüber hinaus ein

Änderungsmanagement systematisch zu strukturieren. Hierzu können Standardwerke, wie z. B. der Change-Management-Prozess der „IT Infrastructure Library“ (ITIL), herangezogen werden. Ein solches Änderungsmanagement muss nicht auf die IT beschränkt sein, sondern kann auch Geschäftsprozesse und Fachaufgaben selbst umfassen. Unter Änderung wird in diesem Baustein alles inbegriffen, was damit einhergeht, IT-Komponenten anzupassen, wie z. B. „Changes“, „Patches", „Updates“, „Upgrades“, „Einbau“, „Ausbau“, etc. Software Entwicklung hingegen wird im Baustein CON.8 *Software-Entwicklung* betrachtet.

Anforderungen zu Test und Freigabe von Patches und Software werden in diesem Baustein nicht im Detail behandelt. Sie finden sich im Baustein OPS.1.1.6 *Software-Tests und -Freigaben.*

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.1.1.3 *Patch- und Änderungsmanagement* von besonderer Bedeutung.

2.1. Mangelhaft festgelegte Zuständigkeiten

Durch mangelhaft festgelegte, sich überschneidende oder ungeklärte Zuständigkeiten können beispielsweise Änderungsanforderungen langsamer kategorisiert und priorisiert werden. Dadurch kann sich insgesamt die Verteilung von Patches und Änderungen verzögern. Auch wenn Patches und Änderungen vorschnell ohne Testlauf und Berücksichtigung aller (fachlichen) Aspekte freigegeben werden, kann sich das gravierend auf die Sicherheit auswirken.

Im Extremfall können mangelhaft festgelegte Zuständigkeiten die gesamte Institution komplett oder in großem Umfang beeinträchtigen. Störungen im Betrieb wirken sich negativ auf die Verfügbarkeit aus. Werden sicherheitsrelevante Patches nicht oder verspätet verteilt, können die Vertraulichkeit und Integrität gefährdet werden.

2.2. Mangelhafte Kommunikation beim Änderungsmanagement

Wenn das Patch- und Änderungsmanagement innerhalb der Institution wenig akzeptiert wird oder die beteiligten Personen mangelhaft kommunizieren, kann das dazu führen, dass Änderungsanforderungen verzögert bearbeitet werden oder über eine Änderungsanforderung falsch entschieden wird. Dadurch kann das Sicherheitsniveau insgesamt verringert und der IT-Betrieb ernsthaft gestört werden. In jedem Fall wird bei mangelhafter Kommunikation der Änderungsprozess ineffizient, da zu viel Zeit und Ressourcen investiert werden müssen. Dies wirkt sich negativ auf die Reaktionsfähigkeit der Institution aus und kann im Extremfall dazu führen, dass Sicherheitslücken entstehen oder wichtige Ziele der Institution nicht erreicht werden.

2.3. Mangelhafte Berücksichtigung von Geschäftsprozessen und Fachaufgaben

Ungeeignete Änderungen können unter anderem den reibungslosen Ablauf der Geschäftsprozesse oder Fachaufgaben beeinträchtigen oder gar dazu führen, dass die beteiligten IT-Systeme komplett ausfallen. Auch ein noch so umfangreiches Testverfahren kann nicht vollkommen ausschließen, dass sich eine Änderung im späteren Produktivbetrieb als fehlerhaft erweist.

Wird im Änderungsprozess die Auswirkung, Kategorie oder Priorität einer eingereichten Änderungsanforderung hinsichtlich der Geschäftsprozesse beziehungsweise Fachaufgaben falsch eingeschätzt, kann sich das angestrebte Sicherheitsniveau verringern. Solche Fehleinschätzungen treten überwiegend auf, wenn sich die für die IT zuständigen Personen und die zuständigen Fachabteilungen nicht ausreichend abstimmen.

2.4. Unzureichende Ressourcen beim Patch- und Änderungsmanagement

Für ein wirkungsvolles Patch- und Änderungsmanagement sind angemessene personelle, zeitliche und finanzielle Ressourcen erforderlich. Sind diese nicht vorhanden, könnten beispielsweise die notwendigen Rollen mit ungeeigneten Personen besetzt werden. Auch können so keine Schnittstellen für bestimmte Informationen geschaffen werden, beispielsweise zwischen der IT und den entsprechenden Ansprechpartnern und Ansprechpartnerinnen in den Fachbereichen. Auch die erforderlichen Kapazitäten für die Infrastruktur der Test- und Verteilungsumgebungen könnten nicht bereitgestellt werden. Können die personellen, zeitlichen und finanziellen Mängel im Regelbetrieb häufig noch ausgeglichen werden, zeigen sie sich unter hohem Zeitdruck umso deutlicher, beispielsweise wenn Notfallpatches eingespielt werden müssen.

2.5. Probleme bei der automatisierten Verteilung von Patches und Änderungen

Häufig werden Patches und Änderungen nicht manuell, sondern zentral softwareunterstützt verteilt. Wird eine solche Software benutzt, können fehlerhafte Patches und Änderungen automatisiert im gesamten Informationsverbund verteilt werden, wodurch große Sicherheitsprobleme entstehen können. Besonders gravierend ist es, wenn auf vielen IT-Systemen gleichzeitig Software installiert wird, die Sicherheitslücken enthält.

Treten nur vereinzelte Fehler auf, lassen sie sich oft per Hand beheben. Problematisch wird es aber, wenn IT-Systeme über einen längeren Zeitraum nicht erreichbar sind. Ein Beispiel sind Mitarbeitende im Außendienst, die ihre IT-Systeme nur selten und unregelmäßig an das LAN der Institution anschließen. Wenn das Werkzeug so konfiguriert wird, dass die Aktualisierungen nur innerhalb eines bestimmten Zeitraums verteilt werden, und dann nicht alle IT-Systeme erreichbar sind, können diese IT-Systeme nicht aktualisiert werden.

2.6. Mangelhafte Wiederherstellungsoptionen beim Patch- und Änderungsmanagement

Wenn Patches oder Änderungen verteilt werden, ohne dass eine Wiederherstellungsoption vorgesehen ist, oder wenn die Wiederherstellungsroutinen der eingesetzten Software nicht oder nicht angemessen wirken, kann fehlerhaft aktualisierte Software nicht zeitnah korrigiert werden. Dadurch können wichtige IT-Systeme ausfallen und hohe Folgeschäden entstehen. Neben dem Verlust der Daten sind vor allem die Verfügbarkeit und Integrität der Daten und der betroffenen IT-Systeme gefährdet.

2.7. Fehleinschätzung der Relevanz von Patches und Änderungen

Werden Änderungen falsch priorisiert, könnten beispielsweise zuerst unwichtige Patches installiert werden. Wichtige Patches hingegen werden dann zu spät installiert. Sicherheitslücken bleiben so länger bestehen. Das Patch- und Änderungsmanagement wird oft durch softwarebasierte Werkzeuge unterstützt. Auch diese Werkzeuge können Softwarefehler enthalten und dadurch unzureichende oder fehlerhafte Angaben über eine Änderung machen. Werden die Angaben, die ein solches Tool über eine Änderung macht, nicht überprüft und auf Plausibilität getestet, kann die tatsächliche von der angenommenen Umsetzung von Änderungen abweichen.

2.8. Manipulation von Daten und Werkzeugen beim Änderungsmanagement

Das Patch- und Änderungsmanagement agiert oft von zentraler Stelle aus. Aufgrund seiner exponierten Stellung ist es besonders gefährdet. Wenn es bei einem Angriff gelingen sollte, die beteiligten Server zu übernehmen, könnten über diesen zentralen Punkt manipulierte Softwareversionen gleichzeitig auf eine Vielzahl von IT-Systemen verteilt werden. Oft entstehen weitere Angriffspunkte dadurch, dass diese IT-Systeme von externen Partnerinstitutionen betrieben werden (Outsourcing). Es könnte auch Wartungszugänge geben, die ermöglichen, auf den zentralen Server zur Verteilung von Änderungen zuzugreifen. Auch diese könnten für Angriffe genutzt werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.1.1.3 *Patch- und Änderungsmanagement* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Fachverantwortliche

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

OPS.1.1.3.A1 Konzept für das Patch- und Änderungsmanagement (B) [Fachverantwortliche]

Wenn IT-Komponenten, Software oder Konfigurationsdaten geändert werden, MUSS es dafür Vorgaben geben, die auch Sicherheitsaspekte berücksichtigen. Diese MÜSSEN in einem Konzept für das Patch- und Änderungsmanagement festgehalten und befolgt werden. Alle Patches und Änderungen MÜSSEN geeignet geplant, genehmigt und dokumentiert werden. Patches und Änderungen SOLLTEN vorab geeignet getestet werden (siehe hierzu auch OPS.1.1.6 *Software-Tests und Freigaben*). Wenn Patches installiert und Änderungen durchgeführt werden, MÜSSEN Rückfall-Lösungen vorhanden sein. Bei größeren Änderungen MUSS zudem der oder die ISB beteiligt sein. Insgesamt MUSS sichergestellt werden, dass das angestrebte Sicherheitsniveau während und nach den Änderungen erhalten bleibt. Insbesondere SOLLTEN auch die gewünschten Sicherheitseinstellungen erhalten bleiben.

OPS.1.1.3.A2 Festlegung der Zuständigkeiten (B)

Für alle Organisationsbereiche MÜSSEN Zuständige für das Patch- und Änderungsmanagement festgelegt werden. Die definierten Zuständigkeiten MÜSSEN sich auch im Berechtigungskonzept widerspiegeln.

OPS.1.1.3.A3 Konfiguration von Autoupdate-Mechanismen (B)

Innerhalb der Strategie zum Patch- und Änderungsmanagement MUSS definiert werden, wie mit integrierten Update-Mechanismen (Autoupdate) der eingesetzten Software umzugehen ist. Insbesondere MUSS festgelegt werden, wie diese Mechanismen abgesichert und passend konfiguriert werden. Außerdem SOLLTEN neue Komponenten daraufhin überprüft werden, welche Update-Mechanismen sie haben.

OPS.1.1.3.A15 Regelmäßige Aktualisierung von IT-Systemen und Software (B)

IT-Systeme und Software SOLLTEN regelmäßig aktualisiert werden.

Grundsätzlich SOLLTEN Patches zeitnah nach Veröffentlichung eingespielt werden. Basierend auf dem Konzept für das Patch- und Änderungsmanagement MÜSSEN Patches zeitnah nach Veröffentlichung bewertet und entsprechend priorisiert werden. Für die Bewertung SOLLTE geprüft werden, ob es zu diesem Patch bekannte Schwachstellen gibt. Es MUSS entschieden werden, ob der Patch eingespielt werden soll. Wenn ein Patch eingespielt wird, SOLLTE kontrolliert werden, ob dieser auf allen relevanten Systemen zeitnah erfolgreich eingespielt wurde. Wenn ein Patch nicht eingespielt wird, MÜSSEN die Entscheidung und die Gründe dafür dokumentiert werden.

Falls Hardware- oder Software-Produkte eingesetzt werden sollen, die nicht mehr von den Herstellenden unterstützt werden oder für die kein Support mehr vorhanden ist, MUSS geprüft werden, ob diese dennoch sicher betrieben werden können. Ist dies nicht der Fall, DÜRFEN diese Hardware- oder Software-Produkte NICHT mehr verwendet werden.

OPS.1.1.3.A16 ENTFALLEN (B)

Diese Anforderung ist entfallen.

3.2. Standard-Anforderungen

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

OPS.1.1.3.A4 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.1.3.A5 Umgang mit Änderungsanforderungen (S) [Fachverantwortliche]

Alle Änderungsanforderungen (Request for Changes, RfCs) SOLLTEN erfasst und dokumentiert werden. Die Änderungsanforderungen SOLLTEN von den jeweiligen Fachverantwortlichen für das Patch- und Änderungsmanagement daraufhin kontrolliert werden, ob die Aspekte der Informationssicherheit ausreichend berücksichtigt wurden.

OPS.1.1.3.A6 Abstimmung von Änderungsanforderungen (S)

Der zu einer Änderung zugehörige Abstimmungsprozess SOLLTE alle relevanten Zielgruppen und die Auswirkungen auf die Informationssicherheit berücksichtigen. Die von der Änderung betroffenen Zielgruppen SOLLTEN sich nachweisbar dazu äußern können. Auch SOLLTE es ein festgelegtes Verfahren geben, wodurch wichtige Änderungsanforderungen beschleunigt werden können.

OPS.1.1.3.A7 Integration des Änderungsmanagements in die Geschäftsprozesse (S)

Der Änderungsmanagementprozess SOLLTE in die Geschäftsprozesse beziehungsweise Fachaufgaben integriert werden. Bei geplanten Änderungen SOLLTE die aktuelle Situation der davon betroffenen Geschäftsprozesse berücksichtigt werden. Alle relevanten Fachabteilungen SOLLTEN über anstehende Änderungen informiert werden. Auch SOLLTE es eine Eskalationsebene geben, deren Mitglieder der

Leitungsebene der Institution angehören. Die Mitglieder dieser Eskalationsebene SOLLTEN in Zweifelsfällen über Priorität und Terminplanung einer Hard- oder Software-Änderung entscheiden.

OPS.1.1.3.A8 Sicherer Einsatz von Werkzeugen für das Patch- und Änderungsmanagement (S)

Anforderungen und Rahmenbedingungen SOLLTEN definiert werden, nach denen Werkzeuge für das Patch- und Änderungsmanagement ausgewählt werden. Außerdem SOLLTE eine spezifische Sicherheitsrichtlinie für die eingesetzten Werkzeuge erstellt werden.

OPS.1.1.3.A9 Test- und Abnahmeverfahren für neue Hardware (S)

Wenn neue Hardware ausgewählt wird, SOLLTE geprüft werden, ob die eingesetzte Software und insbesondere die relevanten Betriebssysteme mit der Hardware und deren Treibersoftware kompatibel sind. Neue Hardware SOLLTE getestet werden, bevor sie eingesetzt wird. Diese SOLLTE ausschließlich in einer isolierten Umgebung getestet werden.

Für IT-Systeme SOLLTE es ein Abnahmeverfahren und eine Freigabeerklärung geben. Die Zuständigen SOLLTEN die Freigabeerklärungen an geeigneter Stelle schriftlich hinterlegen. Für den Fall, dass trotz der Abnahme- und Freigabeverfahren im laufenden Betrieb Fehler festgestellt werden, SOLLTE es ein Verfahren zur Fehlerbehebung geben.

OPS.1.1.3.A10 Sicherstellung der Integrität und Authentizität von Softwarepaketen (S)

Während des gesamten Patch- oder Änderungsprozesses SOLLTE die Authentizität und Integrität von Softwarepaketen sichergestellt werden. Dazu SOLLTE geprüft werden, ob für die eingesetzten Softwarepakete Prüfsummen oder digitale Signaturen verfügbar sind. Falls ja, SOLLTEN diese vor der Installation des Pakets überprüft werden. Ebenso SOLLTE darauf geachtet werden, dass die notwendigen Programme zur Überprüfung vorhanden sind.

Software und Updates SOLLTEN grundsätzlich nur aus vertrauenswürdigen Quellen bezogen werden.

OPS.1.1.3.A11 Kontinuierliche Dokumentation der Informationsverarbeitung (S)

Änderungen SOLLTEN in allen Phasen, allen Anwendungen und allen Systemen dokumentiert werden. Dazu SOLLTEN entsprechende Regelungen erarbeitet werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

OPS.1.1.3.A12 Einsatz von Werkzeugen beim Änderungsmanagement (H)

Bevor ein Werkzeug zum Änderungsmanagement benutzt wird, SOLLTE sorgfältig geprüft werden, ob damit die Änderungen angemessen im Informationsverbund verteilt werden können. Zusätzlich SOLLTEN Unterbrechungspunkte definiert werden können, an denen die Verteilung einer fehlerhaften Änderung gestoppt wird.

OPS.1.1.3.A13 Erfolgsmessung von Änderungsanforderungen (H) [Fachverantwortliche]

Um zu überprüfen, ob eine Änderung erfolgreich war, SOLLTEN die jeweiligen Fachverantwortlichen für das Patch- und Änderungsmanagement sogenannte Nachtests durchführen. Dazu SOLLTEN sie

geeignete Referenzsysteme als Qualitätssicherungssysteme auswählen. Die Ergebnisse der Nachtests SOLLTEN im Rahmen des Änderungsprozesses dokumentiert werden.

OPS.1.1.3.A14 Synchronisierung innerhalb des Änderungsmanagements (H)

Im Änderungsmanagementprozess SOLLTE durch geeignete Mechanismen sichergestellt werden, dass auch zeitweise oder längerfristig nicht erreichbare Geräte die Patches und Änderungen erhalten.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 im Kapitel 12.1.2 Change Management Vorgaben, die für das Patch- und Änderungsmanagement relevant sind.

Die IT Infrastructure Library (ITIL) gibt Hinweise zum Aufbau eines Change-Management-Prozesses.

Bundesamt
für Sicherheit in der
Informationstechnik

OPS.1.1.4 Schutz vor Schadprogrammen

1. Beschreibung

1.1. Einleitung

Schadprogramme sind Programme, die in der Regel ohne Wissen und Einwilligung der Benutzenden schädliche Funktionen auf einem IT-System ausführen. Diese Schadfunktionen können ein breites Feld abdecken, das von Spionage über Erpressung (sogenannte Ransomware) bis hin zur Sabotage und Zerstörung von Informationen oder gar Geräten reicht.

Schadprogramme können grundsätzlich auf allen Betriebssystemen und IT-Systemen ausgeführt werden. Dazu gehören neben klassischen IT-Systemen wie Clients und Servern auch mobile Geräte wie Smartphones. Netzkomponenten wie Router, Industriesteuerungsanlagen und sogar IoT-Geräte wie vernetzte Kameras sind heutzutage ebenfalls vielfach durch Schadprogramme gefährdet.

Schadprogramme verbreiten sich auf klassischen IT-Systemen zumeist über E-Mail-Anhänge, manipulierte Webseiten (Drive-by-Downloads) oder Datenträger. Smartphones werden in der Regel über die Installation von schädlichen Apps infiziert, auch Drive-by-Downloads sind möglich. Darüber hinaus sind offene Netzschnittstellen, fehlerhafte Konfigurationen und Softwareschwachstellen häufige Einfallstore auf allen IT-Systemen.

In diesem Baustein wird der Begriff „Virenschutzprogramm“ verwendet. „Viren“ stehen dabei als Synonym für alle Arten von Schadprogrammen. Gemeint ist mit „Virenschutzprogramm“ demnach ein Programm zum Schutz vor jeglicher Art von Schadprogrammen.

1.2. Zielsetzung

Dieser Baustein beschreibt Anforderungen, die zu erfüllen und umzusetzen sind, um eine Institution effektiv gegen Schadprogramme zu schützen.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.1.1.4 *Schutz vor Schadprogrammen* ist einmal auf den Informationsverbund anzuwenden.

In diesem Baustein werden die allgemeinen Anforderungen für den Schutz gegen Schadprogramme beschrieben. Spezifische Anforderungen, um bestimmte IT-Systeme der Institution vor

Schadprogrammen zu schützen, finden sich bei Bedarf in den jeweiligen Bausteinen der Schicht SYS *IT-Systeme*. Führt ein identifiziertes Schadprogramm zu einem Sicherheitsvorfall, sollten die Anforderungen des Bausteins DER.2.1 *Behandlung von Sicherheitsvorfällen* berücksichtigt werden. Die Anforderungen des Bausteins DER.2.3 *Bereinigung weitreichender Sicherheitsvorfälle* helfen dabei, identifizierte Schadprogramme zu entfernen und einen bereinigten Zustand wiederherzustellen.

Die im Rahmen dieses Bausteins eingesetzten Virenschutzprogramme sollten grundsätzlich auch im Patch- und Änderungsmanagement (OPS.1.1.3 *Patch- und Änderungsmanagement*) berücksichtigt werden. Weiterhin sollte das Thema Schutz vor Schadprogrammen im Rahmen des Bausteins ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit* und CON.3 *Datensicherungskonzept* mit berücksichtigt werden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.1.1.4 *Schutz vor Schadprogrammen* von besonderer Bedeutung.

2.1. Softwareschwachstellen und Drive-by-Downloads

Sind IT-Systeme nicht ausreichend vor Schadprogrammen geschützt, können Softwareschwachstellen bei Angriffen ausgenutzt werden, um Schadcode auszuführen. Dies kann unter anderem passieren, wenn Patches nicht zeitnah eingespielt und Schutzmechanismen von Anwendungsprogrammen, wie Browsern, nicht richtig konfiguriert sind. Bei den sogenannten Drive-by-Downloads reicht es beispielsweise aus, eine mit Schadcode behaftete Website zu besuchen. Eine Schwachstelle im Browser oder in einem installierten Plug-in, wie Java oder Adobe Flash, kann dann ausgenutzt werden, um das IT-System zu infizieren und Angreifenden umfangreiche Kontrolle sowie einen Zugang zum Netz einer Institution zu verschaffen. Besonders gefährdet sind hier IT-Systeme, die nicht regelmäßig aktualisiert werden, z. B. viele Smartphones.

2.2. Erpressung durch Ransomware

Eine weitverbreitete Art von Schadprogrammen ist die sogenannte Ransomware. Diese verschlüsselt die Daten des infizierten IT-Systems sowie häufig auch weitere Daten, die etwa über Netzfreigaben erreichbar sind. In der Regel verwenden die Angreifenden dabei Verschlüsselungsmethoden, die ohne Kenntnis des Schlüssels nicht umkehrbar sind, und erpressen damit ihre Opfer um hohe Geldsummen. Besteht kein wirksamer Schutz gegen Schadprogramme und sind keine ergänzenden Vorkehrungen, wie Datensicherungen, getroffen, kann die Verfügbarkeit von Informationen erheblich eingeschränkt werden, Daten können verloren gehen, sowie massive finanzielle und Image-Schäden können eintreten.

2.3. Gezielte Angriffe und Social Engineering

Institutionen werden häufig mit maßgeschneiderten Schadprogrammen angegriffen. Dabei werden z. B. Führungskräfte über Methoden des Social Engineerings dazu verleitet, schädliche E-Mail-Anhänge zu öffnen. Maßgeschneiderte Schadprogramme können zudem häufig nicht unmittelbar von Virenschutzprogrammen erkannt werden. Auch die Personalabteilung einer Institution kann beispielsweise ein Angriffsziel sein, indem etwa mit Schadsoftware infizierte Bewerbungsunterlagen auf elektronischem Wege zugesendet werden. Konnten die Angreifenden auf diese Weise ein IT-System infizieren, so können sie sich innerhalb der Institution ausbreiten und beispielsweise Informationen einsehen, manipulieren oder zerstören.

2.4. Botnetze

Über Schadprogramme können IT-Systeme einer Institution Teil von sogenannten Botnetzen werden. Angreifende, die in einem solchen Botnetz häufig tausende von Systemen kontrollieren, können diese beispielsweise einsetzen, um Spam zu versenden oder verteilte Denial-of-Service (DDoS)-Angriffe auf Dritte zu starten. Auch wenn die eigene Institution möglicherweise nicht unmittelbar geschädigt wird, kann sich dies trotzdem negativ bezüglich der Verfügbarkeit und Integrität der eigenen Dienste und IT-Systeme auswirken und sogar rechtliche Probleme nach sich ziehen. Wenn z. B. der E-Mail-Server einer Institution auf eine Blockliste gelangt, ist möglicherweise kein Versand und Empfang von E-Mails mehr möglich.

2.5. Infektion von Produktionssystemen und IoT-Geräten

Neben klassischen IT-Systemen werden vermehrt auch Geräte durch Schadprogramme angegriffen, die auf den ersten Blick nicht wie offensichtliche Ziele aussehen. Bei einem Angriff könnte beispielsweise eine über das Internet erreichbare Überwachungskamera infiziert werden, um in der Institution zu spionieren. Aber auch eine vernetzte Glühbirne oder eine Kaffeemaschine mit App-Steuerung kann als Eintrittspunkt in das Netz der Institution oder als Teil eines Botnetzes dienen, wenn diese Geräte nicht ausreichend vor Schadprogrammen geschützt werden. Vernetzte Produktionssysteme oder Industriesteuerungen können ebenfalls durch Schadprogramme manipuliert oder sogar zerstört werden, was Ausfälle und viele weitere Gefährdungen für die Institution und ihre Mitarbeitenden, z. B. durch Brände, nach sich ziehen kann.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.*1.1.4 Schutz vor Schadprogrammen* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

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

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

OPS.1.1.4.A1 Erstellung eines Konzepts für den Schutz vor Schadprogrammen (B)

Es MUSS ein Konzept erstellt werden, das beschreibt, welche IT-Systeme vor Schadprogrammen geschützt werden müssen. Hierbei MÜSSEN auch IoT-Geräte und Produktionssysteme berücksichtigt werden. Außerdem MUSS festgehalten werden, wie der Schutz zu erfolgen hat. Ist kein verlässlicher Schutz möglich, so SOLLTEN die identifizierten IT-Systeme NICHT betrieben werden. Das Konzept SOLLTE nachvollziehbar dokumentiert und aktuell gehalten werden.

OPS.1.1.4.A2 Nutzung systemspezifischer Schutzmechanismen (B)

Es MUSS geprüft werden, welche Schutzmechanismen die verwendeten IT-Systeme sowie die darauf genutzten Betriebssysteme und Anwendungen bieten. Diese Mechanismen MÜSSEN genutzt werden, sofern es keinen mindestens gleichwertigen Ersatz gibt oder gute Gründe dagegen sprechen. Werden sie nicht genutzt, MUSS dies begründet und dokumentiert werden.

OPS.1.1.4.A3 Auswahl eines Virenschutzprogrammes (B)

Abhängig vom verwendeten Betriebssystem, anderen vorhandenen Schutzmechanismen sowie der Verfügbarkeit geeigneter Virenschutzprogramme MUSS für den konkreten Einsatzzweck ein entsprechendes Schutzprogramm ausgewählt und installiert werden. Für Gateways und IT-Systeme, die dem Datenaustausch dienen, MUSS ein geeignetes Virenschutzprogramm ausgewählt und installiert werden.

Es DÜRFEN NUR Produkte für den Enterprise-Bereich mit auf die Institution zugeschnittenen Service- und Supportleistungen eingesetzt werden. Produkte für die reine Heimanwendung oder Produkte ohne Support DÜRFEN NICHT im professionellen Wirkbetrieb eingesetzt werden.

Cloud-Dienste zur Verbesserung der Detektionsleistung der Virenschutzprogramme SOLLTEN genutzt werden. Falls Cloud-Funktionen solcher Produkte verwendet werden, MUSS sichergestellt werden, dass dies nicht im Widerspruch zum Daten- oder Geheimschutz steht. Neben Echtzeit- und On-Demand-Scans MUSS eine eingesetzte Lösung die Möglichkeit bieten, auch komprimierte Daten nach Schadprogrammen zu durchsuchen.

OPS.1.1.4.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

OPS.1.1.4.A5 Betrieb und Konfiguration von Virenschutzprogrammen (B)

Das Virenschutzprogramm MUSS für seine Einsatzumgebung geeignet konfiguriert werden. Die Erkennungsleistung SOLLTE dabei im Vordergrund stehen, sofern nicht Datenschutz- oder Leistungsgründe im jeweiligen Einzelfall dagegen sprechen. Wenn sicherheitsrelevante Funktionen des Virenschutzprogramms nicht genutzt werden, SOLLTE dies begründet und dokumentiert werden. Bei Schutzprogrammen, die speziell für die Desktop-Virtualisierung optimiert sind, SOLLTE nachvollziehbar dokumentiert sein, ob auf bestimmte Detektionsverfahren zugunsten der Leistung verzichtet wird. Es MUSS sichergestellt werden, dass die Benutzenden keine sicherheitsrelevanten Änderungen an den Einstellungen der Antivirenprogramme vornehmen können.

OPS.1.1.4.A6 Regelmäßige Aktualisierung der eingesetzten Virenschutzprogramme (B)

Auf den damit ausgestatteten IT-Systemen MÜSSEN die Virenschutzprogramme nach Empfehlung der herstellenden Institution regelmäßig und zeitnah aktualisiert werden.

OPS.1.1.4.A7 Sensibilisierung und Verpflichtung der Benutzenden (B) [Benutzende]

Benutzende MÜSSEN regelmäßig über die Bedrohung durch Schadprogramme aufgeklärt werden. Sie MÜSSEN die grundlegenden Verhaltensregeln einhalten, um die Gefahr eines Befalls durch Schadprogramme zu reduzieren. Dateien, E-Mails, Webseiten usw. aus nicht vertrauenswürdigen Quellen SOLLTEN NICHT geöffnet werden. Sie MÜSSEN entsprechenden Kontaktpersonen für den Fall eines Verdacht auf eine Infektion mit einem Schadprogramm bekannt sein. Sie MÜSSEN sich an die ihnen benannten Kontaktpersonen wenden, wenn der Verdacht auf eine Infektion mit einem Schadprogramm besteht.

3.2. Standard-Anforderungen

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

OPS.1.1.4.A8 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.1.4.A9 Meldung von Infektionen mit Schadprogrammen (S) [Benutzende]

Das eingesetzte Virenschutzprogramm SOLLTE eine Infektion mit einem Schadprogramm automatisch blockieren und melden. Die automatische Meldung SOLLTE an einer zentralen Stelle angenommen werden. Dabei SOLLTEN die zuständigen Mitarbeitenden je nach Sachlage über das weitere Vorgehen entscheiden. Das Vorgehen bei Meldungen und Alarmen der Virenschutzprogramme SOLLTE geplant, dokumentiert und getestet werden. Es SOLLTE insbesondere geregelt sein, was im Falle einer bestätigten Infektion geschehen soll.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

OPS.1.1.4.A10 Nutzung spezieller Analyseumgebungen (H)

Automatisierte Analysen in einer speziellen Testumgebung (basierend auf Sandboxen bzw. separaten virtuellen oder physischen Systemen) SOLLTEN für eine Bewertung von verdächtigen Dateien ergänzend herangezogen werden.

OPS.1.1.4.A11 Einsatz mehrerer Scan-Engines (H)

Zur Verbesserung der Erkennungsleistung SOLLTEN für besonders schutzwürdige IT-Systeme, wie Gateways und IT-Systeme zum Datenaustausch, Virenschutzprogramme mit mehreren alternativen Scan-Engines eingesetzt werden.

OPS.1.1.4.A12 Einsatz von Datenträgerschleusen (H)

Bevor insbesondere Datenträger von Dritten mit den IT-Systemen der Institution verbunden werden, SOLLTEN diese durch eine Datenträgerschleuse geprüft werden.

OPS.1.1.4.A13 Umgang mit nicht vertrauenswürdigen Dateien (H)

Ist es notwendig, nicht vertrauenswürdige Dateien zu öffnen, SOLLTE dies nur auf einem isolierten IT-System geschehen. Die betroffenen Dateien SOLLTEN dort z. B. in ein ungefährliches Format umgewandelt oder ausgedruckt werden, wenn sich hierdurch das Risiko einer Infektion durch Schadsoftware verringert.

OPS.1.1.4.A14 Auswahl und Einsatz von Cyber-Sicherheitsprodukten gegen gezielte Angriffe (H)

Der Einsatz sowie der Mehrwert von Produkten und Services, die im Vergleich zu herkömmlichen Virenschutzprogrammen einen erweiterten Schutzumfang bieten, SOLLTE geprüft werden. Solche Sicherheitsprodukte gegen gezielte Angriffe SOLLTEN z. B. bei der Ausführung von Dateien in speziellen Analyseumgebungen, bei der Härtung von Clients oder bei der Kapselung von Prozessen eingesetzt werden. Vor einer Kaufentscheidung für ein Sicherheitsprodukt SOLLTEN Schutzwirkung und Kompatibilität zur eigenen IT-Umgebung getestet werden.

OPS.1.1.4.A15 ENTFALLEN (H)

Diese Anforderung ist entfallen.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013, insbesondere in Annex A, A.12.2 „protection from malware“, Vorgaben für den Schutz vor Schadprogrammen.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“, insbesondere Area TS1 Security Solutions, Vorgaben für den Schutz vor Schadprogrammen.

Bundesamt
für Sicherheit in der
Informationstechnik

OPS.1.1.5 Protokollierung

1. Beschreibung

1.1. Einleitung

Damit ein verlässlicher IT-Betrieb gewährleistet ist, sollten IT-Systeme und Anwendungen entweder alle oder zumindest ausgewählte betriebs- und sicherheitsrelevante Ereignisse protokollieren, d. h. sie automatisch speichern und für die Auswertung bereitstellen. Eine Protokollierung wird in vielen Institutionen eingesetzt, um Hard- und Softwareprobleme sowie Ressourcenengpässe rechtzeitig entdecken zu können. Aber auch Sicherheitsprobleme und Angriffe auf die betriebenen Netzdienste können anhand von Protokollierungsdaten nachvollzogen werden. Ebenso können mit solchen Daten durch forensische Untersuchungen Beweise gesichert werden, nachdem ein Angriff auf IT-Systeme oder Anwendungen bekannt wurde.

In jedem Informationsverbund werden lokal Protokollierungsdaten von einer Vielzahl von IT-Systemen und Anwendungen generiert. Um jedoch einen Gesamtüberblick über einen Informationsverbund zu erhalten, können die von verschiedenen IT-Systemen und Anwendungen generierten Protokollierungsereignisse an eine dedizierte Protokollierungsinfrastruktur gesendet und dort zentral gespeichert werden. Nur so lassen sich die Protokollierungsdaten an einer zentralen Stelle auswählen, filtern und systematisch auswerten.

1.2. Zielsetzung

Ziel des Bausteins ist es, alle relevanten Daten sicher zu erheben, zu speichern und geeignet für die Auswertung bereitzustellen, damit möglichst alle sicherheitsrelevanten Ereignisse protokolliert werden können.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.1.1.5 *Protokollierung* ist einmal auf den gesamten Informationsverbund anzuwenden.

Im vorliegenden Baustein werden ausschließlich übergreifende Aspekte betrachtet, die für eine angemessene Protokollierung erforderlich sind. Die Protokollierung spezifischer IT-Systeme oder Anwendungen wird hier nicht behandelt, sondern in den jeweiligen Bausteinen des IT-Grundschutz-Kompendiums beschrieben.

In vielen Betriebssystemen oder Anwendungen sind Protokollierungsfunktionen bereits vorhanden oder können dort mittels Zusatzprodukten integriert werden. Um diese Funktionen und die

gespeicherten Protokollierungsdaten abzusichern, muss das zugrundeliegende Betriebssystem geschützt sein. Das ist jedoch nicht Bestandteil dieses Bausteins. Dafür sind die betriebssystemspezifischen Bausteine umzusetzen, z. B. SYS.1.2.3 *Windows Server*.

Im Vorfeld der Protokollierung von sicherheitsrelevanten Ereignissen ist es wichtig, dass Zuständigkeiten und Kompetenzen klar definiert und zugewiesen werden. Es sollte insbesondere auf den Grundsatz der Funktionstrennung geachtet werden. Dieses Thema ist nicht Bestandteil dieses Bausteins, sondern wird im Baustein ORP.1 *Organisation* behandelt.

Auch ist dieser Baustein abzugrenzen von der Detektion von sicherheitsrelevanten Ereignissen (siehe DER.1 *Detektion von sicherheitsrelevanten Ereignissen*) sowie der Reaktion auf Sicherheitsvorfälle (siehe DER.2.1 *Behandlung von Sicherheitsvorfällen*). Beide Aspekte werden im vorliegenden Baustein nicht oder nur am Rande behandelt.

Ebenfalls an anderer Stelle beschrieben werden die Auswertung von Protokollierungsdaten sowie deren langfristige, sichere, unveränderbare und reproduzierbare Speicherung (siehe DER.1 *Detektion von sicherheitsrelevanten Ereignissen* bzw. OPS.1.2.2 *Archivierung*).

Vorgaben, wie mit personenbezogenen Daten umzugehen ist, werden im Baustein CON.2 *Datenschutz* beschrieben.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.1.1.5 *Protokollierung* von besonderer Bedeutung.

2.1. Fehlende oder unzureichende Protokollierung

In einem Informationsverbund gibt es häufig IT-Systeme oder Anwendungen, bei denen die Protokollierung in der Grundeinstellung nicht aktiviert wurde. Auch können einzelne IT-Systeme oder Anwendungen manchmal gar nicht protokollieren. In beiden Fällen können wichtige Informationen verloren gehen und Angriffe nicht rechtzeitig erkannt werden. Das ist auch dann möglich, wenn die Protokollierung bei einzelnen IT-Systemen oder Anwendungen zwar genutzt wird, aber die Protokollierungsdaten nicht an einer zentralen Stelle zusammengeführt werden. In Informationsverbünden ohne zentrale Protokollierung lässt sich schwer sicherstellen, dass die relevanten Protokollinformationen aller IT-Systeme und Anwendungen erhalten bleiben und ausgewertet werden.

Weiterhin müssen Protokollierungsdaten aussagekräftige Informationen enthalten. Welche Ereignisse protokolliert werden, hängt unter anderem auch vom Schutzbedarf der jeweiligen IT-Systeme oder Anwendungen ab. Wird dieser missachtet, indem beispielsweise bei der Protokollierung nur auf Standard-Einstellungen der IT-Systeme bzw. Anwendungen zurückgegriffen wird, kann dies dazu führen, dass besonders relevante Sicherheitsereignisse nicht protokolliert werden. Somit werden Angriffe eventuell nicht erkannt.

2.2. Fehlerhafte Auswahl von relevanten Protokollierungsdaten

Protokollierungsdaten liefern oft wichtige Informationen, die dabei helfen, Sicherheitsvorfälle zu erkennen. Eine besondere Herausforderung ist es, die relevanten Meldungen aus der großen Menge der verschiedenen Protokollierungsereignisse herauszufiltern. Denn viele Protokollierungsereignisse haben nur informativen Charakter und lenken von den wirklich wichtigen Meldungen ab. Werden zu viele Protokollierungsereignisse ausgewählt, lässt sich die Fülle an Informationen nur schwer und mit hohem Zeitaufwand auswerten.

Des Weiteren können Protokollierungsereignisse verworfen oder überschrieben werden, wenn der Arbeitsspeicher oder die Festplattenkapazität des IT-Systems bzw. der Protokollierungsinfrastruktur nicht ausreichen. Werden dadurch zu wenige oder nicht ausreichend relevante Protokollierungsereignisse aufgezeichnet, dann könnten sicherheitskritische Vorfälle unerkannt bleiben.

2.3. Fehlende oder fehlerhafte Zeitsynchronisation bei der Protokollierung

Wenn in einem Informationsverbund die Zeit nicht auf allen IT-Systemen synchronisiert wird, können die Protokollierungsdaten eventuell nicht miteinander korreliert werden bzw. kann die Korrelation eventuell zu fehlerhaften Aussagen führen. Grund dafür ist, dass die unterschiedlichen Zeitstempel von Ereignissen keine gemeinsame Basis aufweisen. Eine fehlende Zeitsynchronisation erschwert es somit, erhobene Protokollierungsdaten auszuwerten, insbesondere, wenn diese auf einem zentralen Logserver gespeichert werden. Weiterhin kann eine fehlerhafte oder fehlende Zeitsynchronisation dazu führen, dass die Protokollierung nicht zur Beweissicherung herangezogen werden kann.

2.4. Fehlplanung bei der Protokollierung

Wird die Protokollierung nicht ausreichend geplant, dann kann dies dazu führen, dass IT-Systeme oder Anwendungen nicht überwacht und sicherheitsrelevante Ereignisse somit nicht erkannt und angemessen behandelt werden. Datenschutzverstöße könnten ebenfalls nicht nachvollzogen werden.

2.5. Vertraulichkeits- und Integritätsverlust von Protokollierungsdaten

Einige IT-Systeme in einem Informationsverbund generieren Protokollierungsdaten wie Anmeldenamen, IP-Adressen, E-Mail-Adressen und Rechnernamen, die konkreten Personen zugeordnet werden können. Solche Informationen lassen sich kopieren, abhören und manipulieren, wenn sie nicht verschlüsselt übertragen und gesichert gespeichert werden. Dies kann dazu führen, dass Angreifende auf vertrauliche Informationen zugreifen oder dass, durch manipulierte Protokollierungsdaten, Sicherheitsvorfälle bewusst verschleiert werden. Ebenso können Angreifende, wenn sie an eine größere Menge von Protokollierungsdaten gelangen, diese Informationen nutzen, um die interne Struktur des Informationsverbunds aufzudecken und dadurch ihre Angriffe gezielter ausrichten.

2.6. Falsch konfigurierte Protokollierung

Wenn die Protokollierung in IT-Systemen falsch konfiguriert ist, werden wichtige Informationen entweder fehlerhaft oder gar nicht aufgezeichnet. Auch kann es sein, dass zu viele oder falsche Informationen protokolliert werden. So können z. B. personenbezogene Daten unberechtigt protokolliert und gespeichert werden. Die Institution könnte dadurch gegen gesetzliche Anforderungen verstoßen.

Durch eine falsch konfigurierte Protokollierung ist es ebenso möglich, dass die Protokollierungsdaten in inkonsistenten oder proprietären Formaten vorliegen. Dadurch lassen sich die Protokolle eventuell nur schwer auswerten und Sicherheitsvorfälle bleiben unentdeckt.

2.7. Ausfall von Datenquellen für Protokollierungsdaten

Liefern IT-Systeme in einem Informationsverbund nicht mehr die notwendigen Protokollierungsdaten, lassen sich Sicherheitsvorfälle nicht mehr angemessen detektieren. Ursache für solche Ausfälle von Datenquellen können Fehler in der Hard- und Software oder auch fehlerhaft

administrierte IT-Systeme sein. Besonders, wenn nicht bemerkt wird, dass Datenquellen ausgefallen sind, kann dies zu einem falschen Bild der Sicherheitslage in der Institution führen. Dadurch können Angreifende z. B. sehr lange unbemerkt bleiben und institutionskritische Informationen abgreifen oder Produktionssysteme manipulieren.

2.8. Ungenügend dimensionierte Protokollierungsinfrastruktur

Aufgrund der komplexen Informationsverbünde und der vielfältigen Angriffsszenarien steigen die Anforderungen an die Protokollierung, da sehr viele Protokollierungsdaten gespeichert und verarbeitet werden müssen. Weiterhin ist es bei Sicherheitsvorfällen üblich, die Intensität der Protokollierung zu erhöhen. Ist die Protokollierungsinfrastruktur dafür jedoch nicht ausgelegt, kann es passieren, dass Protokollierungsdaten unvollständig gespeichert werden. Somit lassen sich sicherheitsrelevante Ereignisse nicht mehr oder nur unzureichend auswerten und Sicherheitsvorfälle bleiben unentdeckt.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.1.1.5 *Protokollierung* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Fachverantwortliche

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

OPS.1.1.5.A1 Erstellung einer Sicherheitsrichtlinie für die Protokollierung (B) [Fachverantwortliche]

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution MUSS eine spezifische Sicherheitsrichtlinie für die Protokollierung erstellt werden. In dieser Sicherheitsrichtlinie MÜSSEN nachvollziehbar Anforderungen und Vorgaben beschrieben sein, wie die Protokollierung zu planen, aufzubauen und sicher zu betreiben ist. In der spezifischen Sicherheitsrichtlinie MUSS geregelt werden, wie, wo und was zu protokollieren ist. Dabei SOLLTEN sich Art und Umfang der Protokollierung am Schutzbedarf der Informationen orientieren.

Die spezifische Sicherheitsrichtlinie MUSS von dem oder der ISB gemeinsam mit den Fachverantwortlichen erstellt werden. Sie MUSS allen für die Protokollierung zuständigen Mitarbeitenden bekannt und grundlegend für ihre Arbeit sein. Wird die spezifische Sicherheitsrichtlinie verändert oder wird von den Anforderungen abgewichen, MUSS dies mit dem oder der ISB abgestimmt und dokumentiert werden. Es MUSS regelmäßig überprüft werden, ob die spezifische Sicherheitsrichtlinie noch korrekt umgesetzt ist. Die Ergebnisse der Überprüfung MÜSSEN dokumentiert werden.

OPS.1.1.5.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

OPS.1.1.5.A3 Konfiguration der Protokollierung auf System- und Netzebene (B)

Alle sicherheitsrelevanten Ereignisse von IT-Systemen und Anwendungen MÜSSEN protokolliert werden. Sofern die in der Protokollierungsrichtlinie als relevant definierten IT-Systeme und Anwendungen über eine Protokollierungsfunktion verfügen, MUSS diese benutzt werden. Wenn die Protokollierung eingerichtet wird, MÜSSEN dabei die Vorgaben des herstellenden Unternehmens für die jeweiligen IT-Systeme oder Anwendungen beachtet werden.

In angemessenen Intervallen MUSS stichpunktartig überprüft werden, ob die Protokollierung noch korrekt funktioniert. Die Prüfintervalle MÜSSEN in der Protokollierungsrichtlinie definiert werden.

Falls betriebs- und sicherheitsrelevante Ereignisse nicht auf einem IT-System protokolliert werden können, MÜSSEN zusätzliche IT-Systeme zur Protokollierung (z. B. von Ereignissen auf Netzebene) integriert werden.

OPS.1.1.5.A4 Zeitsynchronisation der IT-Systeme (B)

Die Systemzeit aller protokollierenden IT-Systeme und Anwendungen MUSS immer synchron sein. Es MUSS sichergestellt sein, dass das Datums- und Zeitformat der Protokolldateien einheitlich ist.

OPS.1.1.5.A5 Einhaltung rechtlicher Rahmenbedingungen (B)

Bei der Protokollierung MÜSSEN die Bestimmungen aus den aktuellen Gesetzen zum Bundes- sowie Landesdatenschutz eingehalten werden (siehe CON.2 *Datenschutz*).

Darüber hinaus MÜSSEN eventuelle Persönlichkeitsrechte bzw. Mitbestimmungsrechte der Mitarbeitendenvertretungen gewahrt werden.

Ebenso MUSS sichergestellt sein, dass alle weiteren relevanten gesetzlichen Bestimmungen beachtet werden.

Protokollierungsdaten MÜSSEN nach einem festgelegten Prozess gelöscht werden. Es MUSS technisch unterbunden werden, dass Protokollierungsdaten unkontrolliert gelöscht oder verändert werden.

3.2. Standard-Anforderungen

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

OPS.1.1.5.A6 Aufbau einer zentralen Protokollierungsinfrastruktur (S)

Alle gesammelten sicherheitsrelevanten Protokollierungsdaten SOLLTEN an einer zentralen Stelle gespeichert werden. Dafür SOLLTE eine zentrale Protokollierungsinfrastruktur im Sinne eines Logserver-Verbunds aufgebaut und in einem hierfür eingerichteten Netzsegment platziert werden (siehe NET.1.1 *Netzarchitektur und -design*).

Zusätzlich zu sicherheitsrelevanten Ereignissen (siehe OPS.1.1.5.A3 *Konfiguration der Protokollierung auf System- und Netzebene*) SOLLTE eine zentrale Protokollierungsinfrastruktur auch allgemeine Betriebsereignisse protokollieren, die auf einen Fehler hindeuten.

Die Protokollierungsinfrastruktur SOLLTE ausreichend dimensioniert sein. Die Möglichkeit einer Skalierung im Sinne einer erweiterten Protokollierung SOLLTE berücksichtigt werden. Dafür SOLLTEN genügend technische, finanzielle und personelle Ressourcen verfügbar sein.

OPS.1.1.5.A7 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.1.5.A8 Archivierung von Protokollierungsdaten (S)

Protokollierungsdaten SOLLTEN archiviert werden. Dabei SOLLTEN die gesetzlich vorgeschriebenen Regelungen berücksichtigt werden.

OPS.1.1.5.A9 Bereitstellung von Protokollierungsdaten für die Auswertung (S)

Die gesammelten Protokollierungsdaten SOLLTEN gefiltert, normalisiert, aggregiert und korreliert werden. Die so bearbeiteten Protokollierungsdaten SOLLTEN geeignet verfügbar gemacht werden, damit sie ausgewertet werden können.

Damit sich die Daten automatisiert auswerten lassen, SOLLTEN die Protokollanwendungen über entsprechende Schnittstellen für die Auswertungsprogramme verfügen.

Es SOLLTE sichergestellt sein, dass bei der Auswertung von Protokollierungsdaten die Sicherheitsanforderungen eingehalten werden, die in der Protokollierungsrichtlinie definiert sind. Auch wenn die Daten bereitgestellt werden, SOLLTEN betriebliche und interne Vereinbarungen berücksichtigt werden.

Die Protokollierungsdaten SOLLTEN zusätzlich in unveränderter Originalform aufbewahrt werden.

OPS.1.1.5.A10 Zugriffsschutz für Protokollierungsdaten (S)

Es SOLLTE sichergestellt sein, dass die ausführenden Administrierenden selbst keine Berechtigung haben, die aufgezeichneten Protokollierungsdaten zu verändern oder zu löschen.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

OPS.1.1.5.A11 Steigerung des Protokollierungsumfangs (H)

Bei erhöhtem Schutzbedarf von Anwendungen oder IT-Systemen SOLLTEN grundsätzlich mehr Ereignisse protokolliert werden, sodass sicherheitsrelevante Vorfälle möglichst lückenlos nachvollziehbar sind.

Um die Protokollierungsdaten in Echtzeit auswerten zu können, SOLLTEN sie in verkürzten Zeitabständen von den protokollierenden IT-Systemen und Anwendungen zentral gespeichert werden. Die Protokollierung SOLLTE eine Auswertung über den gesamten Informationsverbund ermöglichen. Anwendungen und IT-Systeme, mit denen eine zentrale Protokollierung nicht möglich ist, SOLLTEN bei einem erhöhten Schutzbedarf NICHT eingesetzt werden.

OPS.1.1.5.A12 Verschlüsselung der Protokollierungsdaten (H)

Um Protokollierungsdaten sicher übertragen zu können, SOLLTEN sie verschlüsselt werden. Alle gespeicherten Protokolle SOLLTEN digital signiert werden. Auch archivierte und außerhalb der Protokollierungsinfrastruktur gespeicherte Protokollierungsdaten SOLLTEN immer verschlüsselt gespeichert werden.

OPS.1.1.5.A13 Hochverfügbare Protokollierungsinfrastruktur (H)

Eine hochverfügbare Protokollierungsinfrastruktur SOLLTE aufgebaut werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) regelt in seinem Mindeststandard „Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen“ die Protokollierung und Detektion von sicherheitsrelevanten Ereignissen (SRE). Die Mindeststandards sind von den in § 8 Abs. 1 Satz 1 BSIG genannten Stellen der Bundesverwaltung umzusetzen.

Die International Organization for Standardization (ISO) macht in der Norm ISO/IEC 27001:2013 im Kapitel A.12.4 „Protokollierung und Überwachung“ Vorgaben zur Protokollierung.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ in Kapitel TM1.2 - Security Event Logging - Vorgaben zur Protokollierung.

Das National Institute of Standards and Technology (NIST) beschreibt in seiner Special Publication 800-92 „Guide to Computer Security Log Management“, wie Protokollierung sicher eingesetzt werden kann.

Bundesamt
für Sicherheit in der
Informationstechnik

OPS.1.1.6 Software-Tests und -Freigaben

1. Beschreibung

1.1. Einleitung

Der Einsatz von IT in Institutionen setzt voraus, dass die maschinelle Datenverarbeitung soweit wie möglich fehlerfrei funktioniert, da die Einzelergebnisse in den meisten Fällen nicht mehr kontrolliert werden können. Deswegen muss Software jeglicher Art schon vor Inbetriebnahme im Rahmen von Software-Tests überprüft werden. In diesen Tests muss nachgewiesen werden, dass die Software die erforderlichen Funktionen zuverlässig bereitstellt und darüber hinaus keine unerwünschten Nebeneffekte aufweist. Mit der anschließenden Freigabe der Software durch die fachlich zuständige Organisationseinheit wird die grundsätzliche Erlaubnis erteilt, die Software produktiv in der Institution zu nutzen. Gleichzeitig übernimmt diese Organisationseinheit damit auch die Verantwortung für das IT-Verfahren, das durch die Software unterstützt wird.

Software kann an unterschiedlichen Stellen ihres Lebenszyklus getestet werden. So können Software-Tests bereits bei der Entwicklung, vor der Freigabe für den Produktivbetrieb oder im Zuge des Patch- und Änderungsmanagements notwendig werden. Dies betrifft sowohl Individualsoftware als auch standardisierte Software. Eine besondere Rolle nehmen hierbei Regressionstests ein, denn selbst wenn nur kleinere Aspekte der Software geändert werden, besteht die Möglichkeit, dass sich dies auf ganz andere Aspekte und Funktionen der Software auswirkt. Regressionstests überprüfen Software genau auf diese Auswirkungen hin.

Dieser Baustein beschreibt den Test- und Freigabeprozess für jegliche Art von Software. Der Test- und Freigabeprozess zeichnet sich dadurch aus, dass dieser je nach Ergebnis mehrmals durchlaufen werden kann.

1.2. Zielsetzung

Mit der Umsetzung dieses Bausteins sorgt die Institution dafür, dass die eingesetzte Software den technischen und organisatorischen Anforderungen sowie dem vorliegenden Schutzbedarf der gesamten Institution oder einzelner Organisationseinheiten entspricht. Ein wesentlicher Teilaspekt ist dabei, dass sicherheitskritische Software auf bestehende Schwachstellen systematisch und methodisch überprüft wird.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.1.1.6 *Software-Tests und Freigaben* ist auf den Informationsverbund einmal anzuwenden.

Während der Baustein CON.8 *Software-Entwicklung* auf den Softwareentwicklungsprozess und die darin enthaltenen Software-Tests, die während des Entwicklungsprozesses notwendig sind, eingeht, beschreibt dieser Baustein die speziellen Anforderungen, die an ein Test- und Freigabemanagement gestellt werden. Dabei bezieht sich dieses Test- und Freigabemanagement nicht ausschließlich auf selbst oder im Auftrag der Kundschaft entwickelte Software, sondern auch auf das Testen und die Freigabe von jeglicher Software, wie sie in APP.6 *Allgemeine Software* beschrieben wird, sowie alle weiteren Softwareprodukten der Schicht APP *Anwendungen*.

Software-Tests können auch Bestandteil des Patch- oder Änderungsmanagements oder der Software-Entwicklung werden. Entsprechende Anforderungen sind im Baustein OPS.1.1.3 *Patch- und Änderungsmanagement* sowie CON.8 *Software-Entwicklung* näher spezifiziert.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.*1.1.6 Software-Tests und -Freigaben* von besonderer Bedeutung.

2.1. Software-Tests mit Produktivdaten

Werden Software-Tests mit Produktivdaten durchgeführt, können hierdurch Sicherheitsprobleme entstehen. Insbesondere vertrauliche Produktivdaten könnten dabei von unbefugten Mitarbeitenden oder Dritten eingesehen werden, die mit dem jeweiligen Software-Test beauftragt wurden. Wird mit den „originalen“ Produktivdaten getestet und nicht mit Kopien der Daten, könnten diese ungewollt geändert oder gelöscht werden.

Durch Software-Tests im Produktivbetrieb könnte der gesamte Betrieb massiv gestört werden. Denn Fehlfunktionen der zu testenden Software können sich auch auf andere Anwendungen und IT-Systeme auswirken, die dadurch ebenfalls gestört werden. Hinzu kommt, dass Software-Testende bewusst die Software im Grenzbereich testen und damit beabsichtigen, mögliche Fehler aufzudecken. Dies erhöht wiederum die Gefahr, dass der gesamte Betrieb gestört wird.

2.2. Fehlendes oder unzureichendes Testverfahren

Wird neue Software nicht oder nur unzureichend getestet und ohne Installationsvorschriften freigegeben, können Fehler in der Software unerkannt bleiben. Ebenso ist es möglich, dass dadurch erforderliche und einzuhaltende Installationsparameter nicht erkannt oder nicht beachtet werden.

Diese Software- oder Installationsfehler, die aus einem fehlenden oder unzureichenden Software-Testverfahren resultieren, können den IT-Betrieb der Institution erheblich gefährden. So können beispielsweise wichtige Daten verloren gehen, wenn ein Software-Update eingespielt wird.

2.3. Fehlendes oder unzureichendes Freigabeverfahren

Ein fehlendes oder unzureichendes Freigabeverfahren kann dazu führen, dass Software eingesetzt wird, die von der Fachseite nicht abgenommen wurde. Auf diese Weise kann die Software Funktionen umfassen, die sie nicht enthalten sollte, die nicht wie gewünscht funktionieren oder benötigte Funktionen können fehlen. Außerdem kann die Software zu anderen Anwendungen inkompatibel sein.

2.4. Fehlende oder unzureichende Dokumentation der Tests und Testergebnisse

Software kann in der Regel freigegeben werden, sobald alle Tests durchgeführt wurden und keine Abweichungen gefunden wurden. Sollte die Dokumentation der Software-Tests jedoch unvollständig sein, ist nachträglich nicht erkennbar, was getestet wurde. Wurden erkannte Softwarefehler oder fehlende Funktionen ungenügend dokumentiert und damit bei der Freigabe nicht berücksichtigt, können durch diese Abweichungen die zu verarbeitenden Produktivdaten ungewollt gelöscht oder verändert werden. Außerdem können andere IT-Systeme und Anwendungen gestört werden.

2.5. Fehlende oder unzureichende Dokumentation der Freigabekriterien

Wenn Freigabekriterien nicht klar kommuniziert werden, kann dies dazu führen, dass Software voreilig freigegeben wird oder keine Freigabe erfolgt, obwohl diese erteilt werden könnte. Dadurch könnten zum einen Versionen mit unerkannten Softwarefehlern freigegeben werden, die den Produktivbetrieb stören können. Zum anderen kann eine fehlende oder unzureichende Dokumentation der Freigabekriterien dazu führen, dass sich Projekte verzögern und dadurch finanzielle Schäden entstehen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.1.1.6 *Software-Tests und -Freigaben* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Testende, Fachverantwortliche, Datenschutzbeauftragte, Personalabteilung

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

OPS.1.1.6.A1 Planung der Software-Tests (B)

Die Rahmenbedingungen für Software-Tests MÜSSEN vor den Tests innerhalb der Institution entsprechend der Schutzbedarfe, Organisationseinheiten, technischen Möglichkeiten und Test-Umgebungen festlegt sein. Die Software MUSS auf Basis der Anforderungen des Anforderungskatalogs zu der Software getestet werden. Liegt auch ein Pflichtenheft vor, dann MUSS dieses zusätzlich berücksichtigt werden.

Die Testfälle MÜSSEN so ausgewählt werden, sodass diese möglichst repräsentativ alle Funktionen der Software überprüfen. Zusätzlich SOLLTEN auch Negativ-Tests berücksichtigt werden, die überprüfen, ob die Software keine ungewollten Funktionen enthält.

Die Testumgebung MUSS so ausgewählt werden, sodass diese möglichst repräsentativ alle in der Institution eingesetzten Gerätemodelle und Betriebssystemumgebungen abdeckt. Es SOLLTE dabei getestet werden, ob die Software mit den eingesetzten Betriebssystemen in den vorliegenden Konfigurationen kompatibel und funktionsfähig ist.

OPS.1.1.6.A2 Durchführung von funktionalen Software-Tests (B) [Testende]

Mit funktionalen Software-Tests MUSS die ordnungsgemäße und vollständige Funktion der Software überprüft werden. Die funktionalen Software-Tests MÜSSEN so durchgeführt werden, dass sie den Produktivbetrieb nicht beeinflussen.

OPS.1.1.6.A3 Auswertung der Testergebnisse (B) [Testende]

Die Ergebnisse der Software-Tests MÜSSEN ausgewertet werden. Es SOLLTE ein Soll-Ist-Vergleich mit definierten Vorgaben durchgeführt werden. Die Auswertung MUSS dokumentiert werden.

OPS.1.1.6.A4 Freigabe der Software (B) [Fachverantwortliche]

Die fachlich zuständige Organisationseinheit MUSS die Software freigeben, sobald die Software-Tests erfolgreich durchgeführt wurden. Die Freigabe MUSS in Form einer Freigabeerklärung dokumentiert werden.

Die freigebende Organisationseinheit MUSS überprüfen, ob die Software gemäß den Anforderungen getestet wurde. Die Ergebnisse der Software-Tests MÜSSEN mit den vorher festgelegten Erwartungen übereinstimmen. Auch MUSS überprüft werden, ob die rechtlichen und organisatorischen Vorgaben eingehalten wurden.

OPS.1.1.6.A5 Durchführung von Software-Tests für nicht funktionale Anforderungen (B) [Testende]

Es MÜSSEN Software-Tests durchgeführt werden, die überprüfen, ob alle wesentlichen nichtfunktionalen Anforderungen erfüllt werden. Insbesondere MÜSSEN sicherheitsspezifische Software-Tests durchgeführt werden, wenn die Anwendung sicherheitskritische Funktionen mitbringt. Die durchgeführten Testfälle, sowie die Testergebnisse, MÜSSEN dokumentiert werden.

OPS.1.1.6.A11 Verwendung von anonymisierten oder pseudonymisierten Testdaten (B) [Datenschutzbeauftragte, Testende]

Wenn Produktivdaten für Software-Tests verwendet werden, die schützenswerte Informationen enthalten, dann MÜSSEN diese Testdaten angemessen geschützt werden. Enthalten diese Daten personenbezogene Informationen, dann MÜSSEN diese Daten mindestens pseudonymisiert werden. Falls möglich, SOLLTEN die Testdaten mit Personenbezug vollständig anonymisiert werden. Wenn ein Personenbezug von den Testdaten abgeleitet werden könnte, MUSS der oder die Datenschutzbeauftragte und unter Umständen die Personalvertretung hinzugezogen werden.

3.2. Standard-Anforderungen

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

OPS.1.1.6.A6 Geordnete Einweisung der Software-Testenden (S) [Fachverantwortliche]

Die Software-Testenden SOLLTEN über die durchzuführenden Testarten und die zu testenden Bereiche einer Software von Fachverantwortlichen informiert werden. Darüber hinaus SOLLTEN die

Software-Testende über die Anwendungsfälle und mögliche weitere Anforderungen der Software informiert werden.

OPS.1.1.6.A7 Personalauswahl der Software-Testenden (S) [Personalabteilung, Fachverantwortliche]

Bei der Auswahl der Software-Testenden SOLLTEN gesonderte Auswahlkriterien berücksichtigt werden. Die Software-Testenden SOLLTEN die erforderliche berufliche Qualifikation haben.

Wird Individualsoftware auf Quellcode-Ebene überprüft, dann SOLLTEN die Testenden über ausreichendes Fachwissen über die zu testenden Programmiersprache und der Entwicklungsumgebung verfügen. Der Quellcode SOLLTE NICHT ausschließlich von Testenden überprüft werden, die auch an der Erstellung des Quellcodes beteiligt waren.

OPS.1.1.6.A8 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.1.6.A9 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.1.6.A10 Erstellung eines Abnahmeplans (S)

In einem Abnahmeplan SOLLTEN die durchzuführenden Testarten, Testfälle und die erwarteten Ergebnisse dokumentiert sein. Außerdem SOLLTE der Abnahmeplan die Freigabekriterien beinhalten. Es SOLLTE eine Vorgehensweise für die Situation festgelegt werden, wenn eine Freigabe abgelehnt wird.

OPS.1.1.6.A12 Durchführung von Regressionstests (S) [Testende]

Wenn Software verändert wurde, SOLLTEN Regressionstests durchgeführt werden. Hierbei SOLLTE überprüft werden, ob bisherige bestehende Sicherheitsmechanismen und -einstellungen durch das Update ungewollt verändert wurden. Regressionstests SOLLTEN vollständig durchgeführt werden und hierbei auch Erweiterungen sowie Hilfsmittel umfassen. Werden Testfälle ausgelassen, SOLLTE dies begründet und dokumentiert werden. Die durchgeführten Testfälle und die Testergebnisse SOLLTEN dokumentiert werden.

OPS.1.1.6.A13 Trennung der Testumgebung von der Produktivumgebung (S)

Software SOLLTE nur in einer hierfür vorgesehenen Testumgebung getestet werden. Die Testumgebung SOLLTE von der Produktivumgebung getrennt betrieben werden. Die in der Testumgebung verwendeten Architekturen und Mechanismen SOLLTEN dokumentiert werden. Es SOLLTEN Verfahren dokumentiert werden, wie mit der Testumgebung nach Abschluss des Software-Tests zu verfahren ist.

OPS.1.1.6.A15 Überprüfung der Installation und zugehörigen Dokumentation (S) [Testende]

Die Installation der Software SOLLTE entsprechend der Regelungen zur Installation und Konfiguration von Software (siehe Baustein APP.6 *Allgemeine Software*) überprüft werden. Falls vorhanden, SOLLTE zusätzlich die Installations- und Konfigurationsdokumentation geprüft werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

OPS.1.1.6.A14 Durchführung von Penetrationstests (H) [Testende]

Für Anwendungen beziehungsweise IT-Systeme mit erhöhtem Schutzbedarf SOLLTEN Penetrationstests als Testmethode durchgeführt werden. Ein Konzept für Penetrationstests SOLLTE erstellt werden. Im Konzept für Penetrationstests SOLLTEN neben den zu verwendenden Testmethoden auch die Erfolgskriterien dokumentiert werden.

Der Penetrationstest SOLLTE nach den Rahmenbedingungen des Penetrationstest-Konzepts erfolgen. Die durch den Penetrationstest aufgefundenen Sicherheitslücken SOLLTEN klassifiziert und dokumentiert sein.

OPS.1.1.6.A16 Sicherheitsüberprüfung der Testenden (H)

Sofern Testende auf besonders schützenswerte Informationen zugreifen müssen, SOLLTE die Institution Nachweise über ihre Integrität und Reputation einholen. Handelt es sich dabei um klassifizierte Verschlusssachen, SOLLTEN sich die Software-Testenden einer Sicherheitsüberprüfung nach dem Sicherheitsüberprüfungsgesetz (SÜG) unterziehen. Hierzu SOLLTE der oder die ISB die Geheimschutzbeauftragten bzw. Sicherheitsbevollmächtigten der Institution einbeziehen.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 im Annex A.14 „System Acquisition, Development and maintenance“ Anforderungen an die sichere System-Entwicklung, die auch einen Test- und Freigabeprozess erfordert, sowie direkt an Testdaten selbst. Darüber hinaus hat die ISO die Norm ISO/IEC 29119-2:2013 „Software and systems engineering - Software testing - Part 2: Test processes, International Organization for Standardization“ veröffentlicht, die ausführlich Anforderungen an Software-Tests behandelt.

Das BSI hat die Studie „Durchführungskonzept für Penetrationstests“, die als Grundlage für Penetrationstests verwendet werden kann, sowie den BSI-Leitfäden zur Entwicklung sicherer Webanwendungen, der auch Software-Tests inkludiert, veröffentlicht.

Das Information Security Forum (ISF) führt in „The Standard of Good Practice for Information Security“ Aspekte zum Testen und Freigeben zu allen relevanten Anforderungen (Areas) aus.

Das National Institute of Standards and Technology stellt Richtlinien zum Testen von Software in der NIST Publication 800-53 in der SA 11 Developer Security Testing and Evaluation zur Verfügung.

Das Buch „The Art of Software Testing“ von Glenford J. Myers, Corey Sandler, Tom Badgett, kann für Software-Tests konsultiert werden.

Das Common Vulnerability Scoring System kann als Scoring-System zur Klassifikation des Schweregrades einer Sicherheitslücke verwendet werden und somit die Ergebnisse von Software-Tests in Bezug auf die Informationssicherheit darstellen.

Bundesamt
für Sicherheit in der
Informationstechnik

OPS.1.1.7 Systemmanagement

1. Beschreibung

1.1. Einleitung

Ein zuverlässiges Systemmanagement ist Grundvoraussetzung für den sicheren und effizienten Betrieb moderner vernetzter Systeme. Dazu ist es erforderlich, dass ein Systemmanagement alle relevanten Systeme umfassend integriert. Außerdem müssen geeignete Maßnahmen umgesetzt werden, um die Systemmanagement-Kommunikation und -infrastruktur zu schützen.

Das Systemmanagement umfasst viele wichtige Funktionen wie z. B. die Systemüberwachung, die Konfiguration der Systeme, die Behandlung von Ereignissen und die Protokollierung. Eine weitere wichtige Funktion ist das Reporting, das auch als gemeinsame Plattform für IT-Systeme und Netzkomponenten angelegt werden kann. Alternativ kann es dediziert als einheitliche Plattform oder als Bestandteil der einzelnen Systemmanagement-Komponenten realisiert werden.

Die Systemmanagement-Lösung besteht aus verschiedenen Systemmanagement-Komponenten, zum Beispiel Agenten, die auf einer zugrundeliegenden Systemmanagement-Infrastruktur betrieben werden. Diese Lösung wird genutzt, um die eingebundenen und zu verwaltenden Systeme über die entsprechenden Schnittstellen des Informationsverbundes zu steuern. Die Kombination aus der Lösung, der zugrundeliegenden Infrastruktur, den zu verwaltenden Systemen und dem Betrieb bildet die Gesamtheit des Systemmanagements.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, die Informationssicherheit als integralen Bestandteil des Systemmanagements zu etablieren. Der Baustein beschreibt zum einen, wie das Systemmanagement aufgebaut und abgesichert werden kann, und zum anderen, wie die zugehörige Kommunikation geschützt werden kann.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.1.1.7 *Systemmanagement* ist auf die Systemmanagement-Lösung anzuwenden, die im Informationsverbund eingesetzt wird.

Um ein IT-Grundschutz-Modell für einen konkreten Informationsverbund zu erstellen, muss grundsätzlich die Gesamtheit aller Bausteine betrachtet werden. In der Regel sind mehrere Bausteine auf das Thema bzw. Zielobjekt anzuwenden.

Dieser Baustein behandelt z. B.

- die notwendigen Systemmanagement-Komponenten,
- die konzeptionellen Aufgaben zum Systemmanagement,
- Protokollierung unter dem Gesichtspunkt des Systemmanagements sowie
- die Aktualisierung der Systemmanagement-Lösung.

Folgende Inhalte sind ebenfalls von Bedeutung und werden an anderer Stelle behandelt:

- Anforderungen zum Netzmanagement (siehe NET.1.2 *Netzmanagement)*
- Details bezüglich der Absicherung der zugrundeliegenden Infrastruktur und von zu verwaltenden IT-Systemen, insbesondere deren Management-Schnittstellen (siehe SYS.2 *IT-Systeme)*
- Protokollierungs- und Archivierungskonzepte (siehe OPS.1.1.5 *Protokollierung*, OPS.1.2.2 *Archivierung*)
- Aktualisierung z. B. durch Zusatzsoftware, sogenannte Agenten (siehe OPS.1.1.3 *Patch- und Änderungsmanagement*)
- Zugriffe von Benutzenden auf die Systemmanagement-Lösung (siehe ORP.4 *Identitäts- und Berechtigungsmanagement*, sowie OPS.1.2.5 *Fernwartung* und OPS.1.1.2 *Ordnungsgemäße IT-Administration*).

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.1.1.7 *Systemmanagement* von besonderer Bedeutung.

2.1. Unberechtigter Zugriff auf die Systemmanagement-Lösung

Das Systemmanagement ist aufgrund seiner zentralen Stellung und aufgrund der notwendigen Zugriffsrechte auf alle zu verwaltenden Systeme ein vorrangiges Ziel für Angriffe.

Wenn es Angreifenden gelingt auf Systemmanagement-Lösungen zuzugreifen, z. B. durch ungepatchte Sicherheitslücken, dann können diese alle vom Systemmanagement verwalteten Systeme kontrollieren und neu konfigurieren. So können sie z. B. auf schützenswerte Informationen zugreifen oder auch Dienste oder verwaltete Systeme stören. Beispielsweise könnte ein Unternehmen zentral Konfigurationsserver für eine Systemmanagementlösung bereitstellen. Über eine ungepatchte Schwachstelle werden in diesem Beispiel die Konfigurationsdateien so verändert, dass die verwalteten Systeme eine Ransomware installieren. In Folge werden in diesem Beispiel alle Systeme, die von dieser Systemmanagementlösung verwaltet werden, verschlüsselt.

2.2. Fehler in Automatisierungsfunktionen für das Systemmanagement

Alle Schutzziele des zu verwaltenden Informationssysteme können durch fehlerhaft automatisierte Abläufe beeinträchtigt sein.

Durch Fehler in einer oder mehreren Automatisierungsfunktionen wie z. B. Skripte, können die zu verwaltenden Systeme funktionsunfähig oder kompromittiert werden. Wegen der automatisierten Abläufe kann schnell eine große Anzahl von IT-Systemen kompromittiert werden. Auch besonders kritische IT-Systeme können auf diesem Weg schnell kompromittiert werden.

2.3. Unberechtigte Eingriffe in die Systemmanagement-Kommunikation

Versehentliche Eingriffe in oder gezielte Angriffe auf die Kommunikation des Systemmanagements können die Integrität der verwalteten IT-Systeme verletzen und die Verfügbarkeit von Diensten oder IT-Systemen einschränken.

Wird die Systemmanagement-Kommunikation abgehört und manipuliert, dann können auf diesem Weg aktive Systeme kontrolliert werden. Außerdem können die von und zu den Systemen übertragenen Daten mitgeschnitten und eingesehen werden.

2.4. Unzureichende Zeitsynchronisation der Systemmanagement-Komponenten

Fehler in der Zeitsynchronisation können Probleme und Ereignisse verdecken, sodass z. B. die Erkennung von Sicherheitsvorfällen und Datenabflüssen erschwert wird.

Wenn die Systemzeit der Systemmanagement-Komponenten unzureichend synchronisiert wird, dann können (beispielsweise) Protokolle, die unter anderem Zeitstempel zur Evaluierung der Kommunikationsgültigkeit verwenden, durch unterschiedliche Systemzeiten auf den Systemmanagement-Komponenten und den zu verwaltenden Systemen gestört werden.

Zusätzlich können die Protokollierungsdaten zum Systemmanagement unter Umständen eventuell nicht miteinander korreliert werden. Auch kann die Korrelation eventuell zu fehlerhaften Aussagen führen, wenn Zeitstempel aufgrund fehlerhafter Synchronisation nur scheinbar übereinstimmen oder abweichen.

2.5. Inkompatibilität zwischen den zu verwaltenden Systemen und der Systemmanagement-Lösung

Eine nur unvollständig kompatible Systemmanagement-Lösung kann Fehlfunktionen der zu verwaltenden IT-Systeme auslösen und deren Verfügbarkeit einschränken.

Falls die Systemmanagement-Lösung die zu verwaltenden IT-Systeme nicht vollständig unterstützt, können bestimmte Aktionen nicht wie geplant durchgeführt werden. Diese Gefährdung kann auch bei einer Aktualisierung der Systeme auftreten, bei der die Management-Schnittstellen verändert werden.

2.6. Verbindungsverlust zwischen Anwendenden und Systemmanagement-Lösung

Verbindungsabbrüche können die Verfügbarkeit der Systemmanagement-Lösung einschränken.

Wenn die Verbindung zwischen den Administrierenden und der Systemmanagement-Lösung gestört wird, können IT-Systeme ausfallen. Außerdem können eine Fehlerbehebung und die Verwaltung von IT-Systemen erschwert werden.

Wenn eine Verbindung abbricht oder gestört wird, dann können kostenintensive sicherheitsrelevante sowie zeitkritische Arbeiten nicht fristgerecht durchgeführt werden, beispielsweise können Sicherheitsupdates nicht mehr eingespielt werden oder auf Sicherheitsvorfälle nicht angemessen reagiert werden.

2.7. Verbindungsverlust zwischen Systemmanagement-Lösung und zu verwaltenden Systemen

Verbindungsabbrüche zu den zu verwaltenden Systemen können insbesondere die Verfügbarkeit oder Integrität von Diensten im Informationsverbund beeinträchtigen.

Der Umfang und die Konstellation eines solchen Verbindungsverlusts entscheiden darüber, ob Dienste beeinträchtigt werden und welche Schäden entstehen können. Die resultierenden Fehlerbilder sind unter Umständen schwer zu analysieren und die auftretenden Fehler schwer zu beheben.

2.8. Unzureichende Abstimmung zwischen Systemmanagement und Netzmanagement

Nicht abgestimmte Aktionen im Netzmanagement können sich negativ auf das Systemmanagement auswirken. Dadurch können Inkonsistenzen in der Konfiguration zwischen IT-Systemen und verbindenden Netzen entstehen. So können z. B. Verbindungsverluste im Netz eine große Anzahl von Folgeereignissen im Bereich Systemmanagement auslösen. Diese Ereignisse können bis zu Fehlkonfigurationen reichen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.1.1.7 *Systemmanagement* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

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

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

OPS.1.1.7.A1 Anforderungsspezifikation für das Systemmanagement (B)

Anforderungen an die Systemmanagement-Infrastruktur und -Prozesse MÜSSEN spezifiziert werden. Dabei MÜSSEN alle wesentlichen Elemente für das Systemmanagement berücksichtigt werden. Auch MÜSSEN die Sicherheitsaspekte für das Systemmanagement von Beginn an beachtet werden.

Zudem MÜSSEN die Schnittstellen der zu verwaltenden IT-Systeme dokumentiert werden, z. B. um die Kompatibilität von Systemmanagement-Lösung und zu verwaltendem System zu gewährleisten.

OPS.1.1.7.A2 Planung des Systemmanagements (B)

Die Systemmanagement-Lösung und die zugrundeliegende Infrastruktur MÜSSEN geeignet geplant werden. Die Planung MUSS mindestens die folgenden Inhalte umfassen:

- eine detaillierte Anforderungsanalyse,
- ein aussagekräftiges Grobkonzept,
- einen umfassenden Umsetzungsplan sowie
- Meilensteine für Qualitätssicherung und Abnahme.

Dabei MÜSSEN alle in der Anforderungsspezifikation genannten Punkte sowie das Rollen- und Berechtigungskonzept berücksichtigt werden. Es MÜSSEN mindestens die folgenden Themen berücksichtigt werden:

- Trennung in geeignete Bereiche für das Systemmanagement,
- Zugriffsmöglichkeiten auf und durch das Systemmanagement,
- Berechtigungen des Systemmanagements auf den zu verwaltenden Systemen,
- Netzverbindungen für den Zugriff auf und durch das Systemmanagement,
- Protokolle für den Zugriff von Benutzenden auf die Systemmanagement-Lösung,
- Protokolle für die Kommunikation zwischen der Systemmanagement-Lösung und den zu verwaltenden Systemen,
- Anforderungen an Systemmanagement-Werkzeuge,
- Schnittstellen, um erfasste Ereignis- oder Alarmmeldungen weiterzuleiten,
- Protokollierung, inklusive erforderlicher Schnittstellen zu einer zentralen Protokollierungslösung,
- Unterstützung durch das herstellende bzw. entwickelnde Unternehmen über den geplanten Einsatzzeitraum,
- Möglichkeiten zum Einspielen von Patches für die Systemmanagement-Lösung sowie für die zu verwaltenden Systeme,
- Reporting und Schnittstellen zu übergreifenden Lösungen sowie
- korrespondierende Anforderungen an die zu verwaltenden Systeme.

OPS.1.1.7.A3 Zeitsynchronisation für das Systemmanagement (B)

Alle Komponenten der Systemmanagement-Lösung, inklusive der zu verwaltenden Systeme, MÜSSEN eine synchrone Uhrzeit nutzen. Die Systemzeit MUSS für jedes zu verwaltende System und für die Systemmanagement-Lösung über geeignete Protokolle synchronisiert werden.

OPS.1.1.7.A4 Absicherung der Systemmanagement-Kommunikation (B)

Sobald die Systemmanagement-Lösung und die zu verwaltenden Systeme über die produktive Infrastruktur kommunizieren, MÜSSEN dafür sichere Protokolle verwendet werden. Falls keine sicheren Protokolle verwendet werden können, dann MUSS ein eigens dafür vorgesehenes Administrationsnetz (Out-of-Band-Management) verwendet werden (siehe NET.1.1 *Netzarchitektur und -design*). Ist auch dies nicht möglich, dann MÜSSEN ergänzende Sicherheitsmechanismen auf anderer Ebene eingesetzt werden, z. B. Tunnelmechanismen über verschlüsseltes VPN oder vergleichbare Lösungen.

OPS.1.1.7.A5 Gegenseitige Authentisierung von Systemmanagement-Lösung und zu verwaltenden Systemen (B)

Die Authentisierung zwischen Systemmanagement-Lösung und zu verwaltenden Systemen MUSS in beide Richtungen erfolgen. Die Authentisierung MUSS in das übergreifende Authentisierungskonzept eingebunden sein. Die Authentisierung MUSS mittels sicherer Protokolle erfolgen.

OPS.1.1.7.A6 Absicherung des Zugriffs auf die Systemmanagement-Lösung (B)

Der Zugriff von Benutzenden auf die Systemmanagement-Lösung MUSS abgesichert werden durch

- eine sichere und angemessene Authentisierung und Autorisierung der Benutzenden sowie
- eine sichere Verschlüsselung der übertragenen Daten.

Eine angemessene Authentisierungsmethode MUSS ausgewählt werden. Der Auswahlprozess MUSS dokumentiert werden. Die Stärke der verwendeten kryptografischen Verfahren und Schlüssel MUSS regelmäßig überprüft und bei Bedarf angepasst werden.

Die Systemmanagement-Lösung MUSS über eine Autorisierungskomponente sicherstellen, dass Benutzende ausschließlich solche Aktionen durchführen können, zu denen sie berechtigt sind.

3.2. Standard-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

OPS.1.1.7.A7 Festlegung einer Sicherheitsrichtlinie für das Systemmanagement (S)

Für das Systemmanagement SOLLTE eine Sicherheitsrichtlinie erstellt und nachhaltig gepflegt werden. Die Richtlinie SOLLTE allen Personen, die am Systemmanagement beteiligt sind, bekannt sein. Die Sicherheitsrichtlinie SOLLTE zudem grundlegend für die Arbeit dieser Personen sein. Es SOLLTE regelmäßig und nachvollziehbar überprüft werden, dass die in der Richtlinie geforderten Inhalte umgesetzt werden. Die Ergebnisse SOLLTEN dokumentiert werden.

Die Sicherheitsrichtlinie SOLLTE mindestens das Folgende festlegen:

- die Bereiche des Systemmanagements, die über zentrale Management-Werkzeuge und -Dienste realisiert werden,
- die Aufgaben im Systemmanagement, die automatisiert realisiert werden sollen,
- das Konfigurationsmanagement für die Daten, die von der Systemmanagement-Lösung verwaltet werden, z. B. Versionierung von Konfigurationen,
- Vorgaben für die Netztrennung,
- Vorgaben für die Zugriffskontrolle,
- Vorgaben für die Protokollierung,
- Vorgaben für die Qualitätssicherung beim Einsatz von Automatisierungsfunktionen, z. B. Skripte,
- Vorgaben für den Schutz der Kommunikation,
- die operativen Grundregeln des Systemmanagements sowie
- Vorgaben für die Abstimmung mit dem Netzmanagement, z. B. Vergabe von IP-Adressen oder DNS-Namen.

OPS.1.1.7.A8 Erstellung eines Systemmanagement-Konzepts (S)

Ausgehend von der Sicherheitsrichtlinie für das Systemmanagement SOLLTE ein Systemmanagement-Konzept erstellt und kontinuierlich gepflegt werden. Dabei SOLLTEN mindestens folgende Aspekte bedarfsgerecht berücksichtigt werden:

- Methoden, Techniken und Werkzeuge für das Systemmanagement,
- Absicherung des Zugangs und der Kommunikation,

- Absicherung auf Ebene des Netzes, insbesondere Zuordnung von Systemmanagement-Komponenten zu Sicherheitszonen,
- Umfang des Monitorings und der Alarmierung für jedes zu verwaltende System,
- Protokollierung,
- Automatisierung, insbesondere die zentrale Verteilung von Konfigurationsdateien auf die zu verwaltenden Systeme,
- Vorgaben an Entwicklung und Test von Automatisierungsfunktionen,
- Meldeketten bei Störungen und Sicherheitsvorfällen,
- Bereitstellung von Systemmanagement-Informationen für andere Betriebsbereiche,
- Einbindung des Systemmanagements in die Notfallplanung, sowie
- benötigten Netzübertragungskapazitäten der Systemmanagement-Lösung.

OPS.1.1.7.A9 Fein- und Umsetzungsplanung für das Systemmanagement (S)

Eine Fein- und Umsetzungsplanung für die Systemmanagement-Lösung SOLLTE erstellt werden. Dabei SOLLTEN alle in der Sicherheitsrichtlinie und im Systemmanagement-Konzept adressierten Punkte berücksichtigt werden.

OPS.1.1.7.A10 Konzept für den sicheren Betrieb der Systemmanagement-Lösung (S)

Ausgehend von den Sicherheitsrichtlinien und dem Systemmanagement-Konzept SOLLTE ein Konzept für den sicheren Betrieb der Systemmanagement-Lösung und der zugrundeliegenden Infrastruktur erstellt werden.

Auch SOLLTE geprüft werden, wie sich die Leistungen anderer operativer Einheiten einbinden und steuern lassen.

OPS.1.1.7.A11 Regelmäßiger Soll-Ist-Vergleich im Rahmen des Systemmanagements (S)

Der IT-Betrieb SOLLTE regelmäßig überprüfen, inwieweit die von der Systemmanagement-Lösung verwalteten Daten, Konfigurationen und Skripte dem Sollzustand entsprechen. Mindestens folgende Aspekte SOLLTEN im Soll-Ist-Vergleich geprüft werden:

- die Konfiguration der Systemmanagement-Lösung,
- die Konfiguration der zu verwaltenden Systeme sowie
- die eingesetzten Automatisierungsfunktionen oder Skripte.

Dabei SOLLTE geprüft werden, ob die genannten Aspekte noch die Sicherheitsrichtlinie und Anforderungsspezifikation erfüllen. Weiter SOLLTE verglichen werden, ob die Softwareversion der Systemmanagement-Lösung aktuell ist.

OPS.1.1.7.A12 Auslösung von Aktionen durch die zentralen Komponenten der Systemmanagement-Lösung (S)

Aktionen, die durch das Systemmanagement auf den verwalteten Systemen ausgeführt werden, SOLLTEN ausschließlich von der Systemmanagement-Lösung ausgelöst werden. Dafür SOLLTEN nur diejenigen Management-Funktionen auf der Systemmanagement-Lösung und den zu verwaltenden Systemen aktiviert werden, die tatsächlich benötigt werden.

OPS.1.1.7.A13 Verpflichtung zur Nutzung der vorgesehenen Schnittstellen für das Systemmanagement (S)

Management-Zugriffe auf zu verwaltende Systeme SOLLTEN ausschließlich über die dafür vorgesehenen Schnittstellen der Systemmanagement-Lösung erfolgen. Falls ein direkter Zugriff auf zu verwaltende Systeme notwendig ist, z. B. nach einem Ausfall eines zu verwaltenden Systems, SOLLTEN sowohl der direkte Zugriff als auch alle in diesem Rahmen vorgenommenen Änderungen dokumentiert und im notwendigen Umfang in die Systemmanagement-Lösung eingepflegt werden.

OPS.1.1.7.A14 Zentrale Konfigurationsverwaltung für zu verwaltende Systeme (S)

Software und Konfigurationsdaten für die zu verwaltenden Systeme SOLLTEN konsequent in einem Konfigurationsmanagement verwaltet werden, das eine Versionierung und Änderungsverfolgung ermöglicht. Die zugehörige Dokumentation zur Konfigurationsverwaltung SOLLTE vollständig und immer aktuell sein. Die benötigten Dokumentationen SOLLTEN an zentraler Stelle sicher verfügbar sein sowie in die Datensicherung eingebunden werden. Die zentrale Konfigurationsverwaltung SOLLTE nachhaltig gepflegt und regelmäßig auditiert werden.

Sämtliche Schnittstellen zwischen Systemmanagement-Lösung und anderen Anwendungen und Diensten SOLLTEN dokumentiert und vollständig in einem Konfigurationsmanagement verwaltet werden. Zwischen relevanten Betriebsbereichen SOLLTEN funktionale Änderungen an den Schnittstellen frühzeitig abgestimmt und dokumentiert werden.

Die Konfigurationsdaten für die zu verwaltenden Systeme SOLLTEN automatisch über das Netz verteilt und ohne Betriebsunterbrechung installiert und aktiviert werden können.

OPS.1.1.7.A15 Statusüberwachung, Protokollierung und Alarmierung bei relevanten Ereignissen in der Systemmanagement-Lösung und den zu verwaltenden Systemen (S)

Die grundlegenden Performance- und Verfügbarkeitsparameter der Systemmanagement-Lösung und der zu verwaltenden Systeme SOLLTEN kontinuierlich überwacht werden. Dafür SOLLTEN vorab die jeweiligen Schwellwerte ermittelt werden (Baselining). Werden definierte Schwellwerte überschritten, SOLLTE das zuständige Personal automatisch benachrichtigt werden.

Zur besseren Fehleranalyse SOLLTEN Informationen aus der Statusüberwachung anderer Bereiche, z. B. aus einem eigenen Bereich „Netze“, ebenfalls betrachtet werden, um die genaue Ursache für eine Störung zu finden.

Wichtige Ereignisse auf zu verwaltenden Systemen und auf der Systemmanagement-Lösung SOLLTEN automatisch an eine zentrale Protokollierungsinfrastruktur übermittelt und dort protokolliert werden (siehe OPS.1.1.5 *Protokollierung*).

Wichtige Ereignisse SOLLTEN mindestens für folgende Aspekte definiert werden:

- Ausfall sowie Nichterreichbarkeit von zu verwaltenden Systemen,
- Ausfall sowie Nichterreichbarkeit von Systemmanagement-Komponenten,
- Hardware-Fehlfunktionen,
- Anmeldeversuche an der Systemmanagement-Lösung,
- Anmeldeversuche an zu verwaltenden Systemen,
- kritische Zustände oder Überlastung der Systemmanagement-Lösung sowie
- kritische Zustände oder Überlastung von zu verwaltenden Systemen.

Ereignismeldungen sowie Protokollierungs-Daten SOLLTEN an ein zentrales Logging-System übermittelt werden. Alarmmeldungen SOLLTEN sofort, wenn sie auftreten, übermittelt werden.

OPS.1.1.7.A16 Einbindung des Systemmanagements in die Notfallplanung (S)

Die Systemmanagement-Lösung SOLLTE in die Notfallplanung der Institution eingebunden werden. Dazu SOLLTEN sowohl die Systemmanagement-Lösung als auch die Konfigurationen der zu verwaltenden Systeme gesichert und in die Wiederanlaufpläne integriert sein.

OPS.1.1.7.A17 Kontrolle der Systemmanagement-Kommunikation (S)

Die Kommunikation zwischen den Benutzenden und der Systemmanagement-Lösung sowie zwischen der Systemmanagement-Lösung und den zu verwaltenden IT-Systemen SOLLTE über geeignete Filtertechniken auf unbedingt notwendige Verbindungen eingeschränkt werden.

OPS.1.1.7.A18 Überprüfung des Systemzustands (S)

Die Konsistenz zwischen realem Systemzustand und dem von der Systemmanagement-Lösung angenommenen Zustand SOLLTE regelmäßig geprüft werden. Werden Abweichungen festgestellt, SOLLTE der in der Systemmanagement-Lösung vorgesehene Zustand wiederhergestellt werden.

OPS.1.1.7.A19 Absicherung der Systemmanagement-Kommunikation zwischen der Systemmanagement-Lösung und den zu verwaltenden Systemen (S)

Die Systemmanagement-Kommunikation zwischen der Systemmanagement-Lösung und den zu verwaltenden Systemen SOLLTE grundsätzlich verschlüsselt sein. Die Stärke der verwendeten kryptografischen Verfahren und Schlüssel SOLLTE regelmäßig überprüft und bei Bedarf angepasst werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

OPS.1.1.7.A20 Hochverfügbare Realisierung der Systemmanagement-Lösung (H)

Eine zentrale Systemmanagement-Lösung SOLLTE hochverfügbar betrieben werden. Dazu SOLLTEN die für die Systemmanagement-Lösung eingesetzten Server bzw. Werkzeuge inklusive der Netzanbindungen redundant ausgelegt sein.

OPS.1.1.7.A21 Physische Trennung der zentralen Systemmanagementnetze (H)

Das Managementnetz für das Systemmanagement SOLLTE physisch von den funktionalen, insbesondere produktiven, Netzen getrennt werden.

OPS.1.1.7.A22 Einbindung des Systemmanagements in automatisierte Detektionssysteme (H)

Die Protokollierung von sicherheitsrelevanten Ereignissen des Systemmanagements SOLLTE in ein Security Information and Event Management (SIEM) eingebunden werden. Dabei SOLLTE nachvollziehbar festgelegt werden, welche Ereignisse an das SIEM weitergeleitet werden.

Im Anforderungskatalog zur Auswahl einer Systemmanagement-Lösung SOLLTEN die erforderlichen Schnittstellen und Übergabeformate spezifiziert werden.

Eine Systemmanagement-Lösung SOLLTE mit einem System zur Erkennung sicherheitsrelevanter Schwachstellen automatisiert überwacht werden.

OPS.1.1.7.A23 Standort-übergreifende Zeitsynchronisation für das Systemmanagement (H)

Die Zeitsynchronisation SOLLTE sowohl für die Systemmanagement-Lösung als auch für die zu verwaltenden Systeme über alle Standorte der Institution sichergestellt werden. Dafür SOLLTE eine gemeinsame Referenzzeit benutzt werden.

OPS.1.1.7.A24 Automatisierte Überprüfung von sicherheitsrelevanten Konfigurationen durch geeignete Detektionssysteme (H)

Sicherheitsrelevante Konfigurationen der Systemmanagement-Lösung und der zu verwaltenden Systeme SOLLTEN durch geeignete Detektionssysteme regelmäßig auf Abweichungen vom Sollzustand sowie auf potenzielle Schwachstellen überprüft werden.

OPS.1.1.7.A25 Protokollierung und Reglementierung von Systemmanagement-Sitzungen (H)

Die Sitzungsinhalte, insbesondere die Aktivitäten von Benutzenden auf der Systemmanagement-Lösung sowie sämtliche direkte Zugriffe auf zu verwaltende Systeme, SOLLTEN kontinuierlich durch eine technische Lösung protokolliert und reglementiert werden. Dabei SOLLTEN die Aktivitäten auf Befehlsebene, d. h. manuelle und automatisierte Befehle, kontrolliert und gegebenenfalls unterbunden werden.

Während der Überwachung SOLLTE nicht nur bei konkreten Regelverstößen, sondern auch bei Anomalien im Benutzendenverhalten eine Alarmierung erfolgen.

OPS.1.1.7.A26 Entkopplung von Zugriffen auf die Systemmanagement-Lösung (H)

Jeder administrative Zugriff auf die Systemmanagement-Lösung SOLLTE durch die Nutzung von Sprungservern abgesichert werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Für den Baustein OPS.1.1.7 *Systemmanagement* sind keine weiterführenden Informationen vorhanden.

Bundesamt
für Sicherheit in der
Informationstechnik

OPS.1.2.2 Archivierung

1. Beschreibung

1.1. Einleitung

Die Archivierung spielt im Dokumentenmanagementprozess eine besondere Rolle. Denn es wird einerseits erwartet, dass die digitalen Dokumente bis zum Ablauf einer vorgegebenen Aufbewahrungsfrist verfügbar sind. Andererseits soll ihre Vertraulichkeit und Integrität bewahrt bleiben. Zusätzlich muss der Kontext erhalten werden, damit der jeweilige gespeicherte Vorgang rekonstruierbar ist.

Während der gesamten Dauer der Langzeitspeicherung müssen daher entsprechende Maßnahmen zur Informationserhaltung und, falls erforderlich, Maßnahmen zur Beweiswerterhaltung umgesetzt werden.

Im deutschen informationstechnischen Sprachgebrauch wird mitunter der Begriff „elektronische Archivierung“ synonym zum Begriff „elektronische Langzeitspeicherung“ verwendet. Zur besseren Verständlichkeit wird in diesem Baustein daher allgemein nur von „Archivierung“ oder auch „digitalem Langzeitarchiv“ gesprochen. Ein IT-Verfahren zur Aufbewahrung elektronischer Dokumente wird als „Archivsystem“ bzw. „digitales Archiv“ oder „Langzeitspeicher“ bezeichnet. Die Aufbewahrungsdauer der Dokumente bemisst sich nach den rechtlichen und sonstigen Vorgaben sowie dem Anwendungszweck der Daten.

Der in diesem Baustein verwendete Begriff „Dokumente“ beinhaltet Daten und digitale Dokumente, sofern sie nicht ausdrücklich in anderer Bedeutung gebraucht werden.

Aus rechtlicher Sicht ist der Begriff „Archivierung“ in Deutschland durch die Archivgesetze des Bundes und der Länder konkretisiert und belegt. „Archivierung“ im juristisch korrekten Sinne betrifft allein Unterlagen der öffentlichen Verwaltung. Sie bezieht sich darauf, dass Unterlagen einer Behörde, sobald sie für deren Zwecke nicht mehr benötigt werden, ausgesondert und durch eine zuständige staatliche Einrichtung (Bundesarchiv) auf unbegrenzte Zeit verwahrt werden sollen (vergleiche §§ 1 und 2 BarchG). Diese Art der Archivierung ist von der in diesem Baustein betrachteten zeitlich beschränkten Aufbewahrung zu unterscheiden.

1.2. Zielsetzung

Der Baustein beschreibt, wie digitale Dokumente langfristig, sicher, unveränderbar und wieder reproduzierbar archiviert werden können. Dazu werden Anforderungen definiert, mit denen sich ein Archivsystem sicher planen, umsetzen und betreiben lässt.

Die Aufbewahrung von Papierdokumenten wird in diesem Baustein nicht betrachtet, es werden aber Anforderungen gestellt, wie diese digitalisiert und archiviert werden können.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.1.2.2 *Archivierung* ist auf den Informationsverbund einmal anzuwenden, wenn eine Langzeitarchivierung von elektronischen Dokumenten erfolgt. Dabei kann eine Langzeitarchivierung aufgrund von externen oder internen Vorgaben erforderlich sein oder es ist bereits ein System zur Langzeitarchivierung elektronischer Dokumente im Betrieb.

Der Baustein behandelt nicht die zeitlich unbegrenzte Archivierung im Sinne der Archivgesetze des Bundes und der Länder.

Der vorliegende Baustein beschreibt Sicherheitsmaßnahmen, mit denen elektronische Dokumente für die Langzeitspeicherung im Rahmen von geltenden Aufbewahrungsfristen aufbewahrt und erhalten werden können. Maßnahmen für eine operative Datensicherung werden in diesem Baustein nicht behandelt. Anforderungen dazu werden in CON.3 *Datensicherungskonzept* dargestellt.

Ein digitaler Langzeitspeicher besteht aus einzelnen Komponenten, z. B. einer Datenbank. Wie sich solche Komponenten detailliert sicher betreiben lassen, ist jedoch ebenfalls nicht Thema des vorliegenden Bausteins. Dazu sind zusätzlich die Anforderungen aus den entsprechenden Bausteinen, wie APP.4.3 *Relationale Datenbanken*, SYS.1.1 *Allgemeiner Server* sowie SYS.1.8 *Speicherlösungen*, zu berücksichtigen.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.1.2.2 *Archivierung* von besonderer Bedeutung.

2.1. Überalterung von Archivsystemen

Archivierte Daten sollen typischerweise über einen sehr langen Zeitraum gespeichert bleiben. Während dieses Zeitraums können die zugrundeliegenden technischen Systemkomponenten, Speichermedien und Datenformate aber physisch oder technisch altern und dadurch unbrauchbar werden. Es können sich z. B. im Laufe der Zeit Probleme mit der Kompatibilität der verwendeten Datenformate ergeben.

Wird auf den Alterungsprozess nicht reagiert, ist langfristig damit zu rechnen, dass beispielsweise archivierte Rohdaten nicht mehr von den Archivmedien lesbar sind. Auch können archivierte Daten durch physische Fehler an Archivsystem und -medien verändert werden.

2.2. Unzureichende Ordnungskriterien für Archive

Elektronische Archive können sehr große Datenmengen enthalten. Die einzelnen Datensätze werden dabei nach bestimmten Ordnungskriterien abgelegt, die nach Indexdaten der Geschäftsanwendungen und Indexdaten des Archivsystems unterschieden werden. Werden ungeeignete Ordnungskriterien verwendet, können archivierte Dokumente eventuell nicht mehr oder nur sehr aufwändig recherchiert werden. Auch ist es möglich, dass die Semantik der Dokumente nicht eindeutig bestimmbar ist. Durch eine ungeeignete oder begrenzte Auswahl von Ordnungskriterien könnten auch die Ziele der Aufbewahrung verfehlt werden, z. B. die Nachweisfähigkeit gegenüber Dritten.

2.3. Unbefugte Archivzugriffe aufgrund unzureichender Protokollierung

Unbefugte Archivzugriffe werden üblicherweise mithilfe von Protokolldateien aufgedeckt. Wurde jedoch nicht umfangreich genug protokolliert, könnten solche Zugriffe nicht entdeckt werden. In der Folge könnten Angreifende unbemerkt an die dort gespeicherten Informationen gelangen und sie z. B. kopieren oder verändern.

2.4. Unzulängliche Übertragung von Papierdaten in ein elektronisches Archiv

Wenn Dokumente eingescannt werden, kann dabei das Erscheinungsbild oder die Semantik der aufgenommenen Daten verfälscht werden. Auch können dabei Dokumente verloren gehen. Dadurch können die Informationen im Dokument falsch interpretiert und berechnet werden, z. B. wenn wichtige Teile des Dokuments oder des Dokumentenstapels beim Scannen vergessen werden.

2.5. Unzureichende Erneuerung von kryptografischen Verfahren bei der Archivierung

Kryptografische Verfahren, die z. B. bei Signaturen, Siegeln, Zeitstempeln, technischen Beweisdaten (Evidence Records) oder Verschlüsselungen verwendet werden, müssen regelmäßig an den aktuellen Stand der Technik angepasst werden, damit die Schutzwirkung erhalten bleibt. Geschieht dies nicht, kann beispielsweise aufgrund einer veralteten unsicheren Signatur die Integrität des Dokumentes nicht mehr garantiert werden. Darüber hinaus wird die Datei eventuell nicht als Beweismittel vor Gericht zugelassen, selbst wenn das Dokument noch völlig korrekt ist. Auch geht so die Vertraulichkeit eines verschlüsselten Dokumentes verloren.

2.6. Unzureichende Revisionen der Archivierung

Wenn der Archivierungsprozess zu selten oder zu ungenau überprüft wird, kann dies dazu führen, dass die Fehlfunktionen nicht erkannt werden. Damit kann die Integrität der archivierten Dokumente selbst angezweifelt werden. Hieraus können sich für die Institution rechtliche und wirtschaftliche Nachteile ergeben: So kann unter Umständen eine Datei nicht als Beweismittel vor Gericht zugelassen werden, weil nicht ausgeschlossen werden kann, dass sie manipuliert wurde.

2.7. Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von Archivierung

Bei der Archivierung von elektronischen Dokumenten sind verschiedene rechtliche Rahmenbedingungen zu beachten. Werden diese nicht eingehalten, kann das zivil- oder strafrechtliche Konsequenzen haben, z. B. bei Mindestaufbewahrungsfristen, die sich aus steuerlichen, haushaltsrechtlichen oder sonstigen Gründen ergeben.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.1.2.2 *Archivierung* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Fachverantwortliche
Weitere Zuständigkeiten	Benutzende, IT-Betrieb, Institutionsleitung

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

OPS.1.2.2.A1 Ermittlung von Einflussfaktoren für die elektronische Archivierung (B)

Bevor entschieden wird, welche Verfahren und Produkte für die elektronische Archivierung eingesetzt werden, MÜSSEN die technischen, rechtlichen und organisatorischen Einflussfaktoren ermittelt und dokumentiert werden. Die Ergebnisse MÜSSEN in das Archivierungskonzept einfließen.

OPS.1.2.2.A2 Entwicklung eines Archivierungskonzepts (B)

Es MUSS definiert werden, welche Ziele mit der Archivierung erreicht werden sollen. Hierbei MUSS insbesondere berücksichtigt werden, welche Regularien einzuhalten sind, welche Mitarbeitende zuständig sind und welcher Funktions- und Leistungsumfang angestrebt wird.

Die Ergebnisse MÜSSEN in einem Archivierungskonzept erfasst werden. Die Institutionsleitung MUSS in diesen Prozess einbezogen werden. Das Archivierungskonzept MUSS regelmäßig an die aktuellen Gegebenheiten der Institution angepasst werden.

OPS.1.2.2.A3 Geeignete Aufstellung von Archivsystemen und Lagerung von Archivmedien (B) [IT-Betrieb]

Die IT-Komponenten eines Archivsystems MÜSSEN in gesicherten Räumen aufgestellt werden. Es MUSS sichergestellt sein, dass nur berechtigte Personen die Räume betreten dürfen. Archivspeichermedien MÜSSEN geeignet gelagert werden.

OPS.1.2.2.A4 Konsistente Indizierung von Daten bei der Archivierung (B) [IT-Betrieb, Benutzende]

Alle in einem Archiv abgelegten Daten, Dokumente und Datensätze MÜSSEN eindeutig indiziert werden. Dazu MUSS bereits während der Konzeption festgelegt werden, welche Struktur und welchen Umfang die Indexangaben für ein Archiv haben sollen.

OPS.1.2.2.A5 Regelmäßige Aufbereitung von archivierten Datenbeständen (B) [IT-Betrieb]

Über den gesamten Archivierungszeitraum hinweg MUSS sichergestellt werden, dass

- das verwendete Datenformat von den benutzten Anwendungen verarbeitet werden kann,
- die gespeicherten Daten auch zukünftig lesbar und so reproduzierbar sind, dass Semantik und Beweiskraft beibehalten werden,
- das benutzte Dateisystem auf dem Speichermedium von allen beteiligten Komponenten verarbeitet werden kann,
- die Speichermedien jederzeit technisch einwandfrei gelesen werden können sowie

- die verwendeten kryptografischen Verfahren zur Verschlüsselung und zum Beweiswerterhalt mittels digitaler Signatur, Siegel, Zeitstempel oder technischen Beweisdaten (Evidence Records) dem Stand der Technik entsprechen.

OPS.1.2.2.A6 Schutz der Integrität der Indexdatenbank von Archivsystemen (B) [IT-Betrieb]

Die Integrität der Indexdatenbank MUSS sichergestellt und überprüfbar sein. Außerdem MUSS die Indexdatenbank regelmäßig gesichert werden. Die Datensicherungen MÜSSEN wiederherstellbar sein. Mittlere und große Archive SOLLTEN über redundante Indexdatenbanken verfügen.

OPS.1.2.2.A7 Regelmäßige Datensicherung der System- und Archivdaten (B) [IT-Betrieb]

Alle Archivdaten, die zugehörigen Indexdatenbanken sowie die Systemdaten MÜSSEN regelmäßig gesichert werden (siehe CON.3 *Datensicherungskonzept*).

OPS.1.2.2.A8 Protokollierung der Archivzugriffe (B) [IT-Betrieb]

Alle Zugriffe auf elektronische Archive MÜSSEN protokolliert werden. Dafür SOLLTEN Datum, Uhrzeit, Benutzender, Client und die ausgeführten Aktionen sowie Fehlermeldungen aufgezeichnet werden. Im Archivierungskonzept SOLLTE festgelegt werden, wie lange die Protokolldaten aufbewahrt werden.

Die Protokolldaten der Archivzugriffe SOLLTEN regelmäßig ausgewertet werden. Dabei SOLLTEN die institutionsinternen Vorgaben beachtet werden.

Auch SOLLTE definiert sein, welche Ereignisse welchen Mitarbeitenden angezeigt werden, wie z. B. Systemfehler, Timeouts oder wenn Datensätze kopiert werden. Kritische Ereignisse SOLLTEN sofort nach der Erkennung geprüft und, falls nötig, weiter eskaliert werden.

OPS.1.2.2.A9 Auswahl geeigneter Datenformate für die Archivierung von Dokumenten (B) [IT-Betrieb]

Für die Archivierung MUSS ein geeignetes Datenformat ausgewählt werden. Es MUSS gewährleisten, dass sich Archivdaten sowie ausgewählte Merkmale des ursprünglichen Dokumentmediums langfristig und originalgetreu reproduzieren lassen.

Die Dokumentstruktur des ausgewählten Datenformats MUSS eindeutig interpretierbar und elektronisch verarbeitbar sein. Die Syntax und Semantik der verwendeten Datenformate SOLLTE dokumentiert und von einer Standardisierungsorganisation veröffentlicht sein. Es SOLLTE für eine beweis- und revisionssichere Archivierung ein verlustfreies Bildkompressionsverfahren benutzt werden.

3.2. Standard-Anforderungen

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

OPS.1.2.2.A10 Erstellung einer Richtlinie für die Nutzung von Archivsystemen (S) [IT-Betrieb]

Es SOLLTE sichergestellt werden, dass Mitarbeitende das Archivsystem so benutzen, wie es im Archivierungskonzept vorgesehen ist. Dazu SOLLTE eine Administrations- und eine Benutzungsrichtlinie erstellt werden. Die Administrationsrichtlinie SOLLTE folgende Punkte enthalten:

- Festlegung der Verantwortung für Betrieb und Administration,

- Vereinbarungen über Leistungsparameter beim Betrieb (unter anderem Service Level Agreements),
- Modalitäten der Vergabe von Zutritts- und Zugriffsrechten,
- Modalitäten der Vergabe von Zugangsrechten zu den vom Archiv bereitgestellten Diensten,
- Regelungen zum Umgang mit archivierten Daten und Archivmedien,
- Überwachung des Archivsystems und der Umgebungsbedingungen,
- Regelungen zur Datensicherung,
- Regelungen zur Protokollierung sowie
- Trennung von Produzenten und Konsumenten (OAIS-Modell).

OPS.1.2.2.A11 Einweisung in die Administration und Bedienung des Archivsystems (S) [IT-Betrieb, Benutzende]

Die zuständigen Mitarbeitende des IT-Betriebs und die Benutzenden SOLLTEN für ihren Aufgabenbereich geschult werden.

Die Schulung der Mitarbeitenden des IT-Betriebs SOLLTE folgende Themen umfassen:

- Systemarchitektur und Sicherheitsmechanismen des verwendeten Archivsystems und des darunterliegenden Betriebssystems,
- Installation und Bedienung des Archivsystems und Umgang mit Archivmedien,
- Dokumentation der Administrationstätigkeiten sowie
- Eskalationsprozeduren.

Die Schulung der Benutzende SOLLTE folgende Themen umfassen:

- Umgang mit dem Archivsystem,
- Bedienung des Archivsystems sowie
- rechtliche Rahmenbedingungen der Archivierung.

Die Durchführung der Schulungen sowie die Teilnahme SOLLTEN dokumentiert werden.

OPS.1.2.2.A12 Überwachung der Speicherressourcen von Archivmedien (S) [IT-Betrieb]

Die auf den Archivmedien vorhandene freie Speicherkapazität SOLLTE kontinuierlich überwacht werden. Sobald ein definierter Grenzwert unterschritten wird, MÜSSEN zuständige Mitarbeitende automatisch alarmiert werden. Die Alarmierung SOLLTE rollenbezogen erfolgen. Es MÜSSEN immer ausreichend leere Archivmedien verfügbar sein, um Speicherengpässen schnell vorbeugen zu können.

OPS.1.2.2.A13 Regelmäßige Revision der Archivierungsprozesse (S)

Es SOLLTE regelmäßig überprüft werden, ob die Archivierungsprozesse noch korrekt und ordnungsgemäß funktionieren. Dazu SOLLTE eine Checkliste erstellt werden, die Fragen zu Verantwortlichkeiten, Organisationsprozessen, zum Einsatz der Archivierung, zur Redundanz der Archivdaten, zur Administration und zur technischen Beurteilung des Archivsystems enthält. Die Auditergebnisse SOLLTEN nachvollziehbar dokumentiert und mit dem Soll-Zustand abgeglichen werden. Abweichungen SOLLTE nachgegangen werden.

OPS.1.2.2.A14 Regelmäßige Beobachtung des Marktes für Archivsysteme (S) [IT-Betrieb]

Der Markt für Archivsysteme SOLLTE regelmäßig und systematisch beobachtet werden. Dabei SOLLTEN unter anderem folgende Kriterien beobachtet werden:

- Veränderungen bei Standards,
- Wechsel der Technik bei herstellenden Unternehmen von Hard- und Software,
- veröffentlichte Sicherheitslücken oder Schwachstellen sowie
- der Verlust der Sicherheitseignung bei kryptografischen Algorithmen.

OPS.1.2.2.A15 Regelmäßige Aufbereitung von kryptografisch gesicherten Daten bei der Archivierung (S) [IT-Betrieb]

Es SOLLTE kontinuierlich beobachtet werden, wie sich das Gebiet der Kryptografie entwickelt, um beurteilen zu können, ob ein Algorithmus weiterhin zuverlässig und ausreichend sicher ist (siehe auch OPS.1.2.2.A20 *Geeigneter Einsatz kryptografischer Verfahren bei der Archivierung*).

Archivdaten, die mit kryptografischen Verfahren gesichert wurden, die sich in absehbarer Zeit nicht mehr zur Sicherung eignen werden, SOLLTEN rechtzeitig mit geeigneten Verfahren neu gesichert werden.

OPS.1.2.2.A16 Regelmäßige Erneuerung technischer Archivsystem-Komponenten (S) [IT-Betrieb]

Archivsysteme SOLLTEN über lange Zeiträume auf dem aktuellen technischen Stand gehalten werden. Neue Hard- und Software SOLLTE vor der Installation in einem laufenden Archivsystem ausführlich getestet werden. Wenn neue Komponenten in Betrieb genommen oder neue Dateiformate eingeführt werden, SOLLTE ein Migrationskonzept erstellt werden. Darin SOLLTEN alle Änderungen, Tests und erwarteten Testergebnisse beschrieben sein. Die Konvertierung der einzelnen Daten SOLLTE dokumentiert werden (Transfervermerk).

Wenn Archivdaten in neue Formate konvertiert werden, SOLLTE geprüft werden, ob die Daten aufgrund rechtlicher Anforderungen zusätzlich in ihren ursprünglichen Formaten zu archivieren sind.

OPS.1.2.2.A17 Auswahl eines geeigneten Archivsystems (S) [IT-Betrieb]

Ein neues Archivsystem SOLLTE immer auf Basis der im Archivierungskonzept beschriebenen Vorgaben ausgewählt werden. Es SOLLTE die dort formulierten Anforderungen erfüllen.

OPS.1.2.2.A18 Verwendung geeigneter Archivmedien (S) [IT-Betrieb]

Für die Archivierung SOLLTEN geeignete Medien ausgewählt und benutzt werden. Dabei SOLLTEN folgende Aspekte berücksichtigt werden:

- das zu archivierende Datenvolumen,
- die mittleren Zugriffszeiten sowie
- die mittleren gleichzeitigen Zugriffe auf das Archivsystem.

Ebenfalls SOLLTEN die Archivmedien die Anforderungen an eine Langzeitarchivierung hinsichtlich Revisionssicherheit und Lebensdauer erfüllen.

OPS.1.2.2.A19 Regelmäßige Funktions- und Recoverytests bei der Archivierung (S) [IT-Betrieb]

Für die Archivierung SOLLTEN regelmäßige Funktions- und Recoverytests durchgeführt werden. Die Archivierungsdatenträger SOLLTEN mindestens einmal jährlich daraufhin überprüft werden, ob sie noch lesbar und integer sind. Für die Fehlerbehebung SOLLTEN geeignete Prozesse definiert werden.

Weiterhin SOLLTEN die Hardwarekomponenten des Archivsystems regelmäßig auf ihre einwandfreie Funktion hin geprüft werden. Es SOLLTE regelmäßig geprüft werden, ob alle Archivierungsprozesse fehlerfrei funktionieren.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

OPS.1.2.2.A20 Geeigneter Einsatz kryptografischer Verfahren bei der Archivierung (H) [IT-Betrieb]

Um lange Aufbewahrungsfristen abdecken zu können, SOLLTEN Archivdaten nur mit kryptografischen Verfahren auf Basis aktueller Standards und Normen gesichert werden.

OPS.1.2.2.A21 Übertragung von Papierdaten in elektronische Archive (H)

Werden z. B. Dokumente auf Papier digitalisiert und in ein elektronisches Archiv überführt, SOLLTE sichergestellt werden, dass die digitale Kopie mit dem Originaldokument bildlich und inhaltlich übereinstimmt.

4. Weiterführende Informationen

4.1. Wissenswertes

Die Bundesnetzagentur (BNetzA) listet in ihrer Veröffentlichung „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung: Auflistung geeigneter Algorithmen und Parameter“ als geeignet eingestufte Algorithmen und Parameter auf.

Das Deutsche Institut für Normung e. V. (DIN) definiert in der DIN 31644:2012-04 „Information und Dokumentation - Kriterien für vertrauenswürdige digitale Langzeitarchive“ Kriterien für vertrauenswürdige digitale Langzeitarchive. In der DIN 31647:2015-05 „Information und Dokumentation - Beweiswerterhaltung kryptographisch signierter Dokumente“ werden technische und sicherheitsrelevante Anforderungen an die langfristige Aufbewahrung von digital signierten Dokumenten unter Wahrung der Rechtskraft der digitalen Signatur definiert.

Das BSI hat in seiner technischen Richtlinie „BSI TR-03138 RESISCAN: Ersetzendes Scannen“ die sicherheitsrelevanten technischen und organisatorischen Maßnahmen, die beim ersetzenden Scannen zu berücksichtigen sind, zusammengestellt.

In der technischen Richtlinie „BSI TR-03125 TR-ESOR: Beweiswerterhaltung kryptographisch signierter Dokumente“ nebst seinen Anhängen stellt das BSI einen Leitfaden zur Verfügung, der beschreibt, wie elektronisch signierte Daten und Dokumente über lange Zeiträume, bis zum Ende der Aufbewahrungsfristen, im Sinne eines rechtswirksamen Beweiswerterhalts vertrauenswürdig gespeichert werden können.

Bundesamt
für Sicherheit in der
Informationstechnik

OPS.1.2.4 Telearbeit

1. Beschreibung

1.1. Einleitung

Unter Telearbeit wird jede auf die Informations- und Kommunikationstechnik gestützte Tätigkeit verstanden, die ganz oder teilweise außerhalb der Geschäftsräume und Gebäude der Institution verrichtet wird. Bei der heimbasierten Telearbeit arbeiten die Mitarbeitenden regelmäßig tages- oder stundenweise abwechselnd an ihrem Arbeitsplatz in den Räumlichkeiten der Institution und am häuslichen Arbeitsplatz.

1.2. Zielsetzung

Das Ziel des Bausteins ist der Schutz von Informationen, die während der Telearbeit gespeichert, verarbeitet und übertragen werden. Dazu werden typische Gefährdungen aufgezeigt und spezielle Anforderungen an die sichere Telearbeit definiert.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.1.2.4 *Telearbeit* ist für jeden Telearbeitsplatz anzuwenden.

Dieser Baustein konzentriert sich auf die Form der Telearbeit, die im häuslichen Umfeld durchgeführt wird (heimbasierte Telearbeit). Es wird davon ausgegangen, dass zwischen dem Telearbeitsplatz und der Institution eine sichere Telekommunikationsverbindung besteht, die es ermöglicht, geeignet Informationen auszutauschen und auf Daten auf dem Server der Institution zuzugreifen. Die Anforderungen dieses Bausteins umfassen die folgenden drei Bereiche:

- die Organisation der Telearbeit,
- den Arbeitsplatz-PCs der Mitarbeitenden und
- die Kommunikationsverbindung zwischen Telearbeitsrechnern und Institution.

Sicherheitsanforderungen an die Infrastruktur des Telearbeitsplatzes werden im vorliegenden Baustein nicht berücksichtigt, sondern sind im Baustein INF.8 *Häuslicher Arbeitsplatz* beschrieben. Anforderungen an einen nicht dauerhaft eingerichteten Arbeitsplatz sind im Baustein INF.9 *Mobiler Arbeitsplatz* zu finden.

Detaillierte Empfehlungen, wie die IT-Systeme konfiguriert und abgesichert werden können, werden nicht im Rahmen dieses Bausteins behandelt. Sie sind in SYS.2.1 *Allgemeiner Client* sowie in den betriebssystemspezifischen System-Bausteinen zu finden. Weitere für die Telearbeit relevante

Sicherheitsaspekte, wie z. B. für WLAN, werden in den Bausteinen der Teilschichten NET.2 *Funknetze* oder NET.4 *Telekommunikation* betrachtet.

Sofern Daten, die bei der Telearbeit verändert wurden, nicht unmittelbar auf IT-Systemen der Institution gespeichert werden, muss geregelt werden, wie eine Datensicherung durchgeführt wird. Anforderungen dazu sind im Baustein CON.3 *Datensicherungskonzept* zu finden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.1.2.4 *Telearbeit* von besonderer Bedeutung.

2.1. Fehlende oder unzureichende Regelungen für den Telearbeitsplatz

Die Nutzung eines Telearbeitsplatzes erfordert ergänzende organisatorische Absprachen zwischen den Mitarbeitenden und den Führungskräften. Zudem brauchen sie Handlungsanweisungen für den Fall, dass sicherheitsrelevante Vorkommnisse am Telearbeitsplatz eintreten. Gelangen beispielsweise vertrauliche Informationen in die Hände Dritter, können schwerwiegende Schäden für die Institution entstehen.

2.2. Unerlaubte private Nutzung des dienstlichen Telearbeitsrechners

Im häuslichen Bereich kann leichter nicht geprüfte und nicht freigegebene Hard- oder Software eingesetzt werden und so durch unbedachtes Handeln beispielsweise Schadsoftware auf den Telearbeitsrechner gelangen. Dadurch könnten vertrauliche Informationen kompromittiert werden.

2.3. Verzögerungen durch temporär eingeschränkte Erreichbarkeit der Mitarbeitenden

Haben die Mitarbeitenden keine festen Arbeitszeiten am Telearbeitsplatz und werden keine festen Zeiten vereinbart, an denen sie erreichbar sein müssen, kann aufgrund dessen der Arbeitsablauf verzögert werden.

2.4. Mangelhafte Einbindung der Mitarbeitenden in den Informationsfluss

Da die Mitarbeitenden nicht täglich in der Institution sind, haben sie weniger Gelegenheit, am direkten Informationsaustausch mit den Führungskräften sowie den Kollegen und Kolleginnen teilzuhaben. Es ist daher möglich, dass Telearbeitende insbesondere mündlich weitergegebene Informationen nicht oder erst verzögert erhalten. Hierdurch können Arbeitsabläufe und betriebliche Prozesse gestört und die Produktivität des oder der Mitarbeitenden eingeschränkt werden.

2.5. Nichtbeachtung von Sicherheitsmaßnahmen

Am Telearbeitsplatz können beispielsweise fehlende Kontrollmöglichkeiten dazu führen, dass Mitarbeitende empfohlene oder angeordnete Sicherheitsmaßnahmen nicht oder nicht in vollem Umfang umsetzen. So können z. B. vertrauliche Informationen in die Hände Dritter geraten.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.1.2.4 *Telearbeit* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Informationssicherheitsbeauftragte (ISB)
Weitere Zuständigkeiten	Mitarbeitende, IT-Betrieb, Vorgesetzte, Personalabteilung

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

OPS.1.2.4.A1 Regelungen für Telearbeit (B) [Vorgesetzte, Personalabteilung]

Alle relevanten Aspekte der Telearbeit MÜSSEN geregelt werden. Zu Informationszwecken MÜSSEN den Telearbeitenden die geltenden Regelungen oder ein dafür vorgesehenes Merkblatt ausgehändigt werden, das die zu beachtenden Sicherheitsmaßnahmen erläutert. Alle strittigen Punkte MÜSSEN entweder durch Betriebsvereinbarungen oder durch zusätzlich zum Arbeitsvertrag getroffene individuelle Vereinbarungen zwischen dem Mitarbeitenden und der Institution geregelt werden. Die Regelungen MÜSSEN regelmäßig aktualisiert werden.

OPS.1.2.4.A2 Sicherheitstechnische Anforderungen an den Telearbeitsrechner (B)

Es MÜSSEN sicherheitstechnische Anforderungen festgelegt werden, die ein IT-System für die Telearbeit erfüllen muss.

Es MUSS sichergestellt werden, dass nur autorisierte Personen Zugang zu den Telearbeitsrechnern haben. Darüber hinaus MUSS der Telearbeitsrechner so abgesichert werden, dass er nur für autorisierte Zwecke benutzt werden kann.

OPS.1.2.4.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

OPS.1.2.4.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

OPS.1.2.4.A5 Sensibilisierung und Schulung der Mitarbeitenden (B)

Anhand eines Leitfadens MÜSSEN die Mitarbeitenden für die Gefahren sensibilisiert werden, die mit der Telearbeit verbunden sind. Außerdem MÜSSEN sie in die entsprechenden Sicherheitsmaßnahmen der Institution eingewiesen und im Umgang mit diesen geschult werden. Die Schulungs- und Sensibilisierungsmaßnahmen für Mitarbeitenden SOLLTEN regelmäßig wiederholt werden.

3.2. Standard-Anforderungen

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

OPS.1.2.4.A6 Erstellen eines Sicherheitskonzeptes für Telearbeit (S)

Es SOLLTE ein Sicherheitskonzept für die Telearbeit erstellt werden, das Sicherheitsziele, Schutzbedarf, Sicherheitsanforderungen sowie Risiken beschreibt. Das Konzept SOLLTE regelmäßig aktualisiert und überarbeitet werden. Das Sicherheitskonzept zur Telearbeit SOLLTE auf das übergreifende Sicherheitskonzept der Institution abgestimmt werden.

OPS.1.2.4.A7 Regelung der Nutzung von Kommunikationsmöglichkeiten bei Telearbeit (S) [IT-Betrieb, Mitarbeitende]

Es SOLLTE klar geregelt werden, welche Kommunikationsmöglichkeiten bei der Telearbeit unter welchen Rahmenbedingungen genutzt werden dürfen. Die dienstliche und private Nutzung von Internetdiensten bei der Telearbeit SOLLTE geregelt werden. Dabei SOLLTE auch geklärt werden, ob eine private Nutzung generell erlaubt oder unterbunden wird.

OPS.1.2.4.A8 Informationsfluss zwischen Mitarbeitenden und Institution (S) [Vorgesetzte, Mitarbeitende]

Ein regelmäßiger innerbetrieblicher Informationsaustausch zwischen den Mitarbeitenden und der Institution SOLLTE gewährleistet sein. Alle Mitarbeitenden SOLLTEN zeitnah über geänderte Sicherheitsanforderungen und andere sicherheitsrelevante Aspekte informiert werden. Allen Kollegen und Kolleginnen der jeweiligen Mitarbeitenden SOLLTE bekannt sein, wann und wo diese erreicht werden können. Technische und organisatorische Telearbeitsregelungen zur Aufgabenbewältigung, zu Sicherheitsvorfällen und sonstigen Problemen SOLLTEN geregelt und an die Mitarbeitenden kommuniziert werden.

OPS.1.2.4.A9 Betreuungs- und Wartungskonzept für Telearbeitsplätze (S) [IT-Betrieb, Mitarbeitende]

Für Telearbeitsplätze SOLLTE ein spezielles Betreuungs- und Wartungskonzept erstellt werden. Darin SOLLTEN folgende Aspekte geregelt werden: Kontaktperson des IT-Betriebs, Wartungstermine, Fernwartung, Transport der IT-Geräte und Einführung von Standard-Telearbeitsrechnern. Damit die Mitarbeitenden einsatzfähig bleiben, SOLLTEN für sie Kontaktpersonen für Hard- und Softwareprobleme benannt werden.

OPS.1.2.4.A10 Durchführung einer Anforderungsanalyse für den Telearbeitsplatz (S) [IT-Betrieb]

Bevor ein Telearbeitsplatz eingerichtet wird, SOLLTE eine Anforderungsanalyse durchgeführt werden. Daraus SOLLTE z. B. hervorgehen, welche Hard- und Software-Komponenten für den Telearbeitsplatz benötigt werden. Die Anforderungen an den jeweiligen Telearbeitsplatz SOLLTEN mit den IT-Verantwortlichen abgestimmt werden. Es SOLLTE immer festgestellt und dokumentiert werden, welchen Schutzbedarf die am Telearbeitsplatz verarbeiteten Informationen haben.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Für diesen Baustein sind keine Anforderungen für einen erhöhten Schutzbedarf definiert.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013, insbesondere in Annex A, A.6.2.1 „Mobile device policy“ und A.11.2.6 „Security of equipment and assets off-premises“, Informationen zum Umgang mit Telearbeit.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“, insbesondere in Area PA2 Mobile Computing, ebenfalls Vorgaben zur Telearbeit.

Das National Institute of Standards and Technology (NIST) hat im Rahmen seiner Special Publications die NIST Special Publication 800-46 als „Guide to Enterprise Telework, Remote Access and Bring Your Own Device (BYOD) Security“ veröffentlicht.

Bundesamt
für Sicherheit in der
Informationstechnik

OPS.1.2.5 Fernwartung

1. Beschreibung

1.1. Einleitung

Mit dem Begriff Fernwartung wird ein zeitlich begrenzter Zugriff auf IT-Systeme und die darauf laufenden Anwendungen bezeichnet, der von einem anderen IT-System aus erfolgt. Der Zugriff kann z. B. dazu dienen, Konfigurations-, Wartungs- oder Reparaturarbeiten durchzuführen.

Die Fernwartung kann auf unterschiedliche Weise geschehen. Bei der Fernwartung von Clients werden oft die Tastatur- und Maussignale von IT-Systemen von den Administrierenden an ein entferntes IT-System übertragen. Das entfernte IT-System überträgt die Bildschirmausgabe an das IT-System der Administrierenden. Die Administrierenden führen Aktionen auf dem entfernten IT-System so aus, als wenn sie selbst vor Ort wären (aktive Fernwartung). Bei der Fernwartung von Servern wird oft die Ein- und Ausgabe der Konsole übertragen.

Bei der passiven Fernwartung werden nur die Bildschirminhalte eines IT-Systems zu den Administrierenden übertragen. Administrierende erteilen den Benutzenden vor Ort Anweisungen, die von ihnen ausgeführt und von den Administrierenden beobachtet werden. Allerdings erweist sich dieses Vorgehen in der Praxis meist als sehr zeitintensiv und umständlich, weshalb häufig dem IT-Betrieb voller Zugriff über das IT-System zugewiesen wird.

Da sich viele IT-Systeme außerhalb der Reichweite ihrer Administrierenden befinden (z. B. in entfernten Rechenzentren, Industrieanlagen oder einem Außenstandort ohne IT-Personal), wird Fernwartung in vielen Institutionen eingesetzt. Bei der Fernwartung wird oft über unsichere Netze auf interne IT-Systeme und Anwendungen einer Institution zugegriffen. Wegen der dabei bestehenden tiefgreifenden Eingriffsmöglichkeiten in diese IT-Systeme und Anwendungen ist die Absicherung von Fernwartungskomponenten von besonderer Bedeutung.

1.2. Zielsetzung

Ziel dieses Bausteins ist der Schutz der Informationen, die bei der Fernwartung gespeichert, verarbeitet und übertragen werden sowie der Schutz der Fernwartungsschnittstellen von IT-Systemen. Zu diesem Zweck werden Anforderungen an die Fernwartung gestellt, die sich gleichermaßen auf Funktionen der aktiven und passiven Fernwartung beziehen.

1.3. Abgrenzung und Modellierung

Der Baustein ist auf alle Zielobjekte im Informationsverbund anzuwenden, bei denen Fernwartung genutzt wird.

Dieser Baustein betrachtet die Fernwartung überwiegend aus der Sicht des IT-Betriebs und gibt Hinweise für Administrierende, wie Fernwartung eingesetzt werden kann. Die Sicherheitsaspekte der eingesetzten Kommunikationsverbindungen und Authentisierungsmechanismen sowie die Absicherung der Fernwartungszugänge sind wichtige Bestandteile dieses Bausteins. Dennoch werden darin nicht alle relevanten Aspekte der mit einer Fernwartung in Verbindung stehenden Geschäftsprozesse abgedeckt. Vor allem die Bausteine OPS.1.1.3 *Patch- und Änderungsmanagement*, ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit*, CON.1 *Kryptokonzept* und CON.3 *Datensicherungskonzept* sind zusätzlich zu beachten. Ebenso sind die Vorgaben der Bausteinschicht NET *Netze und Kommunikation* umzusetzen, sofern diese direkt mit der Fernwartung in Verbindung stehen.

Wird die Fernwartung von externen Dienstleistenden durchgeführt, muss zudem der Baustein OPS.2.3 *Nutzung von Outsourcing* beachtet werden. Werden cloudbasierte Fernwartungsprodukte verwendet, müssen auch die allgemeinen Anforderungen aus dem Baustein OPS.2.2 *Cloud-Nutzung* erfüllt werden.

Anforderungen zur Absicherung der Fernwartung mittels Firewalls sind nicht Bestandteil dieses Bausteins. Anforderungen dazu sind im Baustein NET.3.2 *Firewall* zu finden.

Grundsätzliche Aspekte der IT-Administration werden ebenfalls nicht in diesem Baustein betrachtet. Sie sind im Baustein OPS.1.1.2 *Ordnungsgemäße IT-Administration* zu finden. Ebenfalls nicht betrachtet werden Anforderungen des Systemmanagements. Diese sind im Baustein OPS.1.1.7 *Systemmanagement* zu finden.

Nicht im Fokus des Bausteins steht die Fernwartung im industriellen Umfeld. Anforderungen dazu sind im Baustein IND.3.2 *Fernwartung im industriellen Umfeld* zu finden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.1.2.5 *Fernwartung* von besonderer Bedeutung.

2.1. Unzureichende Kenntnisse über Regelungen der Fernwartung

Administrierende, die Fernwartung einrichten und nutzen, sind auf Regelungen angewiesen, die festlegen, wie Fernwartung verwendet werden soll. Beispielsweise ist es notwendig festzulegen, wie Anwendungen zur Fernwartung konfiguriert werden sollen. Ansonsten können mit der Fernwartung zusätzliche Risiken für das interne Netz entstehen. Werden den Beteiligten die Regelungen zur Fernwartung nicht mitgeteilt, ergeben sich Gefahren für den IT-Betrieb. Beispielsweise könnte eine Fernwartungsschnittstelle eingerichtet und dabei ein Authentisierungsverfahren mit unsicherem Passwort erlaubt werden, anstelle eines sicheren, zertifikatbasierten Verfahrens.

2.2. Fehlende oder unzureichende Planung und Regelung der Fernwartung

Wird die Fernwartung nicht sorgfältig geplant, aufgebaut und geregelt, kann die Sicherheit aller IT-Systeme einer Institution beeinträchtigt werden. Werden beispielsweise unsichere Kommunikationsprotokolle, Verschlüsselungsalgorithmen oder Authentisierungsmechanismen eingesetzt, können Sicherheitslücken entstehen. Über unzureichend gesicherte Fernwartungsschnittstellen kann auch ein gekoppeltes Netz eines Dritten kompromittiert werden.

2.3. Ungeeignete Nutzung von Authentisierung bei der Fernwartung

Bei der Fernwartung können unterschiedliche Authentisierungsmechanismen verwendet werden. Wird ein unsicheres Authentisierungsverfahren genutzt, können unberechtigte Dritte administrative Berechtigungen auf Fernwartungssystemen oder für Fernwartungswerkzeuge erlangen. Dadurch können sie auf die IT-Systeme einer Institution zugreifen und weitreichende Schäden verursachen.

Ein Beispiel hierfür ist ein Anmeldeverfahren, das nur ein kurzes Passwort verwendet. Bei einem Angriff kann dieses Passwort in kurzer Zeit erraten und sich so Zugriff auf IT-Systeme der Institution verschafft werden.

2.4. Fehlerhafte Fernwartung

Damit die Sicherheit und Funktionsfähigkeit von IT-Systemen und Anwendungen, auf die nur aus der Ferne zugegriffen werden kann, gewährleistet wird, ist eine professionelle und regelmäßige Fernwartung erforderlich. Werden solche IT-Systeme und Anwendungen nicht ordnungsgemäß per Fernwartung konfiguriert und gewartet, können sie im schlimmsten Fall nicht mehr genutzt werden. Laufen die Fernwartungsprozesse nicht korrekt ab, kann dies zu Fehlfunktionen einzelner Betriebssystemkomponenten führen. Außerdem können durch verspätete oder fehlerhafte IT-Systemwartungen Sicherheitslücken entstehen.

2.5. Verwendung unsicherer Protokolle in der Fernwartung

Die Kommunikation über öffentliche und interne Netze mittels unsicherer Protokolle stellt eine potenzielle Gefahr dar. Werden z. B. veraltete Versionen von IPSec, SSH oder SSL/TLS eingesetzt, um einen Tunnel zwischen zwei Netzen oder Endpunkten herzustellen, kann nicht gewährleistet werden, dass dieser Tunnel ausreichend sicher ist und die darin übertragenen Informationen angemessen geschützt sind. Bei einem Angriff können Schwachstellen dieser Protokolle ausgenutzt werden, um in geschützte Verbindungen eigene Inhalte einzuschleusen. Generell als unsicher gelten Protokolle, bei denen Informationen im Klartext übertragen werden.

2.6. Fehlende Regelungen zur Fremdnutzung der Fernwartungszugänge

Werden IT-Systeme von Dritten ferngewartet, ohne dass es dafür eine vertragliche Grundlage gibt, sind die Zuständigkeiten für die Fernwartung möglicherweise nicht klar geregelt. Dadurch können z. B. Rollentrennungen umgangen werden oder offene Fernwartungszugänge werden nicht dokumentiert.

2.7. Nutzung von Online-Diensten für die Fernwartung

Neben einer Fernwartung, bei der eine direkte Datenverbindung zu der betreffenden Institution aufgebaut wird, können auch Online-Dienste genutzt werden. Hierbei verbinden sich die zu administrierenden IT-Systeme mit den Servern von Online-Diensten und die Administrierenden können z. B. über einen Webbrowser auf die zu administrierenden IT-Systeme zugreifen.

Falls die Kommunikation nicht Ende-zu-Ende verschlüsselt wird, könnten die Online-Dienste den Datenaustausch mitlesen. Zusätzlich könnten auch die IT-Systeme durch unberechtigte Personen administriert werden, indem die Datenverbindung verändert wird. Bauen die IT-Systeme automatisch beim Systemstart eine Datenverbindung zum Online-Dienst auf, könnte direkt auf das IT-System zugegriffen werden, ohne dass dies den Benutzenden des IT-Systems oder den zuständigen Administrierenden bekannt ist.

2.8. Unbekannte Fernwartungskomponenten

Viele IT-Systeme enthalten Komponenten, die integrierte Funktionen zur Fernwartung bieten. Oft sind diese Funktionen aber schlecht dokumentiert und werden bei der Beschaffung sowie beim Betrieb von IT-Systemen nicht berücksichtigt.

Integrierte Fernwartungskomponenten haben weitreichenden Zugriff auf die IT-Systeme, in denen sie verbaut sind. Dieser Zugriff wirkt dabei oft direkt auf andere Komponenten des IT-Systems und kann so die Sicherheitsmechanismen des Betriebssystems umgehen. Zusätzlich können integrierte Fernwartungsfunktionen Schwachstellen enthalten, die einen unberechtigten Zugriff auf das IT-System vereinfachen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.1.2.5 *Fernwartung* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Benutzende

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

OPS.1.2.5.A1 Planung des Einsatzes der Fernwartung (B)

Der Einsatz der Fernwartung MUSS an die Institution angepasst werden. Die Fernwartung MUSS hinsichtlich technischer und organisatorischer Aspekte bedarfsgerecht geplant werden. Dabei MUSS mindestens berücksichtigt werden, welche IT-Systeme ferngewartet werden sollen und wer dafür zuständig ist.

OPS.1.2.5.A2 Sicherer Verbindungsaufbau bei der Fernwartung von Clients (B) [Benutzende]

Wird per Fernwartung auf Desktop-Umgebungen von Clients zugegriffen, MUSS die Fernwartungssoftware so konfiguriert sein, dass sie eine Verbindung erst nach expliziter Zustimmung der Benutzenden aufbaut.

OPS.1.2.5.A3 Absicherung der Schnittstellen zur Fernwartung (B)

Die möglichen Zugänge und Kommunikationsverbindungen für die Fernwartung MÜSSEN auf das notwendige Maß beschränkt werden. Alle Fernwartungsverbindungen MÜSSEN nach dem Fernzugriff getrennt werden.

Es MUSS sichergestellt werden, dass Fernwartungssoftware nur auf IT-Systemen installiert ist, auf denen sie benötigt wird.

Fernwartungsverbindungen über nicht vertrauenswürdige Netze MÜSSEN verschlüsselt werden. Alle anderen Fernwartungsverbindungen SOLLTEN verschlüsselt werden.

OPS.1.2.5.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

3.2. Standard-Anforderungen

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

OPS.1.2.5.A5 Einsatz von Online-Diensten (S)

Die Institution SOLLTE festlegen, unter welchen Umständen Online-Dienste zur Fernwartung genutzt werden dürfen, bei denen die Verbindung über einen externen Server hergestellt wird. Der Einsatz solcher Dienste SOLLTE generell auf möglichst wenige Fälle beschränkt werden. Die IT-Systeme SOLLTEN keine automatisierten Verbindungen zum Online-Dienst aufbauen. Es SOLLTE sichergestellt werden, dass der eingesetzte Online-Dienst die übertragenen Informationen Ende-zu-Ende-verschlüsselt.

OPS.1.2.5.A6 Erstellung einer Richtlinie für die Fernwartung (S)

Die Institution SOLLTE eine Richtlinie zur Fernwartung erstellen, in der alle relevanten Regelungen zur Fernwartung dokumentiert werden. Die Richtlinie SOLLTE allen Zuständigen bekannt sein, die an der Konzeption, dem Aufbau und dem Betrieb der Fernwartung beteiligt sind.

OPS.1.2.5.A7 Dokumentation bei der Fernwartung (S)

Die Fernwartung SOLLTE geeignet dokumentiert werden. Aus der Dokumentation SOLLTE hervorgehen, welche Fernwartungszugänge existieren und ob diese aktiviert sind. Die Dokumente SOLLTEN an geeigneten Orten und vor unberechtigtem Zugriff geschützt abgelegt werden. Die Dokumente SOLLTEN im Rahmen des Notfallmanagements zur Verfügung stehen.

OPS.1.2.5.A8 Sichere Protokolle bei der Fernwartung (S)

Nur als sicher eingestufte Kommunikationsprotokolle SOLLTEN eingesetzt werden. Dafür SOLLTEN sichere kryptografische Verfahren verwendet werden. Die Stärke der verwendeten kryptografischen Verfahren und Schlüssel SOLLTE regelmäßig überprüft und bei Bedarf angepasst werden.

Wird auf die Fernwartungszugänge von IT-Systemen im internen Netz über ein öffentliches Datennetz zugegriffen, SOLLTE ein abgesichertes Virtuelles Privates Netz (VPN) genutzt werden.

OPS.1.2.5.A9 Auswahl und Beschaffung geeigneter Fernwartungswerkzeuge (S)

Die Auswahl geeigneter Fernwartungswerkzeuge SOLLTE sich aus den betrieblichen, sicherheitstechnischen und datenschutzrechtlichen Anforderungen der Institution ergeben. Alle Beschaffungsentscheidungen SOLLTEN mit den System- und Anwendungsverantwortlichen sowie dem oder der Informationssicherheitsbeauftragten abgestimmt werden.

OPS.1.2.5.A10 Umgang mit Fernwartungswerkzeugen (S)

Es SOLLTEN organisatorische Verwaltungsprozesse zum Umgang mit den ausgewählten Fernwartungswerkzeugen etabliert werden. Es SOLLTE eine Bedienungsanleitung für den Umgang mit den Fernwartungswerkzeugen vorliegen. Ergänzend zu den allgemeinen Schulungsmaßnahmen SOLLTEN Musterabläufe für die passive und die aktive Fernwartung erstellt und kommuniziert werden. Zusätzlich zu den allgemeinen Schulungsmaßnahmen SOLLTE der IT-Betrieb besonders im Umgang mit den Fernwartungswerkzeugen sensibilisiert und geschult werden. Es SOLLTE ein Ansprechpartner oder eine Ansprechpartnerin für alle fachlichen Fragen zu den Fernwartungswerkzeugen benannt werden.

OPS.1.2.5.A11 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.2.5.A12 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.2.5.A13 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.2.5.A15 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.2.5.A16 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.2.5.A17 Authentisierungsmechanismen bei der Fernwartung (S)

Für die Fernwartung SOLLTEN Mehr-Faktor-Verfahren zur Authentisierung eingesetzt werden. Die Auswahl der Authentisierungsmethode und die Gründe, die zu der Auswahl geführt haben, SOLLTEN dokumentiert werden. Fernwartungszugänge SOLLTEN im Identitäts- und Berechtigungsmanagement der Institution berücksichtigt werden.

OPS.1.2.5.A18 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.2.5.A19 Fernwartung durch Dritte (S)

Wird die Fernwartung von Externen durchgeführt, SOLLTEN alle Fernwartungsaktivitäten von internen Mitarbeitenden beobachtet werden. Alle Fernwartungsvorgänge durch Dritte SOLLTEN aufgezeichnet werden.

Mit externem Wartungspersonal MÜSSEN vertragliche Regelungen über die Sicherheit der betroffenen IT-Systeme und Informationen geschlossen werden. Die Pflichten und Kompetenzen des externen Wartungspersonals SOLLTEN in den vertraglichen Regelungen festgehalten werden.

Sollten Dienstleistende mehrere Kunden und Kundinnen fernwarten, MUSS gewährleistet sein, dass die Netze der Kunden und Kundinnen nicht miteinander verbunden werden. Die Fernwartungsschnittstellen SOLLTEN so konfiguriert sein, dass es Dienstleistenden nur möglich ist, auf die IT-Systeme und Netzsegmente zuzugreifen, die für seine Arbeit benötigt werden.

OPS.1.2.5.A20 Betrieb der Fernwartung (S)

Ein Meldeprozess für Support- und Fernwartungsanliegen SOLLTE etabliert werden.

Es SOLLTEN Mechanismen zur Erkennung und Abwehr von hochvolumigen Angriffen, TCP-State-Exhaustion-Angriffen und Angriffen auf Applikationsebene implementiert sein.

Alle Fernwartungsvorgänge SOLLTEN protokolliert werden.

OPS.1.2.5.A21 Erstellung eines Notfallplans für den Ausfall der Fernwartung (S)

Es SOLLTE ein Konzept entwickelt werden, wie die Folgen eines Ausfalls von Fernwartungskomponenten minimiert werden können. Dieses SOLLTE festhalten, wie im Falle eines Ausfalls zu reagieren ist. Durch den Notfallplan SOLLTE sichergestellt sein, dass Störungen, Schäden und Folgeschäden minimiert werden. Außerdem SOLLTE festgelegt werden, wie eine zeitnahe Wiederherstellung des Normalbetriebs erfolgen kann.

OPS.1.2.5.A24 Absicherung integrierter Fernwartungssysteme (S)

Bei der Beschaffung von neuen IT-Systemen SOLLTE geprüft werden, ob diese IT-Systeme oder einzelne Komponenten der IT-Systeme über Funktionen zur Fernwartung verfügen. Werden diese Funktionen nicht verwendet, SOLLTEN sie deaktiviert werden. Die Funktionen SOLLTEN ebenfalls deaktiviert werden, wenn sie durch bekannte Sicherheitslücken gefährdet sind.

Werden Fernwartungsfunktionen verwendet, die in die Firmware einzelner Komponenten integriert sind, SOLLTEN deren Funktionen und der Zugriff darauf so weit wie möglich eingeschränkt werden. Die Fernwartungsfunktionen SOLLTEN nur aus einem getrennten Managementnetz erreichbar sein.

OPS.1.2.5.A25 Entkopplung der Kommunikation bei der Fernwartung (S)

Direkte Fernwartungszugriffe von einem Fernwartungs-Client außerhalb der Managementnetze auf ein IT-System SOLLTEN vermieden werden. Ist ein solcher Zugriff notwendig, SOLLTE die Kommunikation entkoppelt werden. Dazu SOLLTEN Sprungserver verwendet werden. Der Zugriff auf Sprungserver SOLLTE nur von vertrauenswürdigen IT-Systemen aus möglich sein.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

OPS.1.2.5.A14 Dedizierte Clients und Konten bei der Fernwartung (H)

Zur Fernwartung SOLLTEN IT-Systeme eingesetzt werden, die ausschließlich zur Administration von anderen IT-Systemen dienen. Alle weiteren Funktionen auf diesen IT-Systemen SOLLTEN deaktiviert werden. Die Netzkommunikation der Administrationssysteme SOLLTE so eingeschränkt werden, dass nur Verbindungen zu IT-Systemen möglich sind, die administriert werden sollen.

Für Fernwartungszugänge SOLLTEN dedizierte Konten verwendet werden.

OPS.1.2.5.A22 Redundante Kommunikationsverbindungen (H)

Für Fernwartungszugänge SOLLTEN redundante Kommunikationsverbindungen eingerichtet werden. Die Institution SOLLTE Anbindungen zum Out-Of-Band-Management vorhalten.

OPS.1.2.5.A23 ENTFALLEN (H)

Diese Anforderung ist entfallen.

4. Weiterführende Informationen

4.1. Wissenswertes

Das Bundesamt für Sicherheit in der Informationstechnik beschreibt in seiner Veröffentlichung „Grundregeln zur Absicherung von Fernwartungszugängen“, wie Fernwartungszugänge sicher betrieben werden können.

Das Bundesamt für Sicherheit in der Informationstechnik beschreibt in seiner Veröffentlichung „Fernwartung im industriellen Umfeld“ wie Fernwartungszugänge im Industrieumfeld sicher betrieben werden können.

Bundesamt
für Sicherheit in der
Informationstechnik

OPS.1.2.6 NTP-Zeitsynchronisation

1. Beschreibung

1.1. Einleitung

Vernetzte IT-Systeme erfordern oftmals synchrone Zustände. Meist dient die Uhrzeit als Referenz. Die interne Uhr von IT-Systemen kann jedoch von der tatsächlichen Zeit abweichen. Das Network Time Protocol (NTP) wird dazu verwendet, regelmäßig eine Referenzzeit zentraler Zeitgeber über Netzverbindungen zu ermitteln und die interne Uhr entsprechend anzupassen.

In Netzen erlaubt eine genaue Zeitsynchronisation Informationen mit einheitlichen Zeitstempeln zu versehen, z. B. um Daten chronologisch zu ordnen, Daten miteinander abzugleichen oder Zugriffsrechte zu befristen. Nur so lassen sich beispielsweise zeitliche Abläufe aus Protokolldaten verschiedener IT-Systeme miteinander in Beziehung bringen. Auch im Bereich der kryptographischen Protokolle sind genaue Zeitinformationen von Bedeutung. Darüber hinaus ist es in OT-Netzen essenziell, sämtliche Zeitgeber genau zu synchronisieren.

NTP-Clients beziehen Zeitinformationen von NTP-Servern. Die NTP-Server können wiederum als NTP-Clients Zeitinformationen von anderen NTP-Servern beziehen. So entsteht eine hierarchische Zeitverteilung (in sogenannte "Strata"). An der Spitze stehen NTP-Server, die ihre Zeit von genauen Quellen (z. B. einer Atomuhr, einem GPS- oder einem DCF77-Empfänger) beziehen. Diese NTP-Server werden als Stratum-1 bezeichnet.

Der NTP-Dienst nutzt Verfahren, um auch bei abweichenden Antworten verschiedener Zeitquellen die Abweichung der Systemuhr zu externen Zeitquellen zu bestimmen. Beispielsweise ignoriert er Zeitangaben einer Zeitquelle, die plötzlich gravierend von der eigenen Systemzeit abweicht.

Steuerungsnachrichten (Control Messages) erlauben es Clients, Statusinformationen abzufragen oder das Verhalten des NTP-Servers auch über das Netz hinweg zu ändern.

NTP-Nachrichten werden meistens ungesichert übertragen. NTP bietet jedoch die Möglichkeit, eine Nachricht mit kryptografischen Schlüsseln zu schützen, damit die Nachricht nicht unberechtigt verändert werden kann.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, NTP-Server und -Clients so abzusichern, dass die IT-Systeme im Informationsverbund verlässlich die Zeit ermitteln und ihre Uhren justieren können.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.1.2.6 *NTP-Zeitsynchronisation* ist auf jedes IT-System des Informationsverbundes anzuwenden, das NTP nutzt.

Um ein IT-Grundschutz-Modell für einen konkreten Informationsverbund zu erstellen, muss grundsätzlich die Gesamtheit aller Bausteine betrachtet werden. In der Regel sind mehrere Bausteine auf das Thema bzw. Zielobjekt anzuwenden.

Dieser Baustein behandelt

- die Planung zum Einsatz des NTP-Protokolls,
- den Betrieb von NTP-Servern sowie
- den Betrieb von NTP-Clients.

Folgende Inhalte sind ebenfalls von Bedeutung und werden an anderer Stelle behandelt:

- Allgemeine Anforderungen an den Betrieb von Servern (siehe SYS.1.1 *Allgemeiner Server*)
- Allgemeine Anforderungen an den Betrieb von Clients (siehe SYS.2.1 *Allgemeiner Client*)

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.1.2.6 *NTP-Zeitsynchronisation* von besonderer Bedeutung.

2.1. Unzureichende Planung des Einsatzes von NTP

Unzureichende Planung kann dazu führen, dass nicht alle IT-Systeme eine ausreichend genaue Systemzeit erhalten.

Wenn nicht richtig geplant wird, wie IT-Systeme ihre Systemzeit justieren können, dann können fehlerhafte Zeitinformationen in Anwendungen entstehen. Insbesondere zeitkritische Anwendungen können in der Folge fehlerhafte Zustände aufweisen oder ausfallen.

Beispielsweise kann ein Netz so segmentiert werden, dass NTP-Server und -Clients nicht mehr miteinander kommunizieren können. Zudem kann die unzureichende Planung der Zeitsynchronisation z. B. dazu führen, dass automatisierte Prozesse zu einem falschen Zeitpunkt ausgeführt werden.

2.2. Keine oder fehlerhafte Zeitinformationen

NTP-Server können ausfallen oder falsche Zeitinformationen übermitteln.

Wenn ein IT-System seine NTP-Server nicht mehr erreichen kann, weil diese ausgefallen oder nicht erreichbar sind, dann kann es seine Systemzeit nicht mehr justieren. Dadurch kann die Zeit der internen Uhr ungenau werden.

Falls ein NTP-Server fehlerhafte Zeitinformationen an NTP-Clients übermittelt, justieren diese möglicherweise ihre Systemuhr falsch. Dadurch können fehlerhafte Zeitinformationen in Anwendungen genutzt werden, beispielsweise in Protokolldaten.

Falsche Zeitinformationen können ebenfalls dazu führen, dass zertifikatsbasierte Dienste oder Dienste, die Einmalpasswörter verwenden, nicht mehr funktionieren. Infolgedessen können sich die Benutzenden nicht mehr auf IT-Systemen oder bei Netzdiensten anmelden.

2.3. Widersprüchliche Zeitinformationen

Zeitinformationen verschiedener Quellen können sich widersprechen.

Falls ein IT-System mehrere NTP-Server verwendet, um seine Systemuhr zu justieren, dann können die Zeitinformationen der verschiedenen NTP-Server unterschiedlich sein. Sobald die Zeitinformationen untolerierbar stark voneinander abweichen, kann das IT-System möglicherweise nicht mehr bestimmen, welche der Zeitinformationen die richtige ist. Dadurch kann die Systemzeit falsch justiert werden.

2.4. Manipulation der NTP-Kommunikation

Netzpakete mit Zeitinformationen können manipuliert werden.

Das NTP-Protokoll ist für verschiedene Angriffe anfällig. Bei einem Angriff können beispielsweise die Zeitinformationen manipuliert werden, während sie übertragen werden, oder NTP-Anfragen können zu einem anderen Server umgeleitet werden. So kann bei einem Angriff die Systemzeit der NTP-Clients manipuliert werden, um beispielsweise zeitlich beschränkte Zugriffsrechte zu nutzen, obwohl sie abgelaufen sind.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.1.2.6 *NTP-Zeitsynchronisation* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Keine

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

OPS.1.2.6.A1 Planung des NTP- Einsatzes (B)

Der IT-Betrieb MUSS planen, wo und wie NTP eingesetzt wird. Dies SOLLTE vollständig dokumentiert werden. Dabei MUSS ermittelt werden, welche Anwendungen auf eine genaue Zeitinformation angewiesen sind. Die Anforderungen des Informationsverbunds hinsichtlich genauer Zeit der IT-Systeme MÜSSEN definiert und dokumentiert werden.

Der IT-Betrieb MUSS definieren, welche NTP-Server von welchen NTP-Clients genutzt werden sollen.

Es MUSS festgelegt werden, ob NTP-Server im Client-Server- oder im Broadcast-Modus arbeiten.

OPS.1.2.6.A2 Sichere Nutzung fremder Zeitquellen (B)

Falls Zeitinformationen von einem NTP-Server außerhalb des Netzes der Institution bezogen werden, dann MUSS der IT-Betrieb beurteilen, ob der NTP-Server hinreichend verlässlich ist. Der IT-Betrieb

MUSS sicherstellen, dass nur als verlässlich eingestufte NTP-Server verwendet werden. Der IT-Betrieb MUSS die Nutzungsregeln des NTP-Servers kennen und beachten.

OPS.1.2.6.A3 Sichere Konfiguration von NTP-Servern (B)

Der IT-Betrieb MUSS den NTP-Server so konfigurieren, dass Clients nur dann Einstellungen des NTP-Servers verändern können, wenn dies explizit vorgesehen ist. Darüber hinaus MUSS sichergestellt werden, dass nur vertrauenswürdige Clients Status-Informationen abfragen können.

Falls die internen NTP-Server der Institution nicht selbst hinreichend genaue Zeitquellen nutzen, dann MUSS der IT-Betrieb diese NTP-Server so konfigurieren, dass sie regelmäßig genaue Zeitinformationen von externen NTP-Servern abfragen.

OPS.1.2.6.A4 Nichtberücksichtigung unaufgeforderter Zeitinformationen (B)

Der IT-Betrieb MUSS alle NTP-Clients so konfigurieren, dass sie Zeitinformationen verwerfen, die sie unaufgefordert von anderen IT-Systemen erhalten.

3.2. Standard-Anforderungen

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

OPS.1.2.6.A5 Nutzung des Client-Server-Modus für NTP (S)

Der IT-Betrieb SOLLTE alle IT-Systeme so konfigurieren, dass sie den NTP-Dienst im Client-Server-Modus nutzen. NTP-Server SOLLTEN Zeitinformationen nur dann an Clients versenden, wenn diese aktiv anfragen.

OPS.1.2.6.A6 Überwachung von IT-Systemen mit NTP-Nutzung (S)

Der IT-Betrieb SOLLTE die Verfügbarkeit, die Kapazität und die Systemzeit der internen NTP-Server überwachen.

Der IT-Betrieb SOLLTE IT-Systeme, die ihre Zeit per NTP synchronisieren, so konfigurieren, dass sie folgende Ereignisse protokollieren:

- unerwartete Neustarts des IT-Systems,
- unerwartete Neustarts des NTP-Dienstes,
- Fehler im Zusammenhang mit dem NTP-Dienst sowie
- ungewöhnliche Zeitinformationen.

Falls der NTP-Server von sich aus regelmäßig Zeitinformationen versendet (Broadcast-Modus), dann SOLLTE der IT-Betrieb die NTP-Clients daraufhin überwachen, ob sie ungewöhnliche Zeitinformationen erhalten.

OPS.1.2.6.A7 Sichere Konfiguration von NTP-Clients (S)

Der IT-Betrieb SOLLTE festlegen, welche Zeitinformationen ein IT-System verwenden soll, wenn es neu gestartet wurde. Der IT-Betrieb SOLLTE festlegen, welche Zeitinformationen ein IT-System verwenden soll, wenn sein NTP-Dienst neu gestartet wurde.

Der IT-Betrieb SOLLTE festlegen, wie NTP-Clients auf stark abweichende Zeitinformationen reagieren. Insbesondere SOLLTE entschieden werden, ob stark abweichende Zeitinformationen von NTP-Servern nach einem Systemneustart akzeptiert werden. Der IT-Betrieb SOLLTE Grenzwerte für stark abweichende Zeitinformationen festlegen.

Der IT-Betrieb SOLLTE sicherstellen, dass NTP-Clients auch dann noch ausreichende Zeitinformationen erhalten, wenn sie von einem NTP-Server aufgefordert werden, weniger oder gar keine Anfragen zu senden.

OPS.1.2.6.A8 Einsatz sicherer Protokolle zur Zeitsynchronisation (S)

Der IT-Betrieb SOLLTE prüfen, ob sichere Protokolle zur Zeitsynchronisation eingesetzt werden können (z. B. Network Time Security (NTS)). Falls dies möglich ist, SOLLTEN sichere Protokolle eingesetzt werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

OPS.1.2.6.A9 Verfügbarkeit ausreichend vieler genauer Zeitquellen (H)

Falls korrekte Systemzeiten von erheblicher Bedeutung sind, dann SOLLTE eine Institution über mehrere Stratum-1-NTP-Server in ihrem Netz verfügen. Die IT-Systeme des Informationsverbunds mit NTP-Dienst SOLLTEN die Stratum-1-NTP-Server direkt oder indirekt als Zeitreferenz nutzen. Die Straum-1-Server SOLLTEN jeweils über verschiedene Zeitquellen verfügen.

OPS.1.2.6.A10 Ausschließlich interne NTP-Server (H)

Jedes IT-System des Informationsverbunds mit NTP-Dienst SOLLTE Zeitinformationen ausschließlich von NTP-Servern innerhalb des Netzes der Institution beziehen.

OPS.1.2.6.A11 Redundante NTP-Server (H)

IT-Systeme, bei denen die Genauigkeit der Systemzeit von erheblicher Bedeutung ist, SOLLTEN Zeitinformationen von mindestens vier unabhängigen NTP-Servern beziehen.

OPS.1.2.6.A12 NTP-Server mit authentifizierten Auskünften (H)

NTP-Server SOLLTEN sich bei der Kommunikation gegenüber Clients authentisieren. Dies SOLLTE auch für die Server gelten, von denen der NTP-Server seinerseits Zeitinformationen erhält. Die NTP-Clients SOLLTEN nur authentifizierte NTP-Daten akzeptieren.

4. Weiterführende Informationen

4.1. Wissenswertes

Für den Baustein OPS.1.2.6 *NTP-Zeitsynchronisation* sind keine weiterführenden Informationen vorhanden.

Bundesamt
für Sicherheit in der
Informationstechnik

OPS.2.2 Cloud-Nutzung

1. Beschreibung

1.1. Einleitung

Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software.

Cloud Computing bietet viele Vorteile: Die IT-Dienste können bedarfsgerecht, skalierbar und flexibel genutzt und je nach Funktionsumfang, Nutzungsdauer und Anzahl der Benutzenden abgerechnet werden. Auch kann auf spezialisierte Kenntnisse und Ressourcen der Cloud-Diensteanbietenden zugegriffen werden, wodurch interne Ressourcen für andere Aufgaben freigesetzt werden können. In der Praxis zeigt sich jedoch häufig, dass sich die Vorteile, die Institutionen von der Cloud-Nutzung erwarten, nicht vollständig auswirken. Die Ursache dafür ist meistens, dass wichtige kritische Erfolgsfaktoren im Vorfeld der Cloud-Nutzung nicht ausreichend betrachtet werden. Daher müssen Cloud-Dienste strategisch geplant sowie (Sicherheits-)Anforderungen, Verantwortlichkeiten und Schnittstellen sorgfältig definiert und vereinbart werden. Auch das Bewusstsein und Verständnis für die notwendigerweise geänderten Rollen, sowohl auf Seiten des IT-Betriebs als auch der Benutzenden der auftraggebenden Institution, ist ein wichtiger Erfolgsfaktor.

Zusätzlich sollte bei der Einführung von Cloud-Diensten auch das Thema Governance berücksichtigt werden (Cloud Governance). Kritische Bereiche sind beispielsweise die Vertragsgestaltung, die Umsetzung von Mandantenfähigkeit, die Sicherstellung von Portabilität unterschiedlicher Services, die Abrechnung genutzter Service-Leistungen, das Monitoring der Service-Erbringung, das Sicherheitsvorfallmanagement und zahlreiche Datenschutzaspekte.

1.2. Zielsetzung

Der Baustein beschreibt Anforderungen, durch die sich Cloud-Dienste sicher nutzen lassen. Er richtet sich an alle Institutionen, die solche Dienste bereits nutzen oder sie zukünftig einsetzen wollen.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.2.2 *Cloud-Nutzung* ist immer auf eine konkrete Cloud-Dienstleistung anzuwenden. Nutzt eine Institution unterschiedliche Cloud-Diensteanbietende, so ist der Baustein für alle Cloud-

Diensteanbietenden anzuwenden. Die Schnittstelle zwischen den Cloud-Diensteanbietenden ist ebenfalls Gegenstand des Bausteins und muss für alle Cloud-Dienstleistungen betrachtet werden.

In nahezu allen Bereitstellungsmodellen, abgesehen von der Nutzung einer Private Cloud On-Premise, stellen Cloud-Dienste eine Sonderform des Outsourcings (siehe Baustein OPS.2.3 *Nutzung von Outsourcing*) dar. Die im vorliegenden Baustein beschriebenen Gefährdungen und Anforderungen werden daher häufig auch im Outsourcing angewendet. Bei Cloud-Diensten gibt es jedoch einige Besonderheiten, die sich ausschließlich in diesem Baustein wiederfinden. Der Baustein OPS.2.3 *Nutzung von Outsourcing* ist daher nicht auf Cloud-Dienste anzuwenden.

Die in diesem Baustein beschriebenen Gefährdungen und Anforderungen gelten dabei grundsätzlich unabhängig vom genutzten Service- und Bereitstellungsmodell.

Sicherheitsanforderungen, mit denen Anbietende ihre Cloud-Dienste schützen können, sind nicht Gegenstand dieses Bausteins. Gefährdungen und spezifische Sicherheitsanforderungen, die durch die Anbindung eines Cloud-Dienstes über entsprechende Schnittstellen (englisch API, Application Programming Interface) als relevant anzusehen sind, werden ebenfalls nicht in diesem Baustein betrachtet.

Abgrenzung zum klassischen IT-Outsourcing

Beim Outsourcing werden Arbeits-, Produktions- oder Geschäftsprozesse einer Institution ganz oder teilweise zu externen Dienstleistenden ausgelagert. Dies ist ein etablierter Bestandteil heutiger Organisationsstrategien. Das klassische IT-Outsourcing ist meist so gestaltet, dass die komplette gemietete Infrastruktur exklusiv von einem Kunden oder einer Kundin genutzt wird (Single Tenant Architektur), auch wenn Anbietende von Outsourcing normalerweise mehrere Kunden oder Kundinnen haben. Zudem werden Outsourcing-Verträge meistens über längere Laufzeiten abgeschlossen.

Die Nutzung von Cloud-Diensten gleicht in vielen Punkten dem klassischen Outsourcing, aber es kommen noch einige Unterschiede hinzu, die zu berücksichtigen sind:

- Aus wirtschaftlichen Gründen teilen sich oft in einer Cloud mehrere Anwendende eine gemeinsame Infrastruktur.
- Cloud-Dienste sind dynamisch und dadurch innerhalb viel kürzerer Zeiträume nach oben und unten skalierbar. So können Cloud-basierte Angebote rascher an den tatsächlichen Bedarf der Anwendenden angepasst werden.
- Die in Anspruch genommenen Cloud-Dienste werden in der Regel mittels einer Webschnittstelle durch die Cloud-Anwendenden selbst gesteuert. So können sie automatisiert die genutzten Dienste auf ihre Bedürfnisse zuschneiden.
- Durch die beim Cloud Computing genutzten Techniken ist es möglich, die IT-Leistung dynamisch über mehrere Standorte zu verteilen, die geographisch sowohl im In- als auch im Ausland weit verstreut sein können.
- Die Anwendenden können die genutzten Dienste und ihre Ressourcen einfach über Web-Oberflächen oder passende Schnittstellen administrieren, wobei wenig Interaktion mit den Cloud-Diensteanbietenden erforderlich ist.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.2.2 *Cloud-Nutzung* von besonderer Bedeutung.

2.1. Fehlende oder unzureichende Strategie für die Cloud-Nutzung

Cloud-Dienste in einer Institution einzusetzen, ist eine strategische Entscheidung. Durch eine fehlende oder unzureichende Strategie für die Cloud-Nutzung ist es z. B. möglich, dass sich eine Institution für ungeeignete Cloud-Dienste oder Cloud-Diensteanbietende entscheidet. Auch könnten die ausgewählten Cloud-Dienste mit der eigenen IT, den internen Geschäftsprozessen oder dem Schutzbedarf nicht kompatibel sein. Dies kann sich organisatorisch, technisch oder auch finanziell negativ auf die Geschäftsprozesse auswirken. Generell kann eine fehlende oder unzureichende Strategie für die Cloud-Nutzung dazu führen, dass die damit verbundenen Ziele nicht erreicht werden oder das Sicherheitsniveau signifikant sinkt.

2.2. Abhängigkeit von Cloud-Diensteanbietenden (Kontrollverlust)

Nutzt eine Institution externe Cloud-Dienste, ist sie mehr oder weniger stark von den Cloud-Diensteanbietenden abhängig. Dadurch kann es passieren, dass die Institution die ausgelagerten Geschäftsprozesse und die damit verbundenen Informationen nicht mehr vollständig kontrollieren kann, insbesondere deren Sicherheit. Auch ist die Institution trotz möglicher Kontrollen ab einem gewissen Punkt darauf angewiesen, dass die Cloud-Diensteanbietenden Sicherheitsmaßnahmen auch korrekt umsetzen. Machen sie das nicht, sind Geschäftsprozesse und geschäftskritische Informationen unzureichend geschützt.

Zudem kann die Nutzung externer Cloud-Dienste dazu führen, dass in der Institution Know-how über Informationssicherheit und -technik verloren geht. Dadurch kann die Institution unter Umständen gar nicht mehr beurteilen, ob die von Anbietenden ergriffenen Schutzmaßnahmen ausreichend sind. Auch ein Wechsel der Cloud-Dienstleistung ist so nur noch sehr schwer möglich. Die Cloud-Diensteanbietenden könnten diese Abhängigkeit zum Beispiel auch ausnutzen, um Preiserhöhungen durchzusetzen oder die Dienstleistungsqualität zu senken.

2.3. Mangelhaftes Anforderungsmanagement bei der Cloud-Nutzung

Wenn sich eine Institution dafür entscheidet, einen Cloud-Dienst zu nutzen, sind daran in der Regel viele Erwartungen geknüpft. So erhoffen sich Mitarbeitende beispielsweise eine höhere Leistungsfähigkeit oder einen größeren Funktionsumfang der ausgelagerten Dienste, während die Institutionsleitung auf geringere Kosten spekuliert. Ein mangelndes Anforderungsmanagement vor der Cloud-Nutzung kann jedoch dazu führen, dass die Erwartungen nicht erfüllt werden und der Dienst nicht den gewünschten Mehrwert, z. B. hinsichtlich der Verfügbarkeit, liefert.

2.4. Verstoß gegen rechtliche Vorgaben

Viele Anbietende bieten ihre Cloud-Dienste in einem internationalen Umfeld an. Damit unterliegen sie oft anderen nationalen Gesetzgebungen. Häufig sieht die Cloud-Kundschaft nur die mit dem Cloud Computing verbundenen Vorteile (z. B. Kostenvorteile) und schätzt die rechtlichen Rahmenbedingungen falsch ein, wie z. B. Datenschutz, Informationspflichten, Insolvenzrecht, Haftung oder Informationszugriff für Dritte. Dadurch könnten geltende Richtlinien und Vorgaben verletzt werden. Auch die Sicherheit der ausgelagerten Informationen könnte beeinträchtigt werden.

2.5. Fehlende Mandantenfähigkeit bei Cloud-Diensteanbietenden

Beim Cloud Computing teilen sich meistens verschiedene Institutionen eine gemeinsame Infrastruktur, wie z. B. IT-Systeme, Netze und Anwendungen. Werden beispielsweise die Ressourcen der verschiedenen Institutionen nicht ausreichend sicher voneinander getrennt, kann eine Institution

eventuell auf die Bereiche einer anderen Institution zugreifen und dort Informationen manipulieren oder löschen.

2.6. Unzulängliche vertragliche Regelungen mit Cloud-Diensteanbietenden

Aufgrund von unzulänglichen vertraglichen Regelungen mit Cloud-Diensteanbietenden können vielfältige und auch schwerwiegende Sicherheitsprobleme auftreten. Wenn Verantwortungsbereiche, Aufgaben, Leistungsparameter oder Aufwände ungenügend oder missverständlich beschrieben wurden, kann es passieren, dass die Cloud-Diensteanbietenden unbeabsichtigt oder aufgrund fehlender Ressourcen Sicherheitsmaßnahmen nicht oder nur ungenügend umsetzen.

Auch wenn Situationen eintreten, die nicht eindeutig vertraglich geregelt sind, können Nachteile für die auftraggebende Institution daraus resultieren. So nutzen Cloud-Diensteanbietende für ihre Services häufig die Dienste Dritter. Bestehen hier unzureichende vertragliche Vereinbarungen oder wurden die Abhängigkeiten zwischen den Dienstleistenden und Dritten nicht offengelegt, kann sich dies auch negativ auf die Informationssicherheit und die Serviceleistung der Institution auswirken.

2.7. Mangelnde Planung der Migration zu Cloud-Diensten

Die Migration zu einem Cloud-Dienst ist fast immer eine kritische Phase. Durch mangelhafte Planungen können Fehler auftreten, die sich auf die Informationssicherheit innerhalb der Institution auswirken. Verzichtet eine Institution beispielsweise durch eine ungenügende Planungsphase leichtfertig auf eine stufenweise Migration, kann dies in der Praxis zu erheblichen Problemen führen. Gibt es im Vorfeld etwa keine Testphasen, Pilot-Benutzenden oder einen zeitlich begrenzten Parallelbetrieb von bestehender Infrastruktur und Cloud-Diensten, können wichtige Daten verloren gehen oder Dienste komplett ausfallen.

2.8. Unzureichende Einbindung von Cloud-Diensten in die eigene IT

Es ist erforderlich, dass Cloud-Dienste angemessen in die IT-Infrastruktur der Institution eingebunden werden. Setzen die Zuständigen dies nur unzureichend um, kann es passieren, dass die Benutzenden die beauftragten Cloud-Dienstleistungen nicht in vollem Umfang abrufen können. Die Cloud-Dienste liefern so eventuell nicht die erforderliche und vereinbarte Leistung oder auf sie kann gar nicht oder nur eingeschränkt zugegriffen werden. Dadurch können Geschäftsprozesse verlangsamt werden oder ganz ausfallen. Werden Cloud-Dienste falsch in die eigene IT eingebunden, können auch schwerwiegende Sicherheitslücken entstehen.

2.9. Unzureichende Regelungen für das Ende eines Cloud-Nutzungs-Vorhabens

Unzureichende Regelungen für eine mögliche Kündigung des Vertragsverhältnisses können gravierende Folgen für die Institution haben. Das ist erfahrungsgemäß immer dann besonders problematisch, wenn ein aus Sicht der Institution kritischer Fall unerwartet eintritt, wie beispielsweise die Insolvenz, der Verkauf der Cloud-Diensteanbietenden oder schwerwiegende Sicherheitsbedenken. Ohne eine ausreichende interne Vorsorge sowie genaue Vertragsregelungen kann sich die Institution nur schwer aus dem für die Cloud-Dienstleistung abgeschlossenen Vertrag lösen. In diesem Fall ist es schwierig bis unmöglich, den ausgelagerten Cloud-Dienst zeitnah beispielsweise auf eine andere Cloud-Computing-Plattform zu übertragen oder ihn wieder in die eigene Institution einzugliedern.

Auch kann eine unzureichend geregelte Datenlöschung nach Vertragsende dazu führen, dass unberechtigt auf die Informationen der Institution zugegriffen wird.

2.10. Unzureichendes Administrationsmodell für die Cloud-Nutzung

Werden Cloud-Dienste genutzt, verändert sich häufig das Rollenverständnis innerhalb des IT-Betriebs auf Seiten der nutzenden Institution. So entwickeln sich Administrierende oft weg von der klassischen Systemadministration hin zu Service-Administration. Wird dieser Prozess nicht ausreichend begleitet, kann sich dies negativ auf die Cloud-Nutzung auswirken, etwa, wenn die Administrierenden nicht das nötige Verständnis für die Umstellungen mitbringen oder sie für ihre neue Aufgabe nicht oder nur unzureichend geschult sind. In der Folge sind eventuell die Cloud-Dienste nicht ordnungsgemäß administriert und so nur noch eingeschränkt verfügbar oder sie fallen ganz aus.

2.11. Unzureichendes Notfallvorsorgekonzept

Eine unzureichende Notfallvorsorge hat bei der Cloud-Nutzung schnell gravierende Folgen. Wenn der Cloud-Dienst oder Teile hiervon ausfallen, führen Versäumnisse bei den Notfallvorsorgekonzepten bei Cloud-Diensteanbietenden sowie bei den Schnittstellen immer zu unnötig langen Ausfallzeiten mit entsprechenden Folgen für die Produktivität bzw. Dienstleistung der auftraggebenden Institution. Daneben können mangelhaft abgestimmte Notfallszenarien zwischen auftraggebender Institution und Dienstleistenden zu Lücken in der Notfallvorsorge führen.

2.12. Ausfall der IT-Systeme der Cloud-Diensteanbietenden

Bei Cloud-Diensteanbietenden können die dort betriebenen Prozesse, IT-Systeme und Anwendungen teilweise oder ganz ausfallen, wovon folglich auch die Cloud-Kundschaft betroffen ist. Werden die Institutionen unzureichend voneinander getrennt, kann auch ein ausgefallenes IT-System, das nicht der Institution zugeordnet ist, dazu führen, dass diese Institution ihre vertraglich zugesicherte Dienstleistung nicht mehr abrufen kann. Ähnliche Probleme ergeben sich, wenn die Anbindung zwischen Cloud-Diensteanbietenden und -Kundschaft 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. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

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

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

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

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 Cloud-Diensteanbietenden 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 (B) [Fachverantwortliche]

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 die Cloud-Diensteanbietenden sowie das festgelegte Schutzniveau für Cloud-Dienste hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit dokumentiert werden. Wenn Cloud-Dienste von internationalen Anbietenden genutzt werden, MÜSSEN die speziellen länderspezifischen Anforderungen und gesetzlichen Bestimmungen berücksichtigt werden.

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

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

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

Basierend auf der Service-Definition für Cloud-Dienste MÜSSEN alle relevanten Schnittstellen und Verantwortlichkeiten für die Cloud-Nutzung identifiziert und dokumentiert werden. Es MUSS klar erkennbar sein, wie die Verantwortungsbereiche zwischen Cloud-Diensteanbietenden und der auftraggebenden Institution voneinander abgegrenzt sind.

3.2. Standard-Anforderungen

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

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

Bevor zu einem Cloud-Dienst migriert wird, SOLLTE 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 Zuständigen ermitteln, ob die Mitarbeitenden auf Seiten 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 ein Sicherheitskonzept für die Nutzung von Cloud-Diensten erstellt werden.

OPS.2.2.A8 Sorgfältige Auswahl von Cloud-Diensteanbietenden (S) [Institutionsleitung]

Basierend auf der Service-Definition für den Cloud-Dienst SOLLTE ein detailliertes Anforderungsprofil für Cloud-Diensteanbietende erstellt werden. Eine Leistungsbeschreibung und ein Lastenheft SOLLTEN erstellt werden. Für die Bewertung von Cloud-Diensteanbietenden SOLLTEN auch ergänzende Informationsquellen herangezogen werden. Ebenso SOLLTEN verfügbare Service-Beschreibungen der Cloud-Diensteanbietenden sorgfältig geprüft und hinterfragt werden.

OPS.2.2.A9 Vertragsgestaltung mit den Cloud-Diensteanbietenden (S) [Institutionsleitung]

Die vertraglichen Regelungen zwischen der auftraggebenden Institution und den Cloud-Diensteanbietenden 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 die Cloud-Diensteanbietenden ihre Leistung erbringen. Zusätzlich SOLLTEN Eskalationsstufen und Kommunikationswege zwischen der Institution und den Cloud-Diensteanbietenden definiert werden. Auch SOLLTE vereinbart werden, wie die Daten der Institution sicher zu löschen sind. Ebenso SOLLTEN Kündigungsregelungen schriftlich fixiert werden. Die Cloud-Diensteanbietenden SOLLTEN alle Subunternehmen offenlegen, die sie für den Cloud-Dienst benötigen.

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

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 die Cloud-Diensteanbietenden die definierten Anforderungen der Institution erfüllen.

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

Für die genutzten Cloud-Dienste SOLLTE ein Notfallkonzept erstellt werden. Es SOLLTE alle notwendigen Angaben zu Zuständigkeiten und Kontaktpersonen 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 regelmäßig aktualisiert werden. Es SOLLTE außerdem periodisch kontrolliert werden, ob die

vertraglich zugesicherten Leistungen erbracht werden. Auch SOLLTEN sich die Cloud-Diensteanbietenden und die Institution 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)

Die Institution SOLLTE sich von den Cloud-Diensteanbietenden 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). Die Institution SOLLTE prüfen, ob der Geltungsbereich und Schutzbedarf die genutzten Cloud-Dienste erfasst.

Nutzen Cloud-Diensteanbietende Subunternehmen, um die Cloud-Dienste zu erbringen, SOLLTEN Cloud-Diensteanbietende der Institution regelmäßig nachweisen, dass diese Subunternehmen die notwendigen Audits durchführen.

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

Wenn das Dienstleistungsverhältnis mit den Cloud-Diensteanbietenden beendet wird, SOLLTE sichergestellt sein, dass dadurch die Geschäftstätigkeit oder die Fachaufgaben der Institution nicht beeinträchtigt wird. Die Verträge mit den Cloud-Diensteanbietenden SOLLTEN regeln, wie das jeweilige Dienstleistungsverhältnis geordnet aufgelöst werden kann.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

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

Die Institution SOLLTE alle Anforderungen definieren, die es ermöglichen, Cloud-Diensteanbietende zu wechseln oder den Cloud-Dienst bzw. die Daten in die eigene IT-Infrastruktur zurückzuholen. Zudem SOLLTE die Institution regelmäßig Portabilitätstests durchführen. In den Verträgen mit den Cloud-Diensteanbietenden SOLLTEN Vorgaben festgehalten werden, mit denen sich die notwendige Portabilität gewährleisten lässt.

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

Die Institution SOLLTE prüfen, ob, zusätzlich zu den vertraglich festgelegten Datensicherungen der Cloud-Diensteanbietenden, eigene Datensicherungen erstellt werden sollen. Zudem SOLLTE sie detaillierte Anforderungen an einen Backup-Service erstellen.

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

Wenn Daten durch Cloud-Diensteanbietende 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 (H) [Fachverantwortliche]

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 die Cloud-Diensteanbietenden übertragen werden. Die Berechtigungen SOLLTEN regelmäßig überprüft werden, sodass nur berechtigten Benutzenden ein SAML-Ticket ausgestellt wird.

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

Mit externen Cloud-Diensteanbietenden 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 Publikation „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 Information 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.

Bundesamt
für Sicherheit in der
Informationstechnik

OPS.2.3 Nutzung von Outsourcing

1. Beschreibung

1.1. Einleitung

Beim Outsourcing lagern Institutionen (Nutzende von Outsourcing) Geschäftsprozesse oder Tätigkeiten ganz oder teilweise zu einem oder mehreren externen Dienstleistungsunternehmen (Anbietende von Outsourcing) aus. Diese sogenannten Anbietenden von Outsourcing betreiben im Rahmen des vereinbarten Outsourcing-Verhältnisses die Geschäftsprozesse oder Tätigkeiten nach festgelegten Kriterien. Allerdings verbleibt die Verantwortung aus Sicht der Informationssicherheit stets bei der auslagernden Institution.

Outsourcing kann die Nutzung und den Betrieb von Hard- und Software betreffen, wobei die Leistung in den Räumlichkeiten der Auftraggebenden oder in einer externen Betriebsstätte der Anbietenden von Outsourcing erbracht werden kann. Typische Beispiele des klassischen "IT-Outsourcings", worauf sich dieser Baustein bezieht, sind der Betrieb eines Rechenzentrums, einer Applikation oder einer Webseite. Outsourcing ist ein Oberbegriff, der oftmals durch weitere Begriffe konkretisiert wird, wie Hosting, Housing oder Colocation.

Ein Outsourcing-Verhältnis betrifft neben den ursprünglichen Nutzenden und Anbietenden von Outsourcing in vielen Fällen weitere, den Anbietenden von Outsourcing nachgelagerte, Sub-Dienstleistende. Werden Teile von Geschäftsprozessen oder Tätigkeiten von Anbietenden von Outsourcing weiter an Sub-Dienstleistende verlagert, so werden die von Nutzenden ausgelagerten Geschäftsprozesse oder Tätigkeiten weiter fragmentiert. Dies wirkt sich auf die Komplexität der Outsourcing-Kette aus, woraus eine schwindende Transparenz für die Nutzenden von Outsourcing folgt. Der Nachweis, dass die an die Anbietenden von Outsourcing gestellten Anforderungen erfüllt werden, erstreckt sich hierbei sowohl auf die Anbietenden von Outsourcing als auch auf die Sub-Dienstleistenden.

Zur besseren Verständlichkeit wird in diesem Baustein der Begriff "Prozess" stellvertretend für Geschäftsprozess, Tätigkeit oder Komponente verwendet, die ausgelagert wird.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, die Grundwerte der Informationssicherheit Vertraulichkeit, Integrität und Verfügbarkeit über den gesamten Lebenszyklus des Outsourcings durch die Nutzenden von Outsourcing sicherzustellen. Mit Outsourcing ist dabei das klassische "IT-Outsourcing" gemeint.

Die Anforderungen des Bausteins OPS.2.3 *Nutzung von Outsourcing* sollen dazu beitragen, dass potenzielle Gefährdungen für den Geschäftsbetrieb erkannt, vorgebeugt und vermindert werden.

Risiken für eine Institution sollen hierdurch in einem für die Institution kontrollierbaren Rahmen bleiben. Dies kann durch mehr Transparenz und Steuerungsinstrumenten erreicht werden. Dazu wird die Institution in ihrer Planung, Durchführung und Kontrolle des Outsourcing-Prozesses über den gesamten Lebenszyklus hinsichtlich technischen und nicht-technischen Aspekten der Informationssicherheit unterstützt.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.2.3 *Nutzung von Outsourcing* ist für jede oder jeden Anbietenden von Outsourcing aus Sicht des Nutzenden von Outsourcing einmal anzuwenden.

Dieser Baustein behandelt Gefährdungen und Sicherheitsanforderungen aus Sicht der Nutzenden von Outsourcing-Leistungen und beschränkt sich auf die Anforderungen des Schutzes von Informationen seitens der auslagernden Institution.

Dieser Baustein behandelt nicht die Übertragungswege zu Anbietenden von Outsourcing.

Ebenso wird die Nutzung von Cloud-Diensten nicht in diesem Baustein behandelt, hierzu ist der Baustein OPS.2.2 *Cloud-Nutzung* anzuwenden.

Vom klassischen „IT-Outsourcing“ (wie dem Betrieb von Hard- und Software, Hosting, Housing usw.) abweichende Szenarien können mit dem Baustein OPS.2.3 *Nutzung von Outsourcing* mitunter nicht abschließend abgebildet werden und benötigen unter Umständen eine separate Risikoanalyse.

Als Sonderfall zählen Sicherheitsdienste, Reinigungskräfte, Wartungsdienste und Fremdpersonal, für die der Baustein OPS.2.3 *Nutzung von Outsourcing* nicht anzuwenden ist. Diese werden über die Anforderungen zu Sicherheitsdiensten, Reinigungskräften, Wartungsdiensten und Fremdpersonal in den Bausteinen ORP.1 *Organisation* und INF.1 *Allgemeines Gebäude* eingebunden.

Das Pendant zum Baustein OPS.2.3 *Nutzung von Outsourcing* bildet der Baustein OPS.3.2 *Anbieten von Outsourcing*, der das Outsourcing-Verhältnis aus der Sicht der Dienstleistenden behandelt. Zusammen bilden die beiden Bausteine ein ganzheitliches Bild des Outsourcing-Verhältnisses ab und sorgen mit ihren Anforderungen für ein grundlegendes sicheres Outsourcing-Vorhaben.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.2.3 *Nutzung von Outsourcing* von besonderer Bedeutung.

2.1. Unzureichende Strategie für das Outsourcing

Eine unzureichende Strategie führt dazu, dass die Informationssicherheit in Outsourcing-Vorhaben nicht angemessen berücksichtigt wird. Hierdurch wird die Informationssicherheit nicht angemessen in den einzelnen Phasen des Outsourcing-Lebenszyklus beachtet und somit kein ausreichendes Niveau der Informationssicherheit in der eigenen Institution sowie bei Anbietenden von Outsourcing angestrebt und umgesetzt. Dadurch können Prozesse beeinträchtigt, ausfallen und Informationen an unbefugte Dritte abfließen.

2.2. Gefahr des Outsourcings von institutionskritischen Prozessen

Prozesse, die aufgrund ihrer Kritikalität oder des Schutzbedarfs in der Institution verbleiben sollten, werden ausgelagert. Infolgedessen kann die Institution den Prozess, der für den ordentlichen Geschäftsbetrieb notwendig ist, nicht mehr angemessen kontrollieren und steuern. Wenn der Prozess ausfällt oder gestört wird, kann kein ordentlicher Geschäftsbetrieb sichergestellt werden. Darüber

hinaus gewinnen die Anbietenden von Outsourcing einen größeren Einfluss. Es droht den Nutzenden von Outsourcing ein Steuerungsverlust.

2.3. Abhängigkeit von Anbietenden von Outsourcing

Entscheidet sich eine Institution für Outsourcing, macht sie sich damit auch von Anbietenden von Outsourcing abhängig. Mit dieser Abhängigkeit kann Wissen verloren gehen und die ausgelagerten Prozesse können nicht mehr vollständig kontrolliert werden. Außerdem könnte der Schutzbedarf der ausgelagerten Geschäftsprozesse und Informationen unterschiedlich eingeschätzt werden. Dies kann dazu führen, dass für den Schutzbedarf entsprechend ungeeignete Sicherheitsmaßnahmen umgesetzt werden. Häufig lagern Institutionen gesamte Geschäftsprozesse an Anbietende von Outsourcing aus. Die Anbietenden von Outsourcing können dadurch die Geschäftsprozesse mit schutzbedürftigen Informationen, Ressourcen und IT-Systemen vollständig kontrollieren. Gleichzeitig nimmt das Wissen über diese Bereiche bei Nutzenden von Outsourcing ab. Als Folge ist es möglich, dass die Nutzenden von Outsourcing Defizite der Informationssicherheit nicht mehr bemerken. Diese Situation könnte von Anbietenden von Outsourcing ausgenutzt werden, z. B. indem sie drastisch die Preise erhöhen oder die Qualität der Dienstleistungen abnimmt.

2.4. Unzureichendes Niveau der Informationssicherheit beim Outsourcing

Ein unzureichendes Niveau an Informationssicherheit kann dazu führen, dass die Informationssicherheit in Outsourcing-Vorhaben nicht angemessen berücksichtigt wird. Die Folge ist, dass die Anbietenden von Outsourcing keinen oder einen nur unzureichenden Standard der Informationssicherheit für den Outsourcing-Prozess aufrechterhalten. Folglich entstehen Schwachstellen, von denen IT-gestützte Angriffe sowie Datenverluste ausgehen können. Darüber hinaus können für die Nutzenden von Outsourcing rechtliche Konsequenzen mit finanziellen Auswirkungen sowie Reputationsverluste entstehen.

2.5. Mangelhaftes Auslagerungsmanagement

Ein nicht vorhandenes oder nur teilweise umgesetztes Auslagerungsmanagement äußert sich dadurch, dass die laufenden ausgelagerten Prozesse unzureichend verwaltet werden. Dadurch verringert oder verliert sich die Transparenz über die ausgelagerten Prozesse. Hierdurch können Nutzende von Outsourcing die Anbietenden von Outsourcing nicht mehr kontrollieren und angemessen steuern. Die Nutzenden von Outsourcing können nicht mehr sicherstellen, dass die Anbietenden von Outsourcing in dem ausgelagerten Prozess die Informationssicherheit sorgfältig behandeln.

2.6. Unzulängliche vertragliche Regelungen mit Anbietenden von Outsourcing

Unzulängliche vertragliche Regelungen mit den Anbietenden von Outsourcing können zu Schwachstellen in der Informationssicherheit entlang des gesamten Outsourcing-Lebenszyklus führen. Die vertraglichen Regelungen definieren den gesamten Outsourcing-Prozess und stellen den Ausgangspunkt für Ansprüche der Nutzenden gegenüber den Anbietenden von Outsourcing dar. Aufgrund von unzulänglichen vertraglichen Regelungen mit den Anbietenden von Outsourcing können vielfältige und auch schwerwiegende Sicherheitsprobleme auftreten. Wenn Aufgaben, Leistungsparameter oder Aufwände ungenügend oder missverständlich beschrieben wurden, können möglicherweise aus Unkenntnis oder wegen fehlender Ressourcen Sicherheitsmaßnahmen nicht umgesetzt werden. Dies kann viele negative Auswirkungen nach sich ziehen, etwa, wenn regulatorische Anforderungen und Pflichten nicht erfüllt oder Auskunftspflichten und Gesetze nicht eingehalten werden. Wird bei der Vertragsgestaltung der Aspekt der Informationssicherheit nicht

berücksichtigt, so können Prozesse und Daten der Nutzenden von Outsourcing unzureichend abgesichert werden.

2.7. Ungeeignete Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten

Je nach Outsourcing-Vorhaben kann es erforderlich sein, dass die Mitarbeitenden von Anbietenden von Outsourcing Zutritts-, Zugangs- und Zugriffsrechte zu IT-Systemen, Informationen, Gebäuden oder Räumen der Nutzenden von Outsourcing benötigen. Diese Rechte können ungeeignet vergeben, verwaltet und kontrolliert werden, hierdurch können im Extremfall sogar unautorisiert Rechte vergeben werden. Außerdem kann der notwendige Schutz der Informationen der Nutzenden von Outsourcing nicht mehr gewährleistet werden. Beispielsweise ist es ein gravierendes Sicherheitsrisiko, unkontrolliert administrative Berechtigungen an Mitarbeitende von Anbietenden von Outsourcing zu vergeben. Diese könnten Berechtigungen ausnutzen und sensible Informationen kopieren oder manipulieren.

2.8. Kontroll- und Steuerverlust durch Weiterverlagerungen

Teile von Geschäftsprozessen oder Tätigkeiten werden von Anbietenden von Outsourcing unter Umständen vollständig oder partiell an Sub-Dienstleistende weitergegeben. Da durch die zusätzlichen Beteiligten der Outsourcing-Prozess komplexer wird, wird dieser für die Nutzenden von Outsourcing intransparenter. Durch diese fehlende Transparenz können die Nutzenden von Outsourcing die ausgelagerten Prozesse nicht mehr angemessen kontrollieren und steuern. Darüber hinaus können Anbietende von Outsourcing versäumen, dass von Nutzenden von Outsourcing geforderte Mindestniveau der Informationssicherheit vom Sub-Dienstleistenden einzufordern. Eine Folge ist, dass unter Umständen die vereinbarten informationstechnischen Sicherheitsaspekte von den Sub-Dienstleistenden nicht vollständig umgesetzt werden.

2.9. Fehlende und unzulängliche Instrumente zur Steuerung von Anbietenden von Outsourcing

Damit eine Institution prüfen kann, ob die ausgelagerten Prozesse von Anbietenden von Outsourcing ordnungsgemäß umgesetzt werden, benötigt sie neben entsprechenden Vereinbarungen auch die Instrumente dazu. Dies können beispielsweise qualitative und quantitative Leistungskennzahlen (KPIs) sein. Um auf Minder- und Schlechtleistung reagieren zu können, werden entsprechend festgelegte Leistungskennzahlen benötigt. Fehlende und unzulängliche Instrumente führen dazu, dass die Anbietenden von Outsourcing nicht adäquat kontrolliert und gesteuert werden können. Dadurch kann nicht mehr geprüft und nachvollzogen werden, ob die festgelegten Sicherheitsanforderungen eingehalten werden.

2.10. Unzulängliche Regelungen für eine geplante und ungeplante Beendigung eines Outsourcing-Verhältnisses

Ein Outsourcing-Verhältnis kann ordentlich gekündigt oder auch außerordentlich beendet werden. Hierbei können unzulängliche oder fehlende Regelungen dazu führen, dass Hardware, Daten und Zugänge nicht oder nicht ordnungsgemäß an die Nutzenden von Outsourcing übergeben bzw. übermittelt werden.

2.11. Unzureichendes Notfallkonzept

Im Falle einer Störung, eines Notfalls oder einer Krise kann ein unzureichendes Notfallmanagement dazu führen, dass die ausgelagerten Prozesse ausfallen. Dabei bereitet insbesondere eine unzureichende

Notfallvorsorge die Institution in ungenügendem Maße auf eine Not- oder Krisensituation vor. Eine effektive Notfallbewältigung kann auf dieser Grundlage nicht sichergestellt werden. Störungen, Not- und Krisensituationen können nicht kontrolliert werden und zu unmittelbaren wirtschaftlichen Auswirkungen führen. In diesem Fall ist nicht nur die eigene Institution, sondern auch alle angebundenen Institutionen, die in der Notfallvorsorge und Notfallbewältigung berücksichtigt werden müssen, betroffen. Kaskadeneffekte durch vor- und nachgelagerte Dienstleistende führen zu beträchtlichen Auswirkungen auf den Geschäftsbetrieb der Nutzenden von Outsourcing.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.2.3 *Nutzung von Outsourcing* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Fachverantwortliche, Beschaffungsstelle, Zentrale Verwaltung, Notfallbeauftragte, Personalabteilung

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

OPS.2.3.A1 Erstellung von Anforderungsprofilen für Prozesse (B) [Fachverantwortliche]

Falls keine Business-Impact-Analyse (BIA) vorhanden ist, MÜSSEN Anforderungsprofile in Form von Steckbriefen für die Prozesse angefertigt werden, die potenziell ausgelagert werden sollen. Diese Anforderungsprofile MÜSSEN die Funktion, verarbeite Daten, Schnittstellen sowie eine Bewertung der Informationssicherheit enthalten. Insbesondere MÜSSEN die Abhängigkeiten zwischen den Prozessen sowie zu untergeordneten Teilprozessen berücksichtigt werden. Die Anforderungsprofile MÜSSEN die Kritikalität des jeweiligen Prozesses für den ordentlichen Geschäftsbetrieb abbilden.

OPS.2.3.A2 Verfolgung eines risikoorientierten Ansatzes im Auslagerungsmanagement (B)

Für Prozesse, die potenziell ausgelagert werden sollen, MUSS risikoorientiert betrachtet und entschieden werden, ob diese ausgelagert werden können. Für diese Bewertung SOLLTEN die Anforderungsprofile als Grundlage genutzt werden. Wenn der Prozess ausgelagert wird, SOLLTE das Resultat im Auslagerungsregister abgelegt werden. Um Änderungen an Prozessen oder der Gefährdungslage zu berücksichtigen, MÜSSEN in regelmäßigen Abständen sowie anlassbezogen die ausgelagerten Prozesse erneut risikoorientiert betrachtet werden.

OPS.2.3.A3 Festlegung von Eignungsanforderungen an Anbietende von Outsourcing (B) [Fachverantwortliche, Institutionsleitung]

Interne Eignungsanforderungen an potenzielle Anbietende von Outsourcing MÜSSEN festgelegt werden. Diese Eignungsanforderungen MÜSSEN die erforderlichen Kompetenzen, um den Prozess aus Sicht der Informationssicherheit abzusichern, sowie die Reputation hinsichtlich der Vertrauenswürdigkeit und Zuverlässigkeit berücksichtigen. Diese Eignungsanforderungen SOLLTEN auf Basis der Unternehmensstrategie (siehe OPS.2.3.A8 *Erstellung einer Strategie für Outsourcing-Vorhaben*) erstellt werden. Es MUSS geprüft werden, ob potenzielle Interessenkonflikte vorliegen. Ferner SOLLTEN die Anbietenden von Outsourcing regelmäßig gegen die Eignungsanforderungen geprüft werden. Wenn die Anbietenden von Outsourcing nicht die Eignungsanforderungen erfüllen, SOLLTEN Handlungsmaßnahmen getroffen und in einem Maßnahmenkatalog festgehalten werden.

OPS.2.3.A4 Grundanforderungen an Verträge mit Anbietenden von Outsourcing (B)

Einheitliche Grundanforderungen an Outsourcing-Verträge MÜSSEN entwickelt werden. Diese Grundanforderungen MÜSSEN Aspekte der Informationssicherheit, einen Zustimmungsvorbehalt bei Weiterverlagerungen sowie ein Recht auf Prüfung, Revision und Audit beinhalten. Bei der Entwicklung der Grundanforderungen SOLLTEN die Resultate der risikoorientierten Betrachtung sowie Eignungsanforderungen an Anbietende von Outsourcing mit einfließen. Mit den Anbietenden von Outsourcing SOLLTE eine Verschwiegenheitserklärung zum Schutz von sensiblen Daten vereinbart werden. Die Grundanforderungen MÜSSEN in Vereinbarungen und Verträgen einheitlich umgesetzt werden. Auf Basis der Grundanforderungen SOLLTE eine einheitliche Vertragsvorlage erstellt und für alle Outsourcing-Vorhaben genutzt werden.

OPS.2.3.A5 Vereinbarung der Mandantenfähigkeit (B)

In einer Vereinbarung zur Mandantenfähigkeit mit den Anbietenden von Outsourcing MUSS sichergestellt werden, dass die Daten und Verarbeitungskontexte durch den Anbietenden von Outsourcing ausreichend sicher getrennt sind. In dieser Vereinbarung SOLLTE ein Mandantentrennungskonzept von den Anbietenden von Outsourcing gefordert werden. Das Mandantentrennungskonzept SOLLTE zwischen mandantenabhängigen und mandantenübergreifenden Daten und Objekten unterscheiden und darlegen, mit welchen Mechanismen die Anbietenden von Outsourcing trennen.

OPS.2.3.A6 Festlegung von Sicherheitsanforderungen und Erstellung eines Sicherheitskonzeptes für das Outsourcing-Vorhaben (B)

Mit den Anbietenden von Outsourcing MUSS vertraglich vereinbart werden, dass IT-Grundschutz umgesetzt oder mindestens die Anforderungen aus den relevanten Bausteinen geeignet erfüllt werden. Darüber hinaus SOLLTE mit den Anbietenden von Outsourcing vereinbart werden, dass sie ein Managementsystem für Informationssicherheit (ISMS) etablieren. Die Nutzenden von Outsourcing MÜSSEN für jedes Outsourcing-Vorhaben ein Sicherheitskonzept basierend auf den sich aus dem IT-Grundschutz ergebenen Sicherheitsanforderungen erstellen. Dabei MUSS das Sicherheitskonzept der Nutzenden mit den Anbietenden von Outsourcing abgestimmt werden. Ebenso SOLLTE jeder Anbietende ein individuelles Sicherheitskonzept für das jeweilige Outsourcing-Vorhaben vorlegen. Das Sicherheitskonzept der Anbietenden von Outsourcing und dessen Umsetzung SOLLTE zu einem gesamten Sicherheitskonzept zusammengeführt werden. Wenn Risikoanalysen notwendig sind, MÜSSEN Vereinbarungen getroffen werden, wie die Risikoanalyse geprüft und gegebenenfalls in das eigene Risikomanagement überführt werden kann. Die Nutzenden von Outsourcing oder unabhängige Dritte MÜSSEN regelmäßig überprüfen, ob das Sicherheitskonzept wirksam ist.

OPS.2.3.A7 Regelungen für eine geplante oder ungeplante Beendigung eines Outsourcing-Verhältnisses (B) [Fachverantwortliche, Institutionsleitung]

Für geplante sowie ungeplante Beendigungen des Outsourcing-Verhältnisses MÜSSEN Regelungen getroffen werden. Es MUSS festgelegt werden, wie alle Informationen, Daten und Hardware der Nutzenden vom Anbietenden von Outsourcing zurückgegeben werden. Hierbei MÜSSEN gesetzliche Vorgaben zur Aufbewahrung von Daten beachtet werden. Ferner SOLLTE überprüft werden, ob die Zugangs-, Zutritts- und Zugriffsrechte für die Anbietenden von Outsourcing mit der Beendigung des Outsourcing-Verhältnisses aufgehoben wurden.

3.2. Standard-Anforderungen

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

OPS.2.3.A8 Erstellung einer Strategie für Outsourcing-Vorhaben (S) [Institutionsleitung]

Eine Strategie für Outsourcing-Vorhaben SOLLTE erstellt und etabliert werden. In dieser Strategie SOLLTEN die Ziele, Chancen und Risiken der Outsourcing-Vorhaben beschrieben werden. Die Strategie SOLL der Institution einen Rahmen für die Anforderungsprofile, die Eignungsanforderung an Anbietende von Outsourcing sowie dem Auslagerungsmanagement vorgeben. Darüber hinaus SOLLTEN neben den wirtschaftlichen, technischen, organisatorischen und rechtlichen Rahmenbedingungen auch die relevanten Aspekte der Informationssicherheit berücksichtigt werden. Es SOLLTE eine Multi-Sourcing Strategie verfolgt werden, um Engpässe sowie Abhängigkeiten von Anbietenden von Outsourcing zu vermeiden. Die Nutzenden von Outsourcing SOLLTEN ausreichend Fähigkeiten, Kompetenzen sowie Ressourcen behalten, um einer Abhängigkeit gegenüber den Anbietenden von Outsourcing vorzubeugen.

OPS.2.3.A9 Etablierung einer Richtlinie zur Auslagerung (S) [Institutionsleitung]

Auf Basis der Strategie für Outsourcing-Vorhaben SOLLTE eine Richtlinie für den Bezug von Outsourcing-Dienstleistungen erstellt und in der Institution etabliert werden. Diese SOLLTE die allgemeinen Anforderungen basierend auf der Anforderung OPS.2.3.A4 *Grundanforderungen an Verträge mit Anbietenden von Outsourcing* sowie weitere Aspekte der Informationssicherheit für Outsourcing-Vorhaben standardisieren. Das Test- und Freigabeverfahren für Outsourcing-Vorhaben SOLLTE in dieser Richtlinie geregelt sein. Darüber hinaus SOLLTEN Maßnahmen berücksichtigt sein, um Compliance-Risiken bei Anbietenden von Outsourcing sowie bei Sub-Dienstleistenden zu bewältigen.

OPS.2.3.A10 Etablierung einer zuständigen Person für das Auslagerungsmanagement (S) [Personalabteilung]

Die verschiedenen Outsourcing-Vorhaben SOLLTEN durch eine zuständige Person für das Auslagerungsmanagement verwaltet werden. Die zuständige Person SOLLTE ernannt und die Befugnisse festgelegt und dokumentiert werden. Die zuständige Person SOLLTE als Schnittstelle in der Kommunikation zwischen den Nutzenden und Anbietenden von Outsourcing eingesetzt werden. Darüber hinaus SOLLTE die zuständige Person Berichte über das Outsourcing in regelmäßigen Abständen und anlassbezogen anfertigen und der Institutionsleitung übergeben. In der Vertragsgestaltung SOLLTE die zuständige Person einbezogen werden. Die zuständige Person SOLLTE ein angemessenes Kontingent von Arbeitstagen für die Aufgaben des Auslagerungsmanagements eingeräumt bekommen. Darüber hinaus SOLLTE die zuständige Person hinsichtlich Informationssicherheit geschult und sensibilisiert sein.

OPS.2.3.A11 Führung eines Auslagerungsregisters (S)

Die zuständige Person für das Auslagerungsmanagement SOLLTE ein Auslagerungsregister erstellen und pflegen, dass die Dokumentation der Outsourcing-Prozesse und Vorhaben in der Institution zentralisiert. Dieses SOLLTE auf der Basis der Anforderungsprofile erstellt werden und Informationen zu den Anbietenden von Outsourcing, Leistungskennzahlen, Kritikalität des Prozesses, abgeschlossene Verträgen und Vereinbarungen sowie Änderungen enthalten. Änderungen am Auslagerungsregister SOLLTEN geeignet nachgehalten werden.

OPS.2.3.A12 Erstellung von Auslagerungsberichten (S)

Die zuständige Person für das Auslagerungsmanagement SOLLTE regelmäßig interne Auslagerungsberichte auf Basis des Auslagerungsregisters erstellen. Diese Auslagerungsberichte SOLLTEN den aktuellen Status des Outsourcing-Vorhabens mit allgemeinen Problemen und Risiken sowie Aspekte der Informationssicherheit enthalten. Der Auslagerungsbericht SOLLTE der Institutionsleitung vorgelegt werden.

OPS.2.3.A13 Bereitstellung der erforderlichen Kompetenzen bei der Vertragsgestaltung (S) [Institutionsleitung]

Die Verträge SOLLTEN durch verschiedene Vertreter aus unterschiedlichen Bereichen gestaltet werden. Dabei SOLLTE ein Interessenkonflikt zwischen operativem Geschäft und Informationssicherheit vermieden werden.

OPS.2.3.A14 Erweiterte Anforderungen an Verträge mit Anbietenden von Outsourcing (S)

Mit Anbietenden von Outsourcing SOLLTE vereinbart werden, auf welche Bereiche und Dienste die Anbietenden im Netz der Nutzenden von Outsourcing zugreifen dürfen. Der Umgang mit anfallenden Metadaten SOLLTE geregelt werden. Die Nutzenden SOLLTEN Leistungskennzahlen für die Anbietenden von Outsourcing definieren und im Vertrag festlegen. Für den Fall, dass die vereinbarten Leistungskennzahlen unzureichend erfüllt werden, SOLLTEN mit den Anbietenden von Outsourcing Konsequenzen, wie z. B. Vertragsstrafen, festgelegt werden. Die Verträge SOLLTEN Kündigungsoptionen, um das Outsourcing-Verhältnisses aufzulösen, enthalten. Hierbei SOLLTE auch geregelt sein, wie das Eigentum der Nutzenden von Outsourcing zurückgegeben wird. Im Vertrag SOLLTEN Verantwortlichkeiten hinsichtlich des Notfall- und Krisenmanagements definiert und benannt werden.

OPS.2.3.A15 Anbindung an die Netze der Outsourcing-Partner (S)

Bevor das Datennetz der Nutzenden an das Datennetz der Anbietenden von Outsourcing angebunden wird, SOLLTEN alle sicherheitsrelevanten Aspekte schriftlich vereinbart werden. Es SOLLTE geprüft und dokumentiert werden, dass die Vereinbarungen für die Netzanbindung eingehalten werden. Das geforderte Sicherheitsniveau SOLLTE nachweislich bei den Anbietenden von Outsourcing umgesetzt und überprüft werden, bevor die Netzanbindung zu den Nutzenden von Outsourcing aktiviert wird. Bevor die Netze angebunden werden, SOLLTE mit Testdaten die Verbindung getestet werden. Gibt es Sicherheitsprobleme auf einer der beiden Seiten, SOLLTE festgelegt sein, wer informiert und wie eskaliert wird.

OPS.2.3.A16 Prüfung der Anbietenden von Outsourcing (S)

Die Anbietenden von Outsourcing SOLLTEN hinsichtlich der vertraglich festgelegten Sicherheitsanforderungen überprüft und die Resultate dokumentiert werden. Die Anbietenden von Outsourcing sind in regelmäßigen Abständen und anlassbezogen zu auditieren.

OPS.2.3.A17 Regelungen für den Einsatz des Personals von Anbietenden von Outsourcing (S)

Die Beschäftigten der Anbietenden von Outsourcing SOLLTEN schriftlich verpflichtet werden, einschlägige Gesetze, Vorschriften sowie die Regelungen der Nutzenden von Outsourcing einzuhalten. Die Beschäftigten der Anbietenden von Outsourcing SOLLTEN geregelt in ihre Aufgaben eingewiesen und über bestehende Regelungen zur Informationssicherheit unterrichtet werden. Für die Beschäftigten der Anbietenden von Outsourcing SOLLTEN Vertretungsregelungen existieren. Es SOLLTE ein geregeltes Verfahren festgelegt werden, das beschreibt, wie das Auftragsverhältnis mit den Beschäftigten der Anbietenden von Outsourcing beendet wird. Fremdpersonal der Anbietenden von Outsourcing, das kurzfristig oder nur einmal eingesetzt wird, SOLLTE wie Besuchende behandelt werden.

OPS.2.3.A18 Überprüfung der Vereinbarungen mit Anbietenden von Outsourcing (S)

Vereinbarungen mit Anbietenden von Outsourcing hinsichtlich der Angemessenheit der festgelegten Sicherheitsanforderungen sowie sonstigen Sicherheitsanforderungen SOLLTEN in regelmäßigen Abständen und anlassbezogen überprüft werden. Vereinbarungen mit Anbietenden von Outsourcing mit unzureichend festgelegten Sicherheitsanforderungen SOLLTEN nachgebessert werden. Die Anbietenden von Outsourcing SOLLTEN dazu verpflichtet werden, bei veränderter Gefährdungs- oder Gesetzeslage, die festgelegten Sicherheitsanforderungen nachzubessern.

OPS.2.3.A19 Überprüfung der Handlungsalternativen hinsichtlich einer geplanten oder ungeplanten Beendigung eines Outsourcing-Verhältnisses (S) [Beschaffungsstelle]

Handlungsalternativen SOLLTEN entwickelt werden für den Fall einer geplanten oder ungeplanten Beendigung des Outsourcing-Verhältnisses. Das Resultat SOLLTE in einem Maßnahmenkatalog für geplante und ungeplante Beendigung des Outsourcing-Verhältnisses dokumentiert werden. Dabei SOLLTEN auch alternative Anbietende von Outsourcing ermittelt werden, die über das notwendige Niveau an Informationssicherheit verfügen, um den Prozess sicher umzusetzen. Dies SOLLTE in regelmäßigen Abständen und anlassbezogen geprüft werden.

OPS.2.3.A20 Etablierung sowie Einbeziehung von Anbietenden von Outsourcing im Notfallkonzept (S) [Notfallbeauftragte]

Ein Notfallkonzept SOLLTE in der Institution etabliert sein. Dies SOLLTE auf der Basis einer Business-Impact-Analyse basieren und die Abhängigkeiten der ausgelagerten Prozesse mit den intern verbliebenen Prozessen berücksichtigen. Das Notfallkonzept SOLLTE den Anbietenden von Outsourcing in seiner Notfallvorsorge und -bewältigung berücksichtigen und mit diesem abgestimmt sein. Dabei SOLLTEN die Schnittstellen zu Anbietenden von Outsourcing mit Verantwortlichen benannt und besetzt werden, um einen Informationsaustausch sowie eine effektive Kollaboration in einer Not- oder Krisensituation zu ermöglichen. Gemeinsame Not- und Krisenfallpläne SOLLTEN für eine Störung oder einen Ausfall der Anbietenden von Outsourcing erstellt werden. Standardisierte Protokolle und Berichte SOLLTEN zur Meldung von Sicherheitsvorfällen etabliert werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

OPS.2.3.A21 Abschluss von ESCROW-Verträgen bei softwarenahen Dienstleistungen (H)

Wird Software von Anbietenden von Outsourcing bezogen, SOLLTE ein ESCROW-Vertrag abgeschlossen werden. Dieser SOLLTE Verwertungs- und Bearbeitungsrechte der Software sowie Herausgabefälle des Quellcodes regeln. Darüber hinaus SOLLTE festgelegt werden, wie häufig der Quellcode hinterlegt und dokumentiert wird. Weiterhin SOLLTEN Geheimhaltungspflichten über den hinterlegten Quellcode und die zugehörige Dokumentation geregelt werden.

OPS.2.3.A22 Durchführung von gemeinsamen Notfall- und Krisenübungen (H) [Notfallbeauftragte]

Gemeinsame Notfall- und Krisenübungen mit den Anbietenden von Outsourcing SOLLTEN durchgeführt und dokumentiert werden (siehe DER.4 *Notfallmanagement*). Das Resultat der Übung SOLLTE dazu genutzt werden, um das Notfallkonzept sowie insbesondere die gemeinsamen Maßnahmenpläne zu verbessern. Die Notfall- und Krisenübungen SOLLTEN regelmäßig und anlassbezogen durchgeführt werden.

OPS.2.3.A23 Einsatz von Verschlüsselungen (H)

Sensible Daten SOLLTEN angemessen verschlüsselt werden, wenn sie zum Anbietenden von Outsourcing übertragen werden. Die abgelegten Daten SOLLTEN durch eine Datenverschlüsselung oder eine Verschlüsselung des Speichermediums geschützt werden. Nach Möglichkeit SOLLTE eine vom BSI geprüfte und freigegebene Verschlüsselungssoftware genutzt werden.

OPS.2.3.A24 Sicherheits- und Eignungsüberprüfung von Mitarbeitenden (H) [Personalabteilung]

Mit externen Anbietenden von Outsourcing SOLLTE vertraglich vereinbart werden, dass die Vertrauenswürdigkeit des eingesetzten Personals geeignet überprüft wird. Dazu SOLLTEN gemeinsam Kriterien festgelegt und dokumentiert werden.

OPS.2.3.A25 Errichtung und Nutzung einer Sandbox für eingehende Daten vom Anbietenden von Outsourcing (H)

Für eingehende Daten vom Anbietenden von Outsourcing SOLLTE eine Sandbox eingerichtet werden. Hierbei SOLLTEN E-Mail-Anhänge in der Sandbox standardisiert geöffnet werden. Updates und Anwendungen eines softwarenahen Anbietenden von Outsourcing SOLLTEN in der Sandbox initial getestet werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 im Kapitel A.15.2 "Steuerung der Dienstleistungserbringung von Lieferanten" Vorgaben für die Steuerung von Anbietenden von Outsourcing. In der DIN ISO 37500:2015-08 werden im "Leitfaden Outsourcing" weiterführende Informationen zum Umgang mit Anbietenden von Outsourcing aufgeführt.

Des Weiteren wird in der ISO 27002:2021 das Outsourcing-Verhältnis von Kapitel 5.19 bis 5.22 detailliert aufgeführt und spezifiziert somit die Vorgaben der ISO/IEC 27001:2013.

Das Information Security Forum (ISF) definiert in seinem Standard "The Standard of Good Practice for Information Security" verschiedene Anforderungen (SC1) an Anbietende von Outsourcing.

Der "Leitfaden Business Process Outsourcing: BPO als Chance für den Standort Deutschland" des Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V. (Bitkom) liefert Informationen, wie Geschäftsprozesse an Anbietenden von Outsourcing ausgelagert werden können.

Ebenso hat die Bitkom den "Leitfaden Rechtliche Aspekte von Outsourcing in der Praxis" herausgegeben, die rechtlichen Aspekte von Outsourcing behandelt.

Das National Institute of Standards and Technology (NIST) nennt in der NIST Special Publication 800-53 Anforderungen an Anbietenden von Outsourcing.

Bundesamt
für Sicherheit in der
Informationstechnik

OPS.3.2 Anbieten von Outsourcing

1. Beschreibung

1.1. Einleitung

Beim Outsourcing lagern Institutionen (Nutzende von Outsourcing) Geschäftsprozesse oder Tätigkeiten ganz oder teilweise zu einem oder mehreren externen Dienstleistungsunternehmen (Anbietende von Outsourcing) aus. Diese sogenannten Anbietende von Outsourcing betreiben im Rahmen des vereinbarten Outsourcing-Verhältnisses die Geschäftsprozesse oder Tätigkeiten nach festgelegten Kriterien. Allerdings verbleibt die Verantwortung aus Sicht der Informationssicherheit stets bei der auslagernden Institution.

Outsourcing kann die Nutzung und den Betrieb von Hard- und Software betreffen, wobei die Leistung in den Räumlichkeiten der Auftraggebenden oder in einer externen Betriebsstätte der Anbietenden von Outsourcing erbracht werden kann. Typische Beispiele des klassischen "IT-Outsourcings", worauf sich dieser Baustein bezieht, sind der Betrieb eines Rechenzentrums, einer Applikation oder einer Webseite. Outsourcing ist ein Oberbegriff, der oftmals durch weitere Begriffe konkretisiert wird, wie Hosting, Housing oder Colocation.

Ein Outsourcing-Verhältnis betrifft neben den ursprünglichen Nutzenden und Anbietenden von Outsourcing in vielen Fällen weitere, den Anbietenden von Outsourcing nachgelagerte, Sub-Dienstleistende. Werden Teile von Geschäftsprozessen oder Tätigkeiten von Anbietenden von Outsourcing weiter an Sub-Dienstleistende verlagert, so werden die von Nutzenden ausgelagerten Geschäftsprozesse oder Tätigkeiten weiter fragmentiert. Dies wirkt sich auf die Komplexität der Outsourcing-Kette aus, woraus eine schwindende Transparenz für die Nutzenden von Outsourcing folgt. Der Nachweis, dass die an die Anbietenden von Outsourcing gestellten Anforderungen erfüllt werden, erstreckt sich hierbei sowohl auf die Anbietenden von Outsourcing als auch auf die Sub-Dienstleistenden.

Zur besseren Verständlichkeit wird in diesem Baustein der Begriff "Prozess" stellvertretend für Geschäftsprozess, Tätigkeit oder Komponente verwendet, die ausgelagert wird.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, die Grundwerte der Informationssicherheit Vertraulichkeit, Integrität und Verfügbarkeit über den gesamten Lebenszyklus des Outsourcings durch die Anbietenden von Outsourcing sicherzustellen. Der Baustein soll dazu beitragen, dass die Anbietenden von Outsourcing gegenüber den Nutzenden von Outsourcing eine grundlegende Informationssicherheit gewährleistet. Mit Outsourcing ist dabei das klassische "IT-Outsourcing" gemeint.

Die Anforderungen des Bausteins OPS.3.2 *Anbieten von Outsourcing* sollen dazu beitragen, dass potenzielle Gefährdungen aus der Dienstleistung der Anbietenden von Outsourcing nicht die Nutzenden von Outsourcing gefährden. Dementsprechend sind diese Risiken zu mindern und vorzubeugen.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.3.2 *Anbieten von Outsourcing* ist aus Sicht der Anbietenden auf jede oder jeden Nutzenden, der Dienstleistungen vom Anbietenden bezieht, einmal anzuwenden.

Dabei bezieht sich der Baustein auf die Perspektive der Anbietenden von Outsourcing im Outsourcing-Verhältnis. Die Anforderungen des Bausteins stellen sicher, dass fundamentale Sicherheitsstandards gegenüber den Nutzenden von Outsourcing eingehalten werden und dazu beitragen, dass die Anforderungen der Nutzenden von Outsourcing an die Informationssicherheit über den gesamten Outsourcing-Prozess eingehalten werden können.

Der Fall einer Weiterverlagerung wird in dem Baustein OPS.3.2 *Anbieten von Outsourcing* nur bedingt betrachtet, da dies ein weiteres Outsourcing-Verhältnis darstellt und somit die Anbietenden von Outsourcing den Baustein OPS.2.3 *Nutzung von Outsourcing* für diese Sub-Dienstleistenden modellieren müssen.

Vom klassischen „IT-Outsourcing“ (wie dem Betrieb von Hard- und Software, Hosting, Housing usw.) abweichende Szenarien können mit dem Baustein OPS.3.2 *Anbieten von Outsourcing* mitunter nicht abschließend abgebildet werden und benötigen unter Umständen eine separate Risikoanalyse.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.3.2 *Anbieten von Outsourcing* von besonderer Bedeutung.

2.1. Unzureichendes Informationssicherheitsmanagement bei Anbietenden von Outsourcing

Ein mangelhaftes Informationssicherheitsmanagement kann dazu führen, dass die Schutzziele der Informationssicherheit durch die Anbietenden von Outsourcing nur unzureichend eingehalten werden. Durch einen Outsourcing-Vertrag sind die Anbietenden von Outsourcing dafür zuständig, das erforderliche Niveau an Informationssicherheit für den Outsourcing-Prozess einzuhalten. Sollten die Anbietenden von Outsourcing ihrer Zuständigkeit nicht nachkommen, so kann dies zu einer Gefahr für alle am Outsourcing-Prozess beteiligten Institutionen führen.

2.2. Unzureichendes Notfallmanagement der Anbietenden von Outsourcing

Wenn Störungen oder Notfälle bei Anbietenden von Outsourcing eintreten, kann dies zu einer Betriebsstörung führen, die auch die ausgelagerten Prozesse der Nutzenden von Outsourcing betreffen können und sich auf deren ordentlichen Geschäftsbetrieb auswirken. Insbesondere die Notfallvorsorge ist im Vorfeld von Not- und Krisensituation von entscheidender Bedeutung. Im Falle einer mangelhaften Notfallvorsorge kann für die Institution keine effektive Notfallbewältigung sichergestellt werden. Somit sind für die einzelnen Institutionen Störungen, Not- und Krisensituationen unter Umständen unkontrollierbar. Es kommt zu einem Kaskadeneffekt, der neben den Anbietenden von Outsourcing auch alle vor- und nachgelagerten Dienstleistenden sowie Kunden beeinträchtigt.

2.3. Unzulängliche vertragliche Regelungen mit Nutzenden von Outsourcing

Unzulänglichkeiten in der Vertragsgestaltung können dazu führen, dass die Informationssicherheit von ausgelagerten Prozessen der Nutzenden von Outsourcing unzureichend abgesichert ist. Vertragliche Regelungen definieren den gesamten Outsourcing-Prozess und stellen die rechtliche Grundlage für Ansprüche der Anbietenden von Outsourcing gegenüber den Nutzenden von Outsourcing dar. Somit übertragen sich die Unzulänglichkeiten aus der Vertragsgestaltung auf den gesamten Outsourcing-Lebenszyklus. Dies ist verbunden mit einer Vielzahl an möglichen Gefährdungsszenarien mit finanziellen und gesellschaftlichen Auswirkungen für die Nutzenden sowie Anbietenden von Outsourcing.

2.4. Schwachstellen bei der Anbindung Nutzender von Outsourcing

Die technische Anbindung der Nutzenden von Outsourcing an die Netze der Anbietenden von Outsourcing kann an den Schnittstellen zu technischen sowie organisatorischen Schwachstellen führen. Die technischen Schwachstellen in der Anbindung können zu Störungen, Datenverlust sowie zum Ausgangspunkt von IT-gestützte Angriffe führen. Dagegen können organisatorische Schwachstellen in Form von unbesetzten Schnittstellen zu Kommunikationsproblemen zwischen den Anbietenden und Nutzenden von Outsourcing führen. Diese können eine Gefahr für die Effizienz von Risikobewältigungsmaßnahmen in Not- und Krisensituationen darstellen.

2.5. Abhängigkeit von Sub-Dienstleistenden

Werden Tätigkeiten von Anbietenden von Outsourcing an Sub-Dienstleistende weiter verlagert, besteht das Risiko, dass die Sub-Dienstleistenden ihre Positionen ausnutzen, um Forderungen durchzusetzen sowie Vorgaben der Vereinbarung zu missachten. Es entsteht eine Abhängigkeit von Dritten, um die Kundenleistung zu erbringen. Sollten die Anbietenden von Outsourcing nicht in der Lage sein, eine Störung oder Ausfall der Sub-Dienstleistenden zu kompensieren, besteht eine zwingende Abhängigkeit. Dies bringt die Sub-Dienstleistenden gegenüber den Anbietenden von Outsourcing in eine vorteilhafte Position. Die Sub-Dienstleistenden können davon absehen, die vertraglich geregelte Qualität sowie das festgelegte Niveau der Informationssicherheit einzuhalten. Dies beeinträchtigt das Outsourcing-Verhältnis mit den Nutzenden von Outsourcing und bedeutet für die Anbietenden von Outsourcing rechtliche und finanzielle Auswirkungen sowie einen Reputationsverlust.

2.6. Ungeeignete Konfiguration und Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten

Eine entweder ungeeignete oder unzureichende Konfiguration eines zentralen Verzeichnisdienstes kann dazu führen, dass Nutzende Rechte erhalten, die sie potenziell dazu befähigen auf sensible oder personenbezogene Daten der Anbietenden von Outsourcing oder anderer Kunden des Anbietenden von Outsourcing zuzugreifen. Unter Umständen erfordern Outsourcing-Vorhaben, dass Nutzende von Outsourcing auf den Informationsverbund der Anbietenden von Outsourcing zugreifen müssen. Dies ist mit entsprechenden Rechten für Zutritt-, Zugang- und Zugriff verbunden, die ein Risiko für die IT-Systeme, Informationen sowie Gebäude darstellen. Eine Folge ist, dass die Integrität und Vertraulichkeit dieser Daten gefährdet sind. Letztlich kann dies dazu führen, dass Vertragsstrafen von den Nutzenden von Outsourcing gegenüber den Anbietenden von Outsourcing geltend gemacht werden sowie ein Reputationsverlust für die Anbietenden von Outsourcing sowie ihre Kunden eintreten kann.

2.7. Unzureichende Mandantenfähigkeit bei Anbietenden von Outsourcing

Anbietende von Outsourcing haben in der Regel unterschiedliche Kunden, die auf die gleichen Ressourcen wie IT-Systeme, Netze oder Personal zurückgreifen. Sind IT-Systeme und Daten der Nutzenden von Outsourcing unzureichend voneinander getrennt und abgesichert, besteht die Gefahr, dass Nutzende auf die Bereiche anderer Nutzender zugreifen und unberechtigt auf Daten zugreifen können. Dies stellt einen unmittelbaren Verstoß gegen die Vertraulichkeit der jeweiligen Daten der Nutzenden dar. Insbesondere ist dies problematisch bei Nutzenden von Outsourcing, die im Wettbewerb miteinander stehen. Die Auswirkungen wären Reputationsverlust für die Anbietenden von Outsourcing sowie rechtliche Folgen durch die geschädigten Nutzenden von Outsourcing.

2.8. Kontroll- und Steuerungsverlust bei der Weiterverlagerung an Sub-Dienstleistende

Ausgelagerte Prozesse werden von Anbietenden von Outsourcing unter Umständen im Rahmen einer Weiterverlagerung vollständig oder partiell an Sub-Dienstleistende weitergegeben. Eine unzureichende Kontrolle der Sub-Dienstleistenden führt dazu, dass vereinbarte Aspekte der Informationssicherheit von Sub-Dienstleistenden unzureichend eingehalten werden. Dies hat im weiteren Verlauf Konsequenzen für das Outsourcing-Verhältnis mit den Nutzenden von Outsourcing sowie unmittelbare finanzielle Auswirkungen und Reputationsverluste für die Anbietenden von Outsourcing zur Folge.

2.9. Unzulängliche Regelungen für eine geplante oder ungeplante Beendigung eines Outsourcing-Verhältnisses

Unzulängliche Regelungen für das Ende eines Outsourcing-Verhältnisses können dazu führen, dass Hardware sowie Daten abschließend nicht ordnungsgemäß an die Nutzenden von Outsourcing übergeben oder übermittelt werden. Hinzu kommt, dass vorhandene Kundendaten nicht nach Speicherfrist der einschlägigen Gesetze und Vorschriften ordnungsgemäß gelöscht werden. Ein Outsourcing-Verhältnis kann durch eine ordentliche Kündigung sowie durch außerordentliche Gründe beendet werden. Exemplarisch hierfür ist eine Insolvenz von Anbietenden von Outsourcing. Die Anbietenden von Outsourcing schützen unter Umständen nach der Vertragsauflösung die vorhandenen Daten der Nutzenden von Outsourcing nicht angemessen gemäß des Schutzbedarfs des jeweiligen Eigentümers. Die Daten können in die Hand Dritter gelangen und bei Veröffentlichung zu Reputationsverlust führen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.3.2 *Anbieten von Outsourcing* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Institution, Datenschutzbeauftragte, Notfallbeauftragte

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig

zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

OPS.3.2.A1 Einhaltung der Schutzziele der Informationssicherheit durch ein Informationssicherheitsmanagement (B)

Der Schutzbedarf für Vertraulichkeit, Integrität und Verfügbarkeit von Nutzenden von Outsourcing MUSS im Outsourcing-Prozess berücksichtigen werden. Dabei MUSS sichergestellt werden, dass das von den Nutzenden von Outsourcing geforderte Minimum an Informationssicherheit eingehalten wird. Zudem MÜSSEN die geltenden regulatorischen und gesetzlichen Aspekte berücksichtigt werden.

OPS.3.2.A2 Grundanforderungen an Verträge mit Nutzenden von Outsourcing (B)

Einheitliche Grundanforderungen an Outsourcing-Verträge MÜSSEN entwickelt werden. Diese SOLLTEN einheitlich in Verträgen umgesetzt werden. Diese Grundanforderungen MÜSSEN Aspekte der Informationssicherheit und Sicherheitsanforderungen der Nutzenden von Outsourcing beinhalten. Zudem MÜSSEN sie beinhalten, wie mit Weiterverlagerungen durch die Anbietenden umgegangen wird. Die Grundanforderungen MÜSSEN beinhalten, dass die Nutzenden das Recht haben Prüfungen, Revisionen und Auditierungen durchzuführen, um sicherzustellen, dass die vertraglich geregelten Anforderungen an die Informationssicherheit eingehalten werden. Mit den Nutzenden von Outsourcing SOLLTE eine Verschwiegenheitserklärung zum Schutz von sensiblen Daten, Vereinbarungen zum Informationsaustausch und Service-Level-Agreements vereinbart werden. Die Grundanforderungen MÜSSEN in Vereinbarungen und Verträgen einheitlich umgesetzt werden. Auf Basis der Grundanforderungen SOLLTE eine einheitliche Vertragsvorlage erstellt und für alle Outsourcing-Vorhaben genutzt werden.

OPS.3.2.A3 Weitergabe der vertraglich geregelten Bestimmungen mit Nutzenden von Outsourcing an Sub-Dienstleistende (B)

Werden Prozesse von Anbietenden von Outsourcing weiter an Sub-Dienstleistende verlagert, MÜSSEN die vertraglichen Bestimmungen mit den Nutzenden von Outsourcing an die Sub-Dienstleistenden weitergegeben werden. Dies MUSS in den Verträgen mit den Sub-Dienstleistenden entsprechend festlegt und durchgesetzt werden. Auf Nachfrage von Nutzenden von Outsourcing MÜSSEN diese Verträge vorgelegt werden.

OPS.3.2.A4 Erstellung eines Mandantentrennungskonzepts (B)

Es MUSS ein Mandantentrennungskonzept erstellt und umgesetzt werden. Das Mandantentrennungskonzept MUSS sicherstellen, dass Daten und Verarbeitungskontexte verschiedener Nutzender von Outsourcing ausreichend sicher getrennt werden. Dabei MUSS zwischen mandantenabhängigen und mandantenübergreifenden Daten und Objekten unterschieden werden. Es MUSS dargelegt werden, mit welchen Mechanismen die Anbietenden von Outsourcing die Mandanten trennen. Die benötigten Mechanismen zur Mandantentrennung MÜSSEN durch die Anbietenden von Outsourcing ausreichend umgesetzt werden. Das Mandantentrennungskonzept MUSS durch die Anbietenden von Outsourcing erstellt und den Nutzenden von Outsourcing zur Verfügung gestellt werden. Darüber hinaus MUSS es für den Schutzbedarf der Daten der Nutzenden von Outsourcing eine angemessene Sicherheit bieten.

OPS.3.2.A5 Erstellung eines Sicherheitskonzepts für die Outsourcing-Dienstleistung (B)

Die Anbietenden von Outsourcing MÜSSEN für ihre Dienstleistungen ein Sicherheitskonzept erstellen. Für individuelle Outsourcing-Vorhaben MÜSSEN zusätzlich spezifische Sicherheitskonzepte erstellt werden, die auf den Sicherheitsanforderungen der Nutzenden von Outsourcing basieren. Das Sicherheitskonzept für das jeweilige Outsourcing-Vorhaben SOLLTE jedem und jeder Nutzenden von Outsourcing vorgelegt werden. Das Sicherheitskonzept der Anbietenden von Outsourcing und dessen Umsetzung SOLLTE zu einem gesamten Sicherheitskonzept zusammengeführt werden. Anbietende und Nutzende von Outsourcing MÜSSEN gemeinsam Sicherheitsziele erarbeiten und diese dokumentieren. Es MUSS außerdem eine gemeinsame Klassifikation für alle schutzbedürftigen Informationen erstellt werden. Darüber hinaus MÜSSEN die Anbietenden von Outsourcing regelmäßig überprüfen, ob das Sicherheitskonzept umgesetzt wurde.

OPS.3.2.A6 Regelungen für eine geplante und ungeplante Beendigung eines Outsourcing-Verhältnisses (B)

Es MÜSSEN Regelungen getroffen werden, wie verfahren wird, wenn Outsourcing-Verhältnisse geplant oder ungeplant beendet werden. Es MUSS festgelegt werden, wie alle Informationen, Daten und Hardware der Nutzenden von den Anbietenden von Outsourcing zurückgegeben werden. Anschließend MÜSSEN die verbleibenden Datenbestände der Nutzenden von Outsourcing nach Ablauf der gesetzlichen Vorgaben zur Datenaufbewahrung sicher gelöscht werden. Dies MUSS durch die Anbietenden von Outsourcing dokumentiert werden. Ferner SOLLTE überprüft werden, ob die Zugangs-, Zutritts- und Zugriffsrechte für die Nutzenden von Outsourcing aufgehoben wurden, nachdem das Outsourcing-Verhältnis beendet wurde.

3.2. Standard-Anforderungen

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

OPS.3.2.A7 Bereitstellung der ausgelagerten Dienstleistung durch multiple Sub-Dienstleistende (S)

Werden Prozesse von Anbietenden von Outsourcing weiter an Sub-Dienstleistende verlagert, SOLLTEN die Anbietenden von Outsourcing mehrere qualifizierte Sub-Dienstleistende zur Verfügung haben, falls Sub-Dienstleistende ausfallen oder kündigen. Dies SOLLTE gemeinsam mit den Nutzenden von Outsourcing dokumentiert werden.

OPS.3.2.A8 Erstellung einer Richtlinie für die Outsourcing-Dienstleistungen (S)

Es SOLLTE eine Richtlinie für das Anbieten von Outsourcing-Dienstleistungen erstellt und in der Institution etabliert werden. Diese SOLLTE das Test- und Freigabeverfahren regeln. Dabei SOLLTE die Weiterverlagerung an Sub-Dienstleistende berücksichtigt werden. Die Richtlinie SOLLTE Maßnahmen berücksichtigen, um Compliance-Risiken bei Anbietenden von Outsourcing sowie bei Sub-Dienstleistenden zu bewältigen.

OPS.3.2.A9 Überprüfung der Vereinbarung mit Nutzenden von Outsourcing (S)

Vereinbarungen mit Nutzenden von Outsourcing hinsichtlich der Angemessenheit der festgelegten Sicherheitsanforderungen sowie sonstigen Sicherheitsanforderungen SOLLTEN in regelmäßigen Abständen und anlassbezogen überprüft werden. Vereinbarungen mit Nutzenden von Outsourcing mit unzureichend festgelegten Sicherheitsanforderungen SOLLTEN nachgebessert werden. Bei veränderter Gefährdungs- oder Gesetzeslage SOLLTEN die festgelegten Sicherheitsanforderungen nachgebessert werden. Alle Änderungen SOLLTEN durch die Anbietenden von Outsourcing dokumentiert werden.

OPS.3.2.A10 Etablierung eines sicheren Kommunikationskanals und Festlegung der Kommunikationspartner (S)

Die Anbietenden von Outsourcing SOLLTEN einen sicheren Kommunikationskanal zu den Nutzenden von Outsourcing einrichten. Es SOLLTE dokumentiert sein, welche Informationen über diesen Kommunikationskanal an den Outsourcing-Partner übermittelt werden. Dabei SOLLTE sichergestellt werden, dass an den jeweiligen Enden des Kommunikationskanals entsprechend Zuständige benannt sind. Dabei SOLLTE regelmäßig und anlassbezogen überprüft werden, ob diese Personen noch in ihrer Funktion als dedizierte Kommunikationspartner beschäftigt sind. Zwischen den Outsourcing-Partnern SOLLTE geregelt sein, nach welchen Kriterien welcher Kommunikationspartner welche Informationen erhalten darf.

OPS.3.2.A11 Etablierung eines Notfallkonzepts (S) [Notfallbeauftragte]

Ein Notfallkonzept SOLLTE in der Institution etabliert sein. In diesem Notfallkonzept SOLLTEN Nutzende von Outsourcing sowie Sub-Dienstleistende berücksichtigt werden.

OPS.3.2.A12 Durchführung einer risikoorientierten Betrachtung von Prozessen, Anwendungen und IT-Systemen (S)

Werden Prozesse, Anwendungen oder IT-Systeme neu aufgebaut und Kunden bereitgestellt, SOLLTEN diese regelmäßig und anlassbezogen risikoorientiert betrachtet und dokumentiert werden. Aus den sich daraus ergebenen Ergebnissen SOLLTEN geeignete Maßnahmen festgelegt werden. Darüber hinaus SOLLTEN die Resultate dazu verwendet werden, um das Informationssicherheitsmanagement weiter zu verbessern.

OPS.3.2.A13 Anbindung an die Netze der Outsourcing-Partner (S)

Bevor das Datennetz der Anbietenden an das Datennetz der Nutzenden von Outsourcing angebunden wird, SOLLTEN alle sicherheitsrelevanten Aspekte schriftlich vereinbart werden. Bevor beide Netze verbunden werden, SOLLTEN sie auf bekannte Sicherheitslücken analysiert werden. Es SOLLTE geprüft werden, ob die Vereinbarungen für die Netzanbindung eingehalten werden und das geforderte Sicherheitsniveau nachweislich erreicht wird. Bevor die Netze angebunden werden, SOLLTE mit Testdaten die Verbindung getestet werden. Gibt es Sicherheitsprobleme auf einer der beiden Seiten, SOLLTE festgelegt sein, wer informiert und wie eskaliert wird.

OPS.3.2.A14 Überwachung der Prozesse, Anwendungen und IT-Systeme (S)

Die für Kunden eingesetzten Prozesse, Anwendungen und IT-Systeme SOLLTEN kontinuierlich überwacht werden.

OPS.3.2.A15 Berichterstattung gegenüber den Nutzenden von Outsourcing (S)

Die Anbietenden von Outsourcing SOLLTEN den Nutzenden von Outsourcing in festgelegten Abständen Berichte über den ausgelagerten Prozess bereitstellen. Es SOLLTE ein Bericht an die Nutzenden von Outsourcing versendet werden, wenn Änderungen am Prozess durch die Anbietenden von Outsourcing oder Sub-Dienstleistenden stattfanden. Dazu SOLLTEN standardisierte Protokolle zur Berichterstattung etabliert werden.

OPS.3.2.A16 Transparenz über die Outsourcing-Kette der ausgelagerten Kundenprozesse (S)

Die Anbietenden von Outsourcing SOLLTEN ein Auslagerungsregister für die in Kundenprozessen eingesetzten Sub-Dienstleistenden führen. Dieses SOLLTE Informationen zu den Sub-Dienstleistenden, Leistungskennzahlen, Kritikalität der Prozesse, abgeschlossenen Verträgen und Vereinbarung sowie Änderungen enthalten. Änderungen am Auslagerungsregister SOLLTEN nachgehalten werden. Das Auslagerungsregister SOLLTE auch die Weiterverlagerungen durch die Sub-Dienstleistenden behandeln. Die Anbietenden von Outsourcing SOLLTEN das Auslagerungsregister regelmäßig und anlassbezogen überprüfen.

OPS.3.2.A17 Zutritts-, Zugangs- und Zugriffskontrolle (S)

Zutritts-, Zugangs- und Zugriffsberechtigungen SOLLTEN sowohl für das Personal der Anbietenden von Outsourcing als auch für das Personal der Nutzenden von Outsourcing geregelt sein. Ebenfalls SOLLTEN Zutritts-, Zugangs- und Zugriffsberechtigungen für Auditoren und andere Prüfer festgelegt werden. Dabei SOLLTEN nur so viele Rechte vergeben werden, wie für die Tätigkeit notwendig ist.

OPS.3.2.A18 Regelungen für den Einsatz von Sub-Dienstleistenden (S)

Personal der Anbietenden von Outsourcing sowie der Sub-Dienstleistenden SOLLTEN in ihre Aufgaben eingewiesen und über bestehende Regelungen zur Informationssicherheit der Anbietenden von Outsourcing unterrichtet werden. Soweit es gefordert ist, SOLLTEN das Personal der Anbietenden von Outsourcing sowie der Sub-Dienstleistenden nach Vorgaben der Nutzenden von Outsourcing überprüft werden, z. B. durch ein Führungszeugnis. Das Personal der Anbietenden von Outsourcing sowie der Sub-Dienstleistenden SOLLTEN schriftlich dazu verpflichtet werden, einschlägige Gesetze und Vorschriften, Vertraulichkeitsvereinbarungen sowie interne Regelungen einzuhalten. Es SOLLTEN Vertretungsregelungen in allen Bereichen existieren.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

OPS.3.2.A19 Sicherheitsüberprüfung von Beschäftigten (H)

Die Vertrauenswürdigkeit des Personals der Anbietenden von Outsourcing SOLLTE durch geeignete Nachweise überprüft werden. Es SOLLTEN mit den Nutzenden von Outsourcing vertragliche Kriterien vereinbart werden.

OPS.3.2.A20 Verschlüsselte Datenübertragung und -speicherung (H)

Für die Übertragung von Daten von und zu den Nutzenden von Outsourcing sowie die Speicherung SOLLTE mit den Nutzenden von Outsourcing eine sicheres Verschlüsselungsverfahren festgelegt werden. Dabei SOLLTE sich die eingesetzte Verschlüsselungsmethode am Schutzbedarf der Daten orientieren. Die Verschlüsselungsmethode SOLLTE regelmäßig und anlassbezogen auf ihre Funktionsfähigkeit hin überprüft werden.

OPS.3.2.A21 Durchführung von gemeinsamen Notfall- und Krisenübungen (H) [Notfallbeauftragte]

Gemeinsame Notfall- und Krisenübungen mit den Nutzenden von Outsourcing SOLLTEN durchgeführt und dokumentiert werden (siehe DER.4 *Notfallmanagement*). Das Resultat der Übung SOLLTE dazu genutzt werden, um das Notfallkonzept sowie insbesondere die gemeinsamen Maßnahmenpläne zu verbessern. Die Notfall- und Krisenübungen SOLLTEN regelmäßig und anlassbezogen durchgeführt werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) macht in der Norm ISO/IEC 27001:2013 im Kapitel A.15.2 „Steuerung der Dienstleistungserbringung von Lieferanten“ Vorgaben für die Steuerung von Dienstleistenden. In der DIN ISO 37500:2015-08 werden im „Leitfaden Outsourcing“ weiterführende Informationen zum Umgang mit Dienstleistenden aufgeführt.

Des Weiteren wird in der ISO 27002:2021 das Outsourcing-Verhältnis von Kapitel 5.19 bis 5.22 detailliert aufgeführt und spezifiziert somit die Vorgaben der ISO/IEC 27001:2013.

Der „Leitfaden zur Umsetzung rechtlicher Rahmenbedingungen“ des Bundesverbandes Informationswirtschaft Telekommunikation und neue Medien e.V. (Bitkom) führt Informationen zur Thematik „Compliance“ in IT-Outsourcing-Projekten auf und liefert Hilfestellungen zur Umsetzung der rechtlichen Rahmenbedingungen in einem Outsourcing-Verhältnis.

Das National Institute of Standards and Technology (NIST) gibt in der NIST Special Publication 800-53 Anforderungen an Dienstleistende. In einer weiteren Publikation NISTIR 8276 beschreibt NIST die Best-Practices im Risikomanagement einer „Cyber Supply Chain“.

Der BSI-Standard 200-4 Notfallmanagement enthält wichtige Informationen sowie Vorlagen zur Erstellung und Etablierung eines funktionsfähigen Notfallkonzepts.