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.