

Sicherheitsanforderung

Betrieb

Deutsche Telekom Gruppe

Version	4.0
Datum	01.12.2025
Status	Freigegeben

Impressum

Herausgeber
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Deutschland

Dateiname	Dokumentennummer 3.61	Dokumententyp Sicherheitsanforderung
Version 4.0	Stand 01.12.2025	Status Freigegeben
Fachlicher Ansprechpartner Telekom Security psa.telekom.de	Gültigkeitsdauer 01.12.2025 - 30.11.2030	Freigegeben von Stefan Pütz, Leiter SEC-T-TST

Zusammenfassung
Anforderungen für einen sicheren Betrieb von Systemen.

Copyright © 2025 by Deutsche Telekom AG.

Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

Inhaltsverzeichnis

1.	Einleitung	4
2.	Organisatorisches	5
2.1.	Systemverantwortung	5
2.2.	Ansprechpartner	5
3.	Prozesse	6
3.1.	Change-Management	6
3.2.	Inventar und Konfigurations-Management	6
3.3.	Account-Management	7
3.4.	Sicherheitsvorfälle	8
3.5.	Schwachstellen	9
3.6.	Überwachung der Sicherheitseinstellungen	10
3.7.	Sicherheitstests	11
3.8.	Katastrophen-Management	11
3.9.	Wartung und Unterstützung durch Dritte	11
3.10.	Kennungen, Schlüssel und Zertifikate	12
4.	System-Management und Tools	15
4.1.	Administrativer Arbeitsplatz	15
4.2.	System-Management und -Monitoring	15
4.3.	Installation und Konfiguration	16
4.4.	Temporäre Dateien	17
4.5.	Sicherheitssoftware	17
4.6.	Protokollierung	17
4.7.	Kommunikationsbeziehungen	18
4.8.	Wiederherstellbarkeit	19

1. Einleitung

Dieses Dokument wurde auf Basis der im Konzern gültigen Sicherheitsrichtlinien erstellt.

Die Sicherheitsanforderung dient u. a. als Grundlage zur Freigabe im PSA-Prozess. Sie dient darüber hinaus als Umsetzungsempfehlung für Einheiten, die nicht am PSA-Verfahren teilnehmen. Diese Anforderungen müssen bereits während der Planungs- und Entscheidungsprozesse berücksichtigt werden. Bei der Umsetzung der Sicherheitsanforderung ist das jeweils vorrangige nationale, internationale und supranationale Recht zu beachten.

Die Sicherheitsanforderung definiert die wesentlichen betrieblichen und prozessualen/organisatorischen Sicherheitsanforderungen für die Produktionsphase eines Systems. Sie richtet sich insbesondere an die mit dem Betrieb von Systemen beauftragten Organisationen. Sie kann verwendet werden bei der Ausgestaltung von Vereinbarungen zwischen der Fachseite (als Auftraggeber) und dem Betreiber als Auftragnehmer und komplementiert somit die mit Lieferanten von Hardware/Software getroffenen Vereinbarungen zur Informationssicherheit.

Folgende Themen sind mit diesem Dokument nicht oder nicht abschließend abgedeckt:

- Systemaufbau (hierzu siehe technische Sicherheitsanforderungen)
- Physische Sicherheit
- Personelle Sicherheit
- Business Continuity Management
- Notfallmanagement
- Missbrauchserkennung
- Geheimhaltungsanforderungen
- Datenschutzthemen, z. B. Abschluss eines Auftragsverarbeitungsvertrags (AVV)
- Bürokommunikation

2. Organisatorisches

2.1. Systemverantwortung

Req 1	Es muss für jedes System einen Verantwortlichen geben, der dieses in der Betriebsphase verantwortet.
-------	--

Der Systemverantwortliche für den Betrieb (technischer Systemverantwortlicher) klärt die jeweils systembezogene Rollen- und Aufgabenverteilung mit dem Verantwortlichen der beauftragenden Fachseite (fachseitiger Systemverantwortlicher). Gemeinsam tragen sie entsprechend der zwischen ihnen definierten Rollen- und Aufgabenverteilung die Umsetzungsverantwortung insbesondere für folgende betriebliche Aspekte:

- die Umsetzung und Pflege des Datenschutz- und Sicherheitskonzeptes (SDSK),
- die zyklische Prüfung der Einhaltung der Datenschutz- und Informationssicherheits-Vorgaben,
- den Sicherheitsstand aller installierter Software (insbesondere Patchmanagement),
- die zeitgerechte Verfügbarkeit von Sicherheits-Updates durch den Lieferanten/Hersteller,
- die Einhaltung der Sicherheitsvorgaben für eingerichtete Kommunikationsverbindungen,
- die Aktualität und Vollständigkeit der im Inventar hinterlegten Informationen (Systeme und Maschinen),
- das Vorliegen einer Sicherheits- und Datenschutzfreigabe zum Zeitpunkt der Übergabe in den Betrieb,
- das Testen sowie die Pflege vorliegender Notfallpläne,
- die Verpflichtung und Schulung der Nutzer und Dienstleister auf Einhaltung der Sicherheitsvorgaben,
- die Nennung eines Kontaktes, der zu vereinbarten Zeiten sicherheitsbezogene Anfragen entgegennehmen und bearbeiten kann,
- die Absicherung der ordnungsgemäßen Außerbetriebnahme oder Migration des Systems. Dazu gehören ggf. die Archivierung und/oder Löschung von Daten, die Zurücknahme von Zugängen und Netz-Freischaltungen sowie die Aktualisierung der Inventardaten.

Der (technische) Systemverantwortliche ist namentlich benannt und an geeigneter Stelle, typischerweise im Systemverzeichnis der verantwortenden Geschäftseinheit, dokumentiert. Dies gilt auch für Services, die aus einer Cloud bezogen werden.

Motivation: Ohne klare Benennung eines Verantwortlichen besteht die Gefahr, dass sicherheitskritische Maßnahmen nicht oder nicht zeitgerecht getroffen und umgesetzt werden.

ID: 3.61-1/4.0

2.2. Ansprechpartner

Req 2	Es muss eine Kontaktmöglichkeit geben, über die zu den vereinbarten Zeiten sicherheitsbezogene Anfragen zu Systemen entgegengenommen und gemäß Vereinbarung bearbeitet werden.
-------	--

Anfragen zum Sicherheitsstatus (z. B. im Falle eines Sicherheitsvorfalls) und Aufträge für Sicherheitsanpassungen (z. B. Einspielen von Patches) müssen zeitnah gemäß zuvor getroffenen Regelungen bearbeitet werden. Dazu muss ein (personen-unabhängiger) Kontakt definiert sein, der zu den vereinbarten (Support-)Zeiten derartige Anfragen und Aufträge entgegennehmen und entsprechend weiterleiten kann. Üblicherweise ist dies ein Service Desk, der im Idealfall 7x24 erreichbar ist.

Der jeweilige (technische) Systemverantwortliche muss sicherstellen, dass dieser Kontakt benannt ist und in der Lage ist, sicherheitsbezogene Anfragen bearbeiten zu können.

Motivation: Im Fall eines Sicherheitsvorfalls muss schnell und kompetent gehandelt werden können. Zur Vermeidung von Verzögerungen ist ein entsprechender Kontakt unumgänglich.

ID: 3.61-2/4.0

3. Prozesse

3.1. Change-Management

Req 3 Änderungen an Systemen müssen einem vorab definierten Änderungsverfahren unterliegen.

Durch Änderungen dürfen die Datenschutz- und Sicherheitsmaßnahmen eines Systems nicht außer Kraft gesetzt oder in ihrer Wirksamkeit verringert werden. Derartige Änderungen sind daher unter Berücksichtigung des damit verbundenen Risikos abzustimmen. Es muss eine adäquate Autorisierung sowie eine angemessene Dokumentation der Änderungen erfolgen.

Es wird empfohlen, Änderungen vorher zu testen sowie Rollback-Prozeduren vorzubereiten. Die Systemdokumentation muss hinsichtlich der Änderungen angepasst werden.

Neben einem dokumentierten Change Management Prozess wird empfohlen, weitere typische Betriebsprozesse zu implementieren, die eng mit dem Change Management verknüpft sind und zusammen mit diesem einen sicheren Betrieb ermöglichen:

- Configuration Management - Überblick über die System-/IT-Landschaft
- Release Management - Kontrollierte Einbringung neuer Releases und (generell) neuer Systeme
- Incident Management - Bearbeitung von Störungen
- Problem Management - Beseitigung der Ursache von Störungen
- Capacity Management - Bereitstellung angemessener Ressourcen

Falls "Frozen Zones" festgelegt sind, muss definiert sein, ob, und wenn ja, wie notwendige Sicherheitsaktualisierungen während dieser Zeit eingespielt werden. Es muss festgelegt sein, wie die Genehmigung sogenannter "Notfall-Changes" (je nach Typ gegebenenfalls vorab) erfolgt.

Motivation: Unautorisierte Änderungen stellen ein hohes Sicherheitsrisiko dar, insbesondere dann, wenn sicherheitsrelevante Aspekte der Änderung vorab nicht ausreichend bewertet wurden.

ID: 3.61-3/4.0

3.2. Inventar und Konfigurations-Management

Req 4 Alle Komponenten (Maschinen, Server, Netzelemente, ...) müssen bekannt, inventarisiert und je einem System zugeordnet sein, so dass eine eindeutige Verantwortung für jede Komponente definiert ist. Die Zuordnung muss stets aktuell sein.

Mit "Komponenten" sind hier alle sicherheitsrelevanten Bestandteile gemeint (i. d. R. sind das aktive Systemkomponenten wie Server, Firewalls, Router, ..., auch "Maschinen" genannt). Dazu gehören auch gemeinsam genutzte Elemente, z. B. Storage-Systeme. Alle diese Komponenten müssen Systemen zugeordnet sein. Systeme sind wiederum Systemverantwortlichen zugeordnet, so dass über diese Beziehung jederzeit eine eindeutige Verantwortung für jede Komponente gegeben ist. Vor Betriebsaufnahme muss festgelegt werden, welche Bestandteile und welche Informationen über diese Bestandteile zwecks sicherheitstechnischer Beurteilung mindestens in einem solchen Inventar geführt werden müssen. Asset- und Konfigurations-Management sind zudem Bestandteil eines ITIL (IT Infrastructure Library) Prozess-Frameworks, das in vielen Bereichen zum Management von IT-Systemen zum Einsatz kommt.

Jedes System und auch jede Komponente/Maschine muss zudem über einen eindeutigen Kennzeichner verfügen, anhand dessen diese eindeutig identifiziert werden können.

Motivation: Ohne eine Zuordnung zu einem System und damit einem Verantwortlichen ist nicht sichergestellt, dass im Falle eines Sicherheitsvorfalls schnell gehandelt werden kann.

Umsetzungsbeispiel: Zur Umsetzung empfiehlt sich eine zentrale Datenbank (Configuration Management Database, CMDB), die alle Komponenten und Systeme sowie deren Beziehungen zueinander enthält. Diese CMDB bildet dann das Systeminventar und die Maschinenlisten. Die notwendige Granularität und Aktualität kann dabei anhand der Geschäftsrelevanz und dem Systemstatus wie Test/Produktion festgelegt werden.

Telekom Security stellt mit [TASTE-OS](https://tos.telekom.de/) (Telekom Automated Security Testing Engine – Offline Scanner, <https://tos.telekom.de/>) ein Tool für die Inventarisierung, die Erfassung und Bewertung sicherheitsrelevanter Systemkonfigurationen und des Patch-Standes von Maschinen zur Verfügung.

ID: 3.61-4/4.0

Req 5	Es müssen aktuelle Konfigurationsdaten zu jedem System und allen Systemkomponenten erfasst sein, so dass jederzeit eine sicherheitstechnische Bewertung der gesamten Systemlandschaft anhand dieser Daten durchgeführt werden kann.
-------	---

Empfohlen wird der Einsatz einer Configuration Management Database (CMDB), die die Quelle aller (sicherheits-) technischen Informationen darstellt. Diese kann zentral oder auch dezentral (z. B. nach Organisation oder verwalteten Techniken) angelegt sein. Die in der CMDB erfassten Daten werden dabei möglichst automatisiert erhoben, so dass die Aktualität und Korrektheit der Daten gewährleistet ist. Nur wenige Metadaten oder Stammdaten sollen manuell gepflegt werden müssen oder werden aus anderen Systemen ergänzt. Für die automatisierte Erfassung bieten sich herstellereigenspezifische wie auch unabhängige Tools an.

Eine CMDB kann das Systemverzeichnis, die Systemverantwortlichen und Maschinenlisten enthalten. Oder entsprechende Verweise auf andere Tools, die diese Daten beinhalten. Eine CMDB sollte als Datenquelle für möglichst alle Betriebsprozesse die notwendigen Informationen zu den Systemen und Maschinen enthalten. Als zentrale Komponente im ITIL (IT Infrastructure Library) Prozess-Framework ist eine CMDB unverzichtbar.

Sofern erfassbar, sind folgende Informationen zu hinterlegen:

1. Alle Maschinen und Systeme mit eindeutigem Kennzeichner
2. Installiertes Betriebssystem, Software und der Patch-Level
3. IP-Adressen (mit Kennzeichnung interner und/oder externer Erreichbarkeit)
4. Eingerichtete Kommunikationsbeziehungen
5. Zugehörigkeit jeder Maschine zu einem System und damit zu einem Verantwortlichen
6. Hostnamen, DNS-Namen (intern wie extern) und erreichbare URLs
7. Benötigte Lizenzen
8. Schutzbedarf der auf dem System verarbeiteten Daten
9. Maschinentypen (physisch, virtuell, Container, Serverless, ...)
- 10 Information, auf welcher Basis-Infrastruktur oder Cloud das System implementiert ist
- 11 (TLS-)Zertifikate, deren Parameter und Namen, für die sie ausgestellt wurden
- 12 Lieferant und Entwickler des Systems und der Software, inkl. Wartungsinformationen
- 13 7x24 Kontakt für (Security-) Incident Management und Response
- 14 Kritikalitätsfaktor des Systems und die Risikokategorie der Maschinen
- 15 Priorität der Wiederherstellung und welche abhängigen Systeme benötigt werden

Der Stand der Daten in der CMDB muss regelmäßig gegen den realen Stand auf den Maschinen und Systemen gegengeprüft werden.

Motivation: Die Kenntnis des aktuellen Systemzustands ist Voraussetzung für a) Prüfung, ob ein System von einer Schwachstelle oder einem Sicherheitsvorfall betroffen ist, b) zum Auffinden von Maschinen und/oder Komponenten bei Vorliegen einer Schwachstelle und c) zur geregelten Wiederherstellung.

Umsetzungsbeispiel: Telekom Security stellt mit [TASTE-OS](https://tos.telekom.de/) (Telekom Automated Security Testing Engine – Offline Scanner, <https://tos.telekom.de/>) ein Tool für die Inventarisierung, die Erfassung und Bewertung sicherheitsrelevanter Systemkonfigurationen und des Patch-Standes von Maschinen zur Verfügung.

ID: 3.61-5/4.0

3.3. Account-Management

Gefordert wird ein funktionierendes Identity- und Access-Management. Im Einzelnen bedeutet das:

- Es darf keine unautorisierten Zugänge/Zugriffe geben.
- Es dürfen nur benötigte, d. h. im Sinne des Systems autorisierte, Rechte vergeben werden.
- Bei Wegfall von Berechtigungen müssen diese gemäß vorab definierten Fristen zeitnah entzogen werden.
- Es sollte ein zentrales Identitäts- und Accountmanagement-System verwendet werden, das (für Berechtigungen interner Mitarbeiter) an ein entsprechendes HR-System angebunden ist. Zugänge und Abgänge von Mitarbeitern werden so automatisiert erfasst und bearbeitet. Für externe Personen muss eine zuverlässige Datenquelle existieren, oder ein interner Mitarbeiter wird als Pate definiert und verantwortet die erteilten Rechte hinsichtlich Umfang und Zeitdauer.
- Es sollte ein rollenbasiertes Zugangsmodell verwendet werden, das einzelne Rechte gemäß den zu erledigenden Aufgaben in einer Rolle bündelt. Rollen sind idealerweise von min. zwei Personen (für Vertretungen) besetzt.
- Die Berechtigungsvergabe muss nach dem 4-Augen-Prinzip erfolgen.
- Das System muss für die Vergabe von Zugriffen mit weitreichenden Berechtigungen (Administrator) eine Zwei-Faktor-Authentifizierung am Zielsystem unterstützen.
- Der Stand der auf den Systemen vorhandenen Berechtigungen (Ist-Stand) muss regelmäßig (min. alle 12 Monate) gegen den dokumentierten, autorisierten Stand (Soll-Stand) kontrolliert werden; die Accounts selbst müssen der Fachseite zur Prüfung auf den aktuellen Bedarf vorgelegt werden.
- Für Systeme, die nicht an ein zentrales Identity- und Access-Management System angebunden sind, muss spätestens alle 3 Monate eine Prüfung der Berechtigungen durchgeführt werden.
- Die Wirksamkeit des Berechtigungskonzeptes muss stichprobenweise überprüft werden.

Zugänge und Berechtigungen von "Machine-to-Machine"- (M2M) Verbindungen müssen genauso sorgfältig verwaltet werden.

Motivation: Nur durch einen etablierten Prozess ist es möglich, sicherzustellen, dass sowohl neu eingestellte als auch ausscheidende Personen keinen unberechtigten Zugriff erhalten.

Umsetzungsbeispiel: Nutzung eines der zentralen IAM-Systeme, siehe [YAM United - PSA - IAM](#).

ID: 3.61-6/4.0

3.4. Sicherheitsvorfälle

Ein Sicherheitsvorfall ist ein Ereignis, das die Vertraulichkeit, Verfügbarkeit oder Integrität eines Systems oder der darin verarbeiteten Daten derart beeinträchtigt, dass ein Schaden für das Unternehmen entstehen kann oder bereits entstanden ist. Für solche Vorfälle muss festgelegt sein, wie sie erkannt werden, klassifiziert werden, an wen innerhalb welcher Zeit eine Meldung abzugeben ist und wer im Falle einer Eskalation und für Freigaben hinzuzuziehen ist. Die Inhalte solcher Notfallkonzepte müssen allen am Betrieb beteiligten Personen bekannt sein. Gegebenenfalls sind dafür Schulungen für Admins und Systemverantwortliche durchzuführen.

Möglichkeiten zur Erkennung von Sicherheitsvorfällen (nicht vollständig):

- Auffälligkeiten, die ein Sicherheitsinformations- und Ereignis-Management (SIEM) meldet
- Meldungen eines Intrusion Detection Systems (IDS), z. B. Hackerangriff, (d)DoS-Angriff
- Analyse von Logfiles
- Kompromittierung kryptografischer Schlüssel
- Monitoring-Systeme (technische Störung)

- Meldung durch Mitarbeiter oder von Extern

Beispielhafte Meldewege:

- Officer-on-Duty
- Cyber Emergency Response Team (CERT) national oder konzernweit: cert@telekom.de, telefonisch +49 800 DTAG CERT
- Lagezentrum national oder Konzernlagezentrum
- (Fachseitiger) Systemverantwortlicher
- Wenn vereinbart: (interne) Kunden

Überlegungen zu Eskalation und Genehmigungen:

- Verfahren zum Melden des Vorfalls
- Person(en), die Gegenmaßnahmen wie das Herunterfahren von Systemen genehmigt oder entscheidet, dass eine sichere Wiederherstellung aus Backups durchgeführt werden kann
- Erforderliches Management für Eskalationen

Mögliche Gegenmaßnahmen:

- Zur Abwehr eines volumenbasierten Denial-of-Service Angriffes kann das System ADPP (Adaptive dDoS Protection Plattform) verwendet werden (sofern das angegriffene System an das IP2-Netz der DTAG [AS3320] angebunden ist).
- Abschaltung des Systems, je nachdem ob mit dem fachseitigen Systemverantwortlichen vereinbart wurde, ob man die Integrität der Daten schützen will und das System vom Netz nimmt (und es damit nicht mehr vor Kunde verfügbar ist), oder ob man die Verfügbarkeit vor Kunde gewährleisten will mit dem Risiko, dass Daten abfließen, verändert oder gelöscht werden.
- Einrichten von Filtern in Firewalls oder anderen vorgelagerten Systemen.
- Trennung von Netzwerksegmenten vom Internet und/oder dem Corporate Network, um Angriffe zu stoppen und eine weitere Ausbreitung zu verhindern, insbesondere im Falle von Ransomware-Angriffen.

Motivation: Sicherheitsvorfälle müssen schnell und kompetent bearbeitet werden um potenziellen Schaden vom Unternehmen, seinen Mitarbeitern und Kunden abzuwenden.

ID: 3.61-7/4.0

3.5. Schwachstellen

Req 8	Hinweise zu Schwachstellen müssen bewertet werden. Nach Abwägung daraus resultierender Bedrohungen sind, falls erforderlich, Gegenmaßnahmen zu implementieren.
-------	--

Schwachstellen stellen eine Bedrohung für ein System dar, wenn sie ausgenutzt werden können. Daher müssen bekannt gewordene Schwachstellen umgehend dahingehend bewertet werden, ob durch sie eine Bedrohung besteht. Dementsprechend müssen Maßnahmen zur Abwehr oder zur Schadenseindämmung getroffen werden.

Mögliches Vorgehen:

- Benachrichtigungen zu Schwachstellen bei den Herstellern und/oder dem DTAG CERT abonnieren (siehe <https://dcert.de/>)
- Nutzung des Security Operations Center (SOC), das per Monitoring Schwachstellen und Sicherheitsvorfälle entdeckt
- Bedrohung ermitteln anhand der Kritikalität der Schwachstelle, der potenziellen Wirkbreite und des Schutzbedarfes betroffener Systeme

- Gegenmaßnahmen für betroffene System definieren und umsetzen, z. B. betroffene Features deaktivieren, Patches einspielen, Zugriff durch Einsatz von netzbasierten Filtern (Firewalls) unterbinden oder den Dienst außer Betrieb nehmen

Motivation: Öffentlich bekannt gewordene Schwachstellen müssen umgehend auf deren potenzielle Bedrohung hin untersucht und bewertet werden. Als notwendig erachtete Gegenmaßnahmen sind entsprechend zu planen, um Schaden vom Unternehmen fernzuhalten.

ID: 3.61-8/4.0

Req 9	Es muss sichergestellt sein, dass Systeme / Anwendungen gemäß der definierten DT Patch-Policy alle notwendigen Sicherheitsaktualisierungen erhalten.
-------	--

Die Patch-Policy der DT gibt abhängig von der Exposition der Systeme und der Kritikalität von Schwachstellen (basierend auf CVSS-Werten) Behebungszeiten vor.

Es sind regelmäßige Wartungsfenster zum Einspielen der Patches vorzusehen, die auch die "Patch-Days" von Herstellern, z. B. Oracle, Microsoft, IBM berücksichtigen.

Es werden eigene Repository-Server empfohlen, die die Softwarepakete der Hersteller lokal zur Verfügung stellen, und die in der Lage sind, diese Softwarepakete hinsichtlich ihrer Integrität zu prüfen (z. B. die Signatur des Herausgebers), bevor sie auf Systemen installiert werden.

Nach einem Update ist zu prüfen, ob alle Sicherheitseinstellungen weiterhin aktiv sind und keine erhöhten Berechtigungen an Nutzer oder Prozesse vergeben wurden.

Motivation: Systeme mit einem aktuellen Patchstand bieten weniger Angriffsfläche. Ein aktueller Patchstand ist damit ein elementarer Bestandteil eines sicheren Systems.

Umsetzungsbeispiel: Patch-Policy der Deutschen Telekom, siehe [Richtliniendatenbank](#).

ID: 3.61-9/4.0

3.6. Überwachung der Sicherheitseinstellungen

Req 10	Sicherheitsrelevante Einstellungen in der Systemkonfiguration müssen regelmäßig gegen den vereinbarten Soll-Stand geprüft werden.
--------	---

Die Konfiguration der Systeme ist bzgl. Sicherheitseinstellungen auf Veränderungen und Konformität zu den Vorgaben (Soll-Stand) zu prüfen. Dabei sind mehrere Teile zu berücksichtigen: Die Integrität einer Firmware / Hypervisor-Software / des Betriebssystems muss durch eine regelmäßige Prüfung der Systemkonfiguration, idealerweise vor dem Start, sichergestellt werden. Die möglichen Kommunikationsbeziehungen (z. B. Firewall-Freischaltungen) müssen auf unautorisierte Änderungen geprüft werden. Die Sicherheitseinstellungen von Anwendungen sind zu prüfen.

Es muss geregelt sein, wie mit der Entdeckung einer Abweichung umzugehen ist. Besteht der Verdacht auf einen Sicherheitsvorfall sind umgehend entsprechende Stellen zu informieren.

Motivation: Regelmäßige Überprüfungen tragen dazu bei, Fehlkonfigurationen und damit verbundene Sicherheitslecks zeitnah zu entdecken und abzustellen.

Umsetzungsbeispiel: Ein Collector ist zur Erhebung aller relevanten Daten auf allen Systemen ausgebracht und die damit gewonnen Informationen werden gegen Vorgaben und Standards geprüft. Steht ein solcher automatisierter Prozess nicht zur Verfügung muss manuell stichprobenhaft auditiert werden.

Telekom Security stellt mit [TASTE-OS](#) (Telekom Automated Security Testing Engine – Offline Scanner, <https://tos.telekom.de/>) ein Tool für die Inventarisierung, die Erfassung und Bewertung sicherheitsrelevanter Systemkonfigurationen und des Patch-Standes von Maschinen zur Verfügung.

3.7. Sicherheitstests

Req 11	Tests auf Schwachstellen müssen je nach Kritikalität und Bedrohungslage für alle Systeme regelmäßig zumindest auf der "Kundenschnittstelle" durchgeführt werden.
--------	--

Es ist zu unterscheiden zwischen einfachen Tests (automatische Scanner), mit denen alle erreichbaren Systeme zumindest auf der "Kundenschnittstelle" einer Basis-Prüfung unterzogen werden, und systemindividuellen Tests, für die vorab spezifische Testfälle definiert wurden. Dies sind meist tiefergehende Tests, bei denen festgelegt ist, wann und wie oft sie durchgeführt werden können, ohne den Betrieb zu gefährden. Die Prinzipien des "ethischen Hackers" sind bei dieser Art Penetrationstests zu berücksichtigen. Ziel dabei ist, Schwachstellen und Konfigurationsfehler zu finden, bevor diese ausgenutzt werden. Die Testergebnisse werden sicher vor unberechtigtem Zugriff abgelegt.

Der Bestand der zu testenden Systeme, Schnittstellen und Anwendungen wird idealerweise aus der Konfigurationsdatenbank (CMDB) entnommen.

Stehen entsprechende Test-/Referenzanlagen zur Verfügung, sollen neue Releases vor deren Einführung sicherheitstechnisch geprüft werden.

Motivation: Viele Sicherheitslücken lassen sich nur durch regelmäßige Tests (von außen / von Kundenseite) entdecken. Manchmal reichen schon kleine Konfigurationsänderungen an einer Anwendungssoftware, um eine Sicherheitslücke für das System zu generieren. Um diese Lücken ausfindig zu machen, bevor es ein Angreifer tut, sind Tests unabdingbar.

Umsetzungsbeispiel: Telekom Security stellt mit [DTSP](https://dtsp.telekom-dienste.de/) (Deutsche Telekom Scan Plattform, <https://dtsp.telekom-dienste.de/>) ein Tool für vielfältige Sicherheitstests zur Verfügung.

3.8. Katastrophen-Management

Req 12	Falls Notfallpläne / Disaster Recovery Maßnahmen vereinbart wurden, müssen diese gemäß den Vereinbarungen geprüft, getestet und aktualisiert werden.
--------	--

Disaster Recovery (DR)-Strategien müssen regelmäßig auf ihre Wirksamkeit geprüft werden. Dazu gehören Planspiele, Schreibtischtests und Übungen. Die Ergebnisse sind zu dokumentieren und für Verbesserungen der Abläufe zu verwenden. Ein (fachseitiger) Systemverantwortlicher mit DR-Anforderungen muss stets über den Stand der DR-Fähigkeit seines Betreibers informiert sein.

Motivation: Ohne ausreichendes Testen von Notfallplänen liegt im Notfall nicht das notwendige Wissen und die Routine vor, um den Plan effizient und effektiv umzusetzen.

3.9. Wartung und Unterstützung durch Dritte

Req 13	Mit Lieferanten, Service- und Wartungspartnern müssen geeignete Vereinbarungen getroffen werden, um auf bekannt gewordene Schwachstellen, Sicherheitsvorfälle und Systemausfälle reagieren zu können.
--------	---

Bei Sicherheitsvorfällen kann die Mitwirkung des Lieferanten notwendig sein, um eine schnellstmögliche Bearbeitung sicherzustellen. Mit diesem sind Vereinbarungen zu treffen zur zeitnahen Korrektur von Sicherheitsfehlern in der Software, dem Austausch defekter Hardware und gegebenenfalls zu Sonderregelungen für einen Zwischenfall (Disaster Recovery).

Für Supportfälle muss geregelt sein, wie der Versand von Daten, Informationen, Datenträgern oder Geräten an den Support-Partner gesichert erfolgen kann, bzw. wie der Zugriff auf interne Systeme unter Einhaltung der geltenden Sicherheitsanforderungen erfolgt. Der Kontakt und die vereinbarten Support-Zeiten müssen bekannt sein und sind möglichst in der CMDB hinterlegt.

Motivation: Damit ein System in der vorgesehenen Zeit aktualisiert oder wiederhergestellt werden kann, müssen mit den Lieferanten geeignete Liefervereinbarungen getroffen sein.

Umsetzungsbeispiel: Es wird der "Information Security Annex" als Vertragsbestandteil mit dem Lieferanten vereinbart (Abwicklung über Einkauf, siehe [hier](#) im YAM United).

Nutzung des Vulnerability Advisory Service (VAS) des Telekom CERTs, <https://dcert.de/>

ID: 3.61-13/4.0

Req 14	Zugriffe externer Kräfte für Betriebstätigkeiten, Störungsbeseitigung und Wartung müssen kontrolliert erfolgen.
--------	---

Ist ein Fernzugriff für Dritte erforderlich, muss dafür eine Zugangsplattform verwendet werden, die für diese Nutzung freigegeben ist. Es ist sicherzustellen, dass die Zugänge darüber nur kontrolliert erfolgen. Je nach Einzelfall und Vereinbarung kann dazu erforderlich sein:

- Aktivierung erst nach Freigabe durch internen Mitarbeiter
- Aktivierung nur für bestimmte Zeit
- Rücknahme der Aktivierung
- Zielbegrenzung: nur gewünschte Systeme erreichbar
- Logging der Aktivitäten (Command Line / Graphical Interface)
- Session-Timeout kontrollieren
- Auf Anforderung trennen
- Authentifizierung überwachen

Motivation: Kontrollmöglichkeit der durch einen Dritten durchgeführten Änderungen an Systemen sicherstellen.

Umsetzungsbeispiel: Nutzung des "CRD-Portals" der Telekom Technik Deutschland, siehe [hier](#) im YAM United.

ID: 3.61-14/4.0

3.10. Kennungen, Schlüssel und Zertifikate

Req 15	Kryptografische Schlüssel und Zertifikate müssen vor dem definierten Gültigkeitsende erneuert werden.
--------	---

Zertifikate müssen dahingehend überwacht werden, dass sie vor Ablauf (sofern weiterhin benötigt) gemäß einem vorab definierten Prozess ausgetauscht werden. Empfohlen wird, die Gültigkeitsinformation von Zertifikaten in einem Datenbestand einsehen zu können, um rechtzeitig neue ausstellen und verteilen zu können. Zusätzlich ist eine Online-Prüfung vorzunehmen, um den real installierten Stand abprüfen und mit dem Soll-Stand vergleichen zu können.

Je nach Einsatzzweck sind sehr unterschiedliche Gültigkeitsdauern für kryptografisches Material sinnvoll.

Schutzbedürftiges Schlüsselmaterial wie symmetrische Schlüssel (pre shared keys) müssen über einen sicheren Kanal transportiert werden.

Tipp: Zertifikate nicht am 29.2. ausstellen, da deren Ablaufdatum Probleme bereiten kann.

Motivation: Kompromittiertes Schlüsselmaterial kann zu Verlust der Integrität, Vertraulichkeit und Authentizität führen. Abgelaufene Zertifikate führen häufig zu Störungen von Anwendungen.

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Integrität
- Vertraulichkeit

ID: 3.61-15/4.0

Req 16	Zugangsdaten wie Passwörter und kryptografische Schlüssel müssen vor missbräuchlicher Nutzung geschützt werden.
--------	---

Passwörter personenbezogener Accounts dürfen niemals weitergegeben werden.

Für Passwörter technisch bedingter System-Accounts (z. B. root, Oracle-Admin) ist festzulegen und zu dokumentieren

- wer sie kennt,
- wie und wie häufig sie ausgetauscht werden,
- wie sichergestellt wird, dass nach Ausscheiden eines der Berechtigten eine Änderung erfolgt,
- wie ein Zugriff im Notfall durch andere Personen gewährleistet werden kann.

Werden Passwörter oder Kryptografische Schlüssel für Notfallzugänge hinterlegt, müssen diese sicher vor fremdem Zugriff sein (Safe, physisch oder elektronisch). Es muss festgelegt sein, ob nach einem Zugriff darauf ein neues Passwort oder neuer Schlüssel generiert und eingerichtet werden muss. Passwörter für den Zugriff auf privilegierte Konten sind individuell für jedes System und jede Maschine und nach Möglichkeit in einem PAM-System (Privileged Access Management) hinterlegt.

Kryptografisches Material zur ständigen Nutzung muss sicher abgelegt sein und vor Zugriff durch Unberechtigte geschützt werden. So sind z. B. personenbezogene SSH-Keys am besten auf Smartcards gespeichert und mit einer PIN geschützt. Bei SSH-Agent-Forwarding sollte eine Interaktion eingeschaltet werden, so dass niemand unbemerkt von Remote den Schlüssel missbrauchen kann.

Private Schlüssel von TLS(SSL)-Zertifikaten müssen mit minimalen Zugriffsrechten gespeichert sein und mit einer Passphrase geschützt sein, die getrennt vom Schlüssel gespeichert ist. Der Transport sollte, wenn überhaupt, nur verschlüsselt erfolgen.

Motivation: Sicherstellen, dass nur berechtigte Personen Zugriff auf Systeme haben.

ID: 3.61-16/4.0

Req 17	Zugangsdaten, die zur Automatisierung in den Bereichen Entwicklung, Verteilung und Betrieb von Anwendungen genutzt werden, müssen durch einen "Secrets Manager" geschützt werden.
--------	---

Ein "Secrets Manager" versorgt die angeschlossenen Prozesse und Anwendungen mit den erforderlichen Authentisierungsdaten genau dort, wo sie zur Laufzeit benötigt werden. Die Authentisierungsdaten lassen sich leicht aktualisieren und deren Nutzung wird automatisch in den Logs des Secrets Managers erfasst.

Motivation: Die Nutzung eines Secrets Managers reduziert die Exposition der Authentisierungsdaten und verhindert deren Verlust. Die Zugriffsprotokolle schaffen Transparenz im Falle von Sicherheitsvorfällen.

Umsetzungsbeispiel: Beispielhaft seien hier die Produkte HashiCorp Vault, AWS Secrets Manager, Azure Key Vault und Kubernetes Secrets genannt.

ID: 3.61-17/4.0

Req 18	Potenziell kompromittierte Passwörter, Schlüssel oder Zertifikate müssen umgehend deaktiviert und ausgetauscht werden.
--------	--

Besteht der Verdacht, dass ein Passwort, kryptografischer Schlüssel oder Zertifikat in falsche Hände gelangt sind, müssen die damit möglichen Zugänge umgehend gesperrt werden. Ein Wechsel der Authentisierungsdaten ist unter

folgenden Randbedingungen zwingend durchzuführen:

- wenn die Änderung von Startpassworten nicht technisch erzwungen wird,
- wenn der Verdacht besteht, dass Dritte Kenntnis von Authentisierungsdaten erlangt haben,
- wenn im Zuge einer Vorführung Authentisierungsdaten verwendet und so den Teilnehmern bekannt wurden,
- nach Abschluss von Arbeiten (z. B. Arbeiten einer Systemfirma vor Ort), für deren Durchführung Authentisierungsdaten bewusst bekannt gegeben wurden,
- wenn jemandem, z. B. zum Zweck der Indiziensicherung, entsprechende Datenträger (Systemplatten, Magnetbänder) überlassen werden müssen.

Motivation: Um dem Missbrauch einer Zugangs- und Zugriffsberechtigung vorzubeugen, ist ein Wechsel der Authentisierungsdaten nach Bekanntwerden einer Kompromittierung notwendig.

Umsetzungsbeispiel: Zum Entdecken kompromittierter Accounts kann auch der "ID-Alarm" der Telekom Security genutzt werden, siehe <https://digital-schutzpaket-id-alarm.telekom.de/>.

ID: 3.61-18/4.0

4. System-Management und Tools

4.1. Administrativer Arbeitsplatz

Req 19	Die Sicherheit der Arbeitsplätze zur (interaktiven) Administration von Produktionssystemen muss dem Schutzbedarf dieser Systeme genügen.
--------	--

Abhängig vom Schutzbedarf der zu administrierenden Systeme, deren Kritikalität, Größe und allgemein Zumutbarkeit müssen passende Maßnahmen zur Sicherung der Arbeitsplätze getroffen werden, um eine Kompromittierung der Produktionssysteme auf diesem Wege zu vermeiden. Dazu sind pro System, Kunde oder Umgebung geeignete und angemessene Maßnahmen zu wählen. Möglichkeiten für eine Absicherung von Arbeitsplätzen sind:

- Nutzung gesonderter Admin-Arbeitsplätze gänzlich ohne Bürofunktionalität, so genannte "Privileged Access Workstation" (PAW)
- Arbeitsplätze verwenden keinen ungeschützten Zugang zum Internet, dem WWW und zum Lesen von E-Mail
- Kein direkter Zugriff von Office-Arbeitsplätzen (Standard-Bürokommunikation) auf produktive Systeme mit der Rolle eines Administrators
- Nutzung von Jumphosts für Zugriffsreglementierung (ggf. mit Protokollierung bei besonderer Anforderung und entsprechender Vereinbarung)
- Nutzung geeigneter (grafischer) Terminal-Lösungen
- Automatische Zugangssperre: Bei Inaktivität der Arbeitsstation bzw. des Terminals muss ein (kennwort-) geschützter Bildschirmschoner mit Hilfe der betriebssystemeigenen Mechanismen automatisch aktiviert werden (oder manuell früher aktiviert)
- Arbeitsplatz ermöglicht die Nutzung einer 2-Faktor Authentifizierung am Zielsystem
- Dateiübertragung vom/zum System nur über Zwischensysteme mit Malware-Scannern

Potenziell unsichere Funktionen dürfen nicht verwendet werden. So dürfen bei Nutzung eines SSH-Clients lokales Portforwarding, Tunnel oder Gateway-Ports nicht generell aktiviert sein, sondern müssen im Einzelfall kontrolliert freigegeben werden.

Zur Vermeidung von Man-in-the-middle Angriffen muss die Identität des Zielsystems geprüft werden: Beim Login über SSH muss bspw. der SSH-Hostkey geprüft werden. Dazu ist notwendig, dass die Hostkeys in geeigneter Weise bereitgestellt werden. Bei Windows-Logins kann das Remote Desktop Protocol (RDP) ab 6.0 mit Zertifikaten bzw. mit Network Level Authentication (NLA) abgesichert werden. Veraltete Zugangsprotokolle wie Telnet oder FTP bieten keinerlei Möglichkeiten einer zuverlässigen Prüfung des Zielsystems außer der IP-Adresse, da sie keine kryptografische Authentifizierung bieten.

Motivation: Eine Kompromittierung durch eingeschleuste Malware per E-Mail / aus dem Web oder durch nicht-autorisierte Benutzer muss verhindert werden.

ID: 3.61-19/4.0

4.2. System-Management und -Monitoring

Req 20	Für Betriebszwecke zusätzlich installierte Software wie Tools, Monitoring- und Management-Agenten, müssen sicherheitstechnisch geprüft und freigegeben sein.
--------	--

Verwendet ein System standardisierte Systemmanagement/-monitoring Tools, so ist eine Referenz oder "Kundeninformation" zur Nutzung dieser Tools in der Systembeschreibung zu hinterlegen. Werden individuelle Lösungen implementiert, müssen diese in der Systembeschreibung enthalten sein.

Es ist sicherzustellen, dass mit den Tools nur die damit vorgesehenen Aktivitäten durchgeführt werden können, und diese Tools generell nur mit den minimal dafür benötigten Rechten ablaufen. Für durch den Betreiber eigenverantwortlich installierte Tools ist zu beachten:

- Agenten laufen nicht als von außen erreichbare Netzwerkdienste

- Die Richtung des Kommunikationsaufbaus für Agenten hängt von der Vertrauensstellung daran beteiligter Systeme und den zu übermittelnden Daten ab
- Keine Schreibrechte für den User/die Prozesse einer Agenten-Software, die nur Monitoringfunktionen ausführt
- Ausreichende Authentifizierung der Agenten gegenüber dem Management-Server und andersherum
- Tools nur den vorgesehenen Zweck verwenden. So darf bspw. ein Backup-Systeme, das rein für interne Daten/Systeme vorgesehen ist, nicht missbraucht werden, um Daten extern erreichbarer Maschinen zu sichern.

Generell gilt: Weniger ist mehr. Jedes weitere Tool erhöht die Angriffsmöglichkeiten auf das System.

Motivation: Zusätzlich installierte aktive Management- und Monitoring-Software stellt eine potenzielle Bedrohung für jedes System dar. Für die sicherheitstechnische Bewertung eines Systems müssen alle installierten Komponenten bekannt sein und dürfen nicht nach Inbetriebnahme nachträglich ohne Sicherheitsfreigabe installiert werden. System-Management und -Monitoring Software darf nicht zu Zwecken missbraucht werden, für deren Einsatz sie nicht geplant und freigegeben ist.

Umsetzungsbeispiel: Werden zur Fehlersuche Sniffer-Tools wie tcpdump und wireshark benötigt, müssen diese zum einen nicht dauerhaft installiert sein, zum anderen kann die grafische Auswertung auf einem anderen System (einem entsprechenden Arbeitsplatz) erfolgen, so dass auf dem Wirksystem lediglich die Daten erhoben werden.

ID: 3.61-20/4.0

Req 21	Passwörter für den System-Administrator Account (privilegierter Benutzer) müssen auf jeder Maschine individuell sein.
--------	---

Unter Unix/Linux ist der root Account gemeint, unter Windows die Administrator-Accounts. Bei Netzwerk- und Storagekomponenten die entsprechenden User mit den höchsten Berechtigungen. Diese Admin Accounts sollten nur in dem Fall benötigt werden, wenn Benutzer-individuellen Konten nicht ausreichende Berechtigungen gegeben werden können.

Ein Login über das Netz in diese Admin Accounts sollte üblicherweise nicht möglich sein. Im Grunde ist es ein lokaler (Notfall-) Account.

Es ist Aufgabe der Betriebseinheiten, zentral sicherzustellen, dass diese Passwörter in keinem Fall systemübergreifend eingesetzt werden.

Motivation: Erhöhtes Risiko von Kompromittierung: Ein gemeinsames Passwort bedeutet, dass ein Angreifer nur eine Schwachstelle finden muss, um Zugang zu allen Maschinen zu erhalten. Dies erhöht die Wahrscheinlichkeit, dass die gesamte Systemumgebung kompromittiert wird.

Need-to-know: Ein Administrator/eine Administratorin eines Systems darf nur das Wissen besitzen, um die ihm/ihr zugeordneten Systeme zu betreuen. Bei Ausscheiden des Mitarbeiters/der Mitarbeiterin besteht nicht die Gefahr, dass das Wissen über ein zentral, vielfach genutztes Passwort das Unternehmen verlässt.

ID: 3.61-21/4.0

4.3. Installation und Konfiguration

Req 22	Die Integrität und Authentizität verwendeter Software und Konfigurationen müssen sichergestellt werden.
--------	---

Bei der initialen Installation eines Systems, bei späteren Installationsvorgängen und Einspielen von Upgrades/Updates (insb. Patches) ist sicherzustellen, dass es sich um nicht-kompromittierte Original-Software und autorisierte Konfigurationsdateien handelt. Diese müssen daher aus vertrauenswürdigen Quellen verwendet werden.

Vom Hersteller implementierte Authentifikationsmechanismen (meist digitale Signaturen) sind zu verwenden, sofern vorhanden. Heruntergeladene Software (z. B. per TLS authentifiziert) kann häufig gegen auf einem anderen Weg bereitgestellte Checksummen geprüft werden.

Motivation: Sicherstellen der Integrität und Authentizität der installierten Software und verwendeten Konfigurationen.

Umsetzungsbeispiel: Einsatz eigener, überwachter, Repository-Server und Versionsmanagementsysteme (z. B. GIT) wie <https://devops.telekom.de/>.

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Integrität

ID: 3.61-22/4.0

4.4. Temporäre Dateien

Req 23	Von einem Administrator temporär angelegte, schutzbedürftige, Daten müssen umgehend gelöscht, verschlüsselt oder anderweitig gegen unberechtigte Einsichtnahme gesichert werden.
--------	--

Temporäre Dateien können schutzbedürftige Daten enthalten. So enthalten z. B. Sicherungsdateien der Systemkonfiguration oder ein Netz-Mitschnitt, der zur weiteren Bearbeitung auf ein anderes System kopiert werden soll, Daten, die vor unberechtigter Einsichtnahme zu schützen sind. Wenn solche Daten nicht unmittelbar nach deren Erzeugung (sicher) gelöscht werden können oder sollen, muss jeder unberechtigte Zugriff verhindert werden.

Die Speicherung auf mobilen Datenträgern ist aufgrund des hohen Verlustrisikos zu vermeiden. Sollte eine Speicherung dennoch unumgänglich sein, so sind die darauf gespeicherten Daten zu verschlüsseln. Nicht mehr benötigte Daten darauf sind umgehend zu löschen. Die verwendeten Geräte sind - soweit technisch möglich - gegen Verlust/Diebstahl zu schützen.

Motivation: Schutz vor unberechtigter Einsichtnahme Dritter.

ID: 3.61-23/4.0

4.5. Sicherheitssoftware

Req 24	Sicherheitssoftware muss stets aktuell gehalten werden.
--------	---

Zu Sicherheitssoftware zählen u. a. Antivirus-Lösungen (auf Arbeitsplätzen und auf Servern, sofern dort sinnvoll) sowie Intrusion Detection Systeme. Damit diese möglichst viel Schadsoftware und Angriffe erkennen, müssen diese und ihre Konfigurationen, z. B. Signaturen, aktuell gehalten werden. Es ist zu prüfen, ob diese Aktualisierungen erfolgreich durchgeführt werden.

Auch Content-Filter auf (Web-)Proxies, Spam-Filter auf E-Mail-Systemen, sowohl eingehend als ausgehend, und in einer PKI hinterlegte Gültigkeiten von Zertifikaten (Revocation Lists) sind aktuell zu halten.

Motivation: Schad-Software stellt ein großes Risiko dar, da ein Zugriff auf weitere Systeme nicht einfach ausgeschlossen werden kann.

ID: 3.61-24/4.0

4.6. Protokollierung

Req 25	Sicherheitsrelevante Ereignisse müssen an ein zentrales Logging-System weitergeleitet werden.
--------	---

Alle Systeme sind sicherheitstechnischen Bedrohungen ausgesetzt, deren Identifizierung und Analyse nachgelagert möglich sein muss. Dazu müssen alle sicherheitsrelevanten Logdaten aus Betriebssystemen und Anwendungen zentral erfasst werden.

Die Zeitstempel der Logs müssen korrekt sein - einliefernde Systeme benötigen daher eine funktionierende Zeitsynchronisation. Logs sollen in einer einheitlichen Sprache, bevorzugt Englisch, erfasst werden.

Es ist Aufgabe der Betriebseinheiten, zentrale Logserver bereitzustellen und ein dafür angepasstes Logging zu konfigurieren.

Motivation: Nachverfolgung von Events mit zentraler Korrelation aus unterschiedlichen Quellen. Ein unabhängiger Logserver garantiert Analyse nicht kompromittierter Informationen.

ID: 3.61-25/4.0

Req 26	Alle Serverplattformen müssen an eine EDR Lösung angeschlossen werden. Cloud Dienste, Appliances, Infrastrukturkomponenten (Router, Switches, Firewalls, etc.) müssen Logs an ein SIEM weiterleiten.
--------	--

Zur Sicherstellung der Analyse von sicherheitsrelevanten Ereignissen und Erkennung von Bedrohungen auf produktiven Systemen müssen diese in ein Security Monitoring eingebunden werden.

Die Art der Anbindung ist system- bzw. plattformabhängig und erfolgt entweder per Agent an eine Endpoint Protection und Response Lösung (EDR) oder per Logweiterleitung an ein SIEM (Security Information und Event Management).

Grundsätzlich gilt und die Priorisierung ist wie folgt:

1. Es müssen alle Serverplattformen (Unix/Linux/Windows Systeme) an eine EDR Lösung angeschlossen werden. Sollte die Nutzung einer EDR-Lösung technisch nicht umsetzbar sein, nehmen sie bitte Kontakt mit dem Content Engineering and Threat Hunting Squad auf (Kontakt siehe unten).
2. Cloud Dienste, Appliances, Infrastrukturkomponenten (Router, Switches, Firewalls, etc.) müssen Logs an ein SIEM System weiterleiten.
3. Die Anbindung von applikationspezifischen Logs erfolgt basieren auf der Kritikalität der jeweiligen Applikation

Motivation: Es ist wichtig ein solches Securitymonitoring zu etablieren, um Cyberangriffe bzw. Angriffsversuche automatisiert zu erkennen und nachgelagert manuell untersuchen zu können. Wenn Hacker ein Unternehmen angreifen, beschränken sie ihre Aktivitäten nicht auf eine bestimmte Umgebung. Sie greifen Ressourcen in jedem Unternehmensteil und jeder Umgebung mit einer beliebigen verfügbaren Methode an. Um solche verteilten Angriffe schnell erkennen und darauf reagieren zu können, wird eine möglichst unternehmensweite Plattform (SIEM bzw. EDR) benötigt, in der diese Informationen zusammenlaufen, korreliert und ausgewertet werden können. Im Auftrag und für die Deutsche Telekom AG betreibt die Telekom IT (Microsoft Defender EDR) bzw. die Telekom Security (DT SIEM Splunk) ein solches System in Zusammenarbeit mit dem Telekom SOC Bonn und dem Telekom CERT.

Umsetzungsbeispiel: Weitere Umsetzungsbestimmungen, Anleitungen und Hilfen finden Sie im [YAM](#).

ID: 3.61-26/4.0

4.7. Kommunikationsbeziehungen

Req 27	Das Regelwerk aller Kommunikationsbeziehungen muss den aktuellen und dokumentierten Anforderungen entsprechen und nachvollziehbar sein.
--------	---

Eine Kommunikationsmatrix dokumentiert die Kommunikations-Verbindungen zwischen und innerhalb von Systemen. Anhand der Kommunikationsmatrix werden Routingeinträge und Firewall-Freischaltungen durchgeführt. Änderungen müssen dokumentiert werden, so dass die Kommunikationsmatrix immer den aktuellen Zustand widerspiegelt.

Ein Abgleich der real existierenden Verbindungen gegen den dokumentierten Soll-Stand ist regelmäßig durchzuführen. Nicht mehr benötigte Freischaltungen müssen aus Firewalls und anderen filternden (Netzwerk-)Elementen entfernt werden.

Motivation: Nicht mehr benötigte und damit nicht mehr zulässige Kommunikationsmöglichkeiten stellen eine unnötige Bedrohung der Systeme dar.

ID: 3.61-27/4.0

4.8. Wiederherstellbarkeit

Req 28	Ein System und seine Daten müssen nach einem ungeplanten Ausfall gemäß vereinbarter Parameter wiederhergestellt werden können.
--------	--

Es müssen Restore-Tests gemäß Anforderungen und Vereinbarungen durchgeführt werden. Wenn im Laufe der Zeit die Menge der zu sichernden Daten ansteigt, muss weiterhin sichergestellt sein, dass ein Restore innerhalb der vereinbarten Zeit durchgeführt werden kann.

Im Falle einer größeren Störung, bei der mehrere Systeme wiederherzustellen sind, muss dies anhand einer vorher festgelegten Priorisierung und Reihenfolge erfolgen. Dabei ist auch die Sicherung und Wiederherstellung der benötigten Infrastruktur wie Netzwerksysteme zu berücksichtigen und zu testen.

Wurde als Wiederherstellungsmethode Backup (vollständig / inkrementell) gewählt, richten sich Häufigkeit und Tiefe der Backups sowie Art der gesicherten Daten nach dem geforderten Schutzbedarf des Systems; beispielsweise die permanente Spiegelung von Daten auf einen anderen Datenträger an einer anderen Lokation.

Backup-Datenträger sollten in angemessen räumlicher Entfernung stehen bzw. gelagert werden, mindestens jedoch in einem anderen Brandabschnitt. Es ist zu prüfen, ob eine Verschlüsselung und/oder Archivierung der Backup-Daten notwendig ist und wie diese durchgeführt werden kann. Backup-Daten dürfen nur von berechtigten Personen und Systemen abgerufen werden. Es ist zu prüfen, ob ggf. vertrauliche Daten aus dem Backup ausgeschlossen werden müssen (beispielsweise private Schlüssel von TLS-Zertifikaten).

Auf ein klassisches Backup kann verzichtet werden, wenn die Funktionalität des Systems auf andere Art wiederhergestellt werden kann. Sind keine zu sichernden Anwendungsdaten vorhanden, kann das System rein auf Basis von Templates und in einer Konfigurationsdatenbank hinterlegten Informationen neu aufgesetzt werden. Dies kann so weit gehen, ganze Systemumgebungen einschließlich aller Schnittstellen anhand der hinterlegten Konfigurationsdaten neu zu installieren.

Motivation: Backup- und Restore-Möglichkeiten ermöglichen im Schadensfall eine schnelle Wiederaufnahme des Betriebs.

ID: 3.61-28/4.0

Req 29	Alle Systeme müssen über ein lokales Notfall-Konto verfügen.
--------	--

Lokale Konten ermöglichen den Zugriff, wenn das zentrale Authentisierungssystem kompromittiert oder nicht verfügbar ist.

Es muss immer mindestens ein lokaler Administrator-Account so eingerichtet sein, dass man sich in diesen einloggen kann, auch wenn keinerlei Netzwerkverbindungen zu anderen Systemen mehr bestehen. Je nach Art der Komponente können das bspw. Zugänge über lokale Tastatur und Monitor an Servern sein, sogenanntes "Lights-Out Management", serielle Konsolen an Netzwerk- und Spezialhardware oder auch PIN-Codes zur Freigabe lokaler Zugriffe.

Der lokale Zugriff muss so eingerichtet sein, dass stets die Eingabe eines Authentisierungsmerkmals, z. B. eines Passworts, notwendig ist. Diese für den lokalen Zugriff erforderlichen Credentials müssen für jede Komponente individuell sein. Idealerweise sind sie an einer Stelle hinterlegt, auf die auch ohne funktionierende IT zugegriffen werden kann, z. B. ein Tresor. Nicht dafür zugelassen sind IT-Anwendungen, in denen diese Passwörter in Klartext abgelegt sind.

Motivation: Sicherstellen des Zugriffs bei Störungen der Erreichbarkeit zentraler Authentisierungssysteme. Dazu gehören Ransomware Angriffe, Ausfälle des Netzes oder zentraler Identity Systeme. Kleinere Störungen, wie Verlust einer Netz-basierten Multi-Faktor-Authentifizierung, gesperrte Konten oder falsch konfigurierte Richtlinien können ebenso abgemildert werden.

Insbesondere die Authentisierungssysteme selbst müssen einen lokalen Zugang ermöglichen.

ID: 3.61-29/4.0