

Sicherheitsanforderung

Windows Server

Deutsche Telekom Gruppe

Version	10.0
Datum	01.12.2025
Status	Freigegeben

Impressum

Herausgeber
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Deutschland

Dateiname	Dokumentennummer 3.15	Dokumententyp Sicherheitsanforderung
Version 10.0	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
Windows Server

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.	Generelle Systemhärtung	5
2.1.	Installation	5
2.2.	Konfiguration	10
2.3.	Konfiguration (alt)	11
2.4.	Netzwerk	15
3.	Systemaktualisierung	19
4.	Schutz von Daten und Informationen	21
5.	Schutz von Sitzungen	24
6.	Verfügbarkeit und Integrität	26
7.	Authentifizierung und Autorisierung	29
8.	Authentisierungsmerkmal Passwort	40
9.	Protokollierung	46

1. Einleitung

Dieses Dokument wurde auf Basis der Vorgaben aus den 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.

2. Generelle Systemhärtung

2.1. Installation

Req 1	Software und Hardware des Systems müssen von einem Sicherheitsschwachstellen-Support seitens des Herstellers abgedeckt werden.
-------	--

In einem System dürfen nur Software- und Hardware-Produkte eingesetzt werden, für die ein Sicherheitsschwachstellen-Support durch den Hersteller besteht.

Ein solcher Support muss umfassen, dass der Hersteller

- das Produkt kontinuierlich auf eine Betroffenheit von Sicherheitsschwachstellen beobachtet und analysiert,
- über Art, Schweregrad und Ausnutzbarkeit von im Produkt entdeckten Schwachstellen umgehend informiert
- zeitnah Produktaktualisierungen oder wirksame Workarounds zur Behebung der Schwachstellen bereitstellt.

Der Sicherheitsschwachstellen-Support muss für die gesamte Dauer bestehen, in der das betroffene Produkt im Einsatz verbleibt.

Support-Phasen mit eingeschränktem Leistungsumfang

Viele Hersteller bieten für ihre Produkte als Option einen zeitlich ausgedehnten Support an, welcher über die für den allgemeinen Markt vorgesehene Support-Phase hinausgeht, aber oftmals mit Einschränkungen verbunden ist. Einige Hersteller definieren ihren Support grundlegend in Abstufungen, die Einschränkungen schon während der letzten Phase vor dem absoluten Endtermin des regulären Supports enthalten können.

Wird ein Produkt innerhalb von Support-Phasen eingesetzt, die Einschränkungen unterliegen, muss explizit sichergestellt werden, dass diese Einschränkungen die Verfügbarkeit des Sicherheitsschwachstellen-Support nicht beeinträchtigen.

Open Source Software und Hardware

Open Source Produkte werden häufig von freien Organisationen oder Communities entwickelt; entsprechend ist ein vertraglich vereinbarter Sicherheitsschwachstellen-Support unter Umständen nicht verfügbar. Grundsätzlich muss auch hier sichergestellt werden, dass von der Organisation/Community (oder einem offiziell durch diese eingesetzten Dritten) für das betroffene Produkt ein umfassendes Sicherheitsschwachstellen-Management betrieben wird, welches die oben genannten Kriterien erfüllt und als zuverlässig etabliert gilt.

Motivation: Hardware- und Software-Produkte, für die kein vollumfassender Sicherheitsschwachstellen-Support durch den Hersteller besteht, stellen ein Risiko dar. Dies bedeutet, dass ein Produkt nicht ausreichend auf eine Betroffenheit durch weiterentwickelte Angriffsformen oder neu entdeckte Schwächen technischer Umsetzungen geprüft wird. Analog werden bei vorhandenen Sicherheitsschwachstellen in einem Produkt keine Nachbesserungen (z. B. Updates, Patches) bereitgestellt. Hieraus resultiert ein System, dessen Schwachstellen nicht behoben werden können, so dass sie für einen Angreifer ausnutzbar bleiben, um das System zu kompromittieren oder es negativ zu beeinträchtigen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.01-1/9.0

Req 2	Kritische Windows Server Systeme müssen mit einer Windows Server Version im Long-Term Servicing Channel (LTSC) betrieben werden.
-------	--

Ab September 2023 verfügt Windows Server über zwei primäre Releasekanäle, den Langzeitwartungskanal (Long-Term Servicing Channel, LTSC) und den jährlichen Kanal (Annual Channel, AC). Der Long-Term Servicing Channel

bietet einen langfristigen Fokus auf die Bereitstellung eines herkömmlichen Lebenszyklus von Qualitäts- und Sicherheitsupdates, während der Annual Channel häufigere Releases bietet.

Windows Server im Long-Term Servicing Channel werden durch Microsoft 10 Jahre unterstützt (5 Jahre Mainstream Support und 5 weitere Jahre Extended Support).

Ein Release eines Windows Servers im Annual Channel wird durch Microsoft maximal 24 Monate lang unterstützt (18 Monate Mainstream Support und 6 Monate Extended Support), im Regelfall erfolgt ein neues Release alle 12 Monate.

Zusätzlich stellt im Annual Channel ein neues Windows Server Release kein Update dar. Um auf das neue Windows Server Release zu wechseln, muss zwingend eine Neuinstallation durchgeführt werden.

Siehe hierzu: <https://learn.microsoft.com/de-de/windows-server/get-started/servicing-channels-comparison>

Motivation: Um die Verfügbarkeit und die Unterstützung durch Securityupdates längerfristig zu gewährleisten, ist eine Windows Server Version aus dem Long-Time-Service-Channel zu bevorzugen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.15-2/10.0

Req 3	Eingesetzte Software muss aus vertrauenswürdigen Quellen bezogen und auf Integrität geprüft werden.
-------	---

Die auf dem System eingesetzte Software muss aus vertrauenswürdigen Quellen bezogen und vor der Installation auf ihre Integrität geprüft werden.

Diese Anforderung bezieht sich auf sämtliche Arten von Software:

- Firmware sowie Microcode für Hardware-Komponenten
- Betriebssysteme
- Software-Bibliotheken
- Applikationen und Anwendungssoftware
- vorintegrierte Anwendungslösungen, wie z. B. Software Appliances oder Container

sowie weitere Software, die ggf. zum Einsatz kommt.

Vertrauenswürdige Quellen

Als vertrauenswürdige Bezugsquellen gelten allgemein:

- die offiziellen Vertriebs- und Bereitstellungs Kanäle des Herstellers
- dritte Distributoren, sofern sie durch den Hersteller autorisiert und legitimer Bestandteil von dessen Bereitstellungs Kanälen sind
- Internet-Downloads, sofern diese von offiziellen Bereitstellungs-Servern des Herstellers oder autorisierter Distributoren erfolgen

(1) Bietet der Bereitstellungs-Server verschiedene Formen von Downloads an, müssen durch Verschlüsselung bzw. kryptografische Signaturen geschützte Downloads jenen ohne einen solchen Schutz vorgezogen werden.

(2) Sichert der Bereitstellungs-Server die Transport-Schicht mittels kryptografischer Protokolle (z. B. HTTPS, sftp), müssen die zugehörig präsentierten Server-Zertifikate oder Server-Keys/Fingerprints bei jedem Down-

load validiert werden, um die Identität des Bereitstellungs-Servers zu bestätigen; schlägt die Validierung fehl, ist der Download abzubrechen und der Bereitstellungs-Server als nicht vertrauenswürdige Quelle zu bewerten.

Integritätsprüfung

Die Integritätsprüfung soll sicherstellen, dass die erhaltene Software frei von Manipulationen und Schadsoftware-Befall ist. Sofern vorhanden, müssen zur Prüfung die vom Hersteller implementierten Mechanismen verwendet werden.

Valide Mechanismen sind:

- physikalische Siegel bzw. fest aufgebrachte Echtheitszertifikate (bei Bereitstellung der Software auf physikalischen Datenträgern)
- Abgleich von kryptografischen Hash Werten (z. B. SHA256, SHA512) der erhaltenen Software gegen Soll-Werte, die der Hersteller separat benennt
- Prüfung von kryptografischen Signaturen (z. B. GPG, Zertifikate), mit denen der Hersteller seine Software versieht

Zusätzlich ist eine Überprüfung der Software mittels eines Anti-Virus- bzw. Anti-Malware Scanners empfohlen (falls der Hersteller keinen der zuvor erwähnten Integritätsschutz-Mechanismen für seine Software implementiert hat, ist diese Überprüfung verpflichtend).

Erweiterte Integritätsprüfung bei Bezug von Software aus öffentlichen Registries

Öffentliche Registries ermöglichen es Entwicklern, beliebige eigene Software-Projekte zur Nutzung bereitzustellen. Die Bandbreite umfasst sowohl Projekte von namhaften Anbietern mit kontrollierten Entwicklungsprozessen als auch von kleineren Anbietern oder Amateur-Entwicklern.

Beispiele für solche Registries sind:

- Code Registries (z. B. GitHub, Bitbucket, SourceForge, Python Package Index)
- Container Registries (z. B. Docker Hub)

Software aus öffentlichen Registries muss vor dem Einsatz einer erweiterten Integritätsprüfung unterzogen werden. Zusätzlich zu den im vorherigen Abschnitt beschriebenen Bestandteilen der Integritätsprüfung soll die erweiterte Prüfung explizit sicherstellen, dass die Software ihre Funktion tatsächlich wie beschrieben erfüllt, keine inhärenten Sicherheits-Risiken wie etwa gezielt implementierte Malware-Funktionen enthält und nicht von bekannten Sicherheits-Schwachstellen betroffen ist. Sofern die Software direkte Abhängigkeiten zu dritten Software-Projekten aufweist (sog. "Dependencies", sehr typisch in Open Source Software), die zum Einsatz der Software ebenfalls bezogen und installiert werden müssen, sind diese in die erweiterte Integritätsprüfung mit einzubeziehen.

Methoden für eine erweiterte Integritätsprüfung können beispielsweise sein:

- strikte Validierung der Projekt-/Paket-Namen (Vermeidung der Verwechslung mit maliziösen, gezielt nachgeahmten Software-Projekten)
- dynamische Code Analyse / strukturierte Funktionsprüfung in einer Test-Umgebung
- statische Code Analyse mittels eines Linters (z. B. Splint, JSLint, Pylint)
- Untersuchung mittels eines Sicherheitsschwachstellen-Scanners (z. B. Qualys, Nessus)
- Untersuchung mittels eines Container Security Scanners (z. B. JFrog Xray, Harbor, Clair, Docker Scan)
- Untersuchung mittels eines SCA (Software Composition Analysis) Tools bzw. Dependency-Scanners (z. B. OWASP Dependency Check, Snyk)

Die Prüfungsmethoden sind passend zur exakten Form der Software-Bereitstellung (Quellcode, Binaries/Artefakte, Container) auszuwählen und angemessen zu kombinieren.

Motivation: Softwarelieferketten enthalten diverse Angriffsvektoren. Ein Angreifer kann an verschiedenen Stellen ansetzen, um Software zu manipulieren oder gezielt eigene Routinen einzubringen und die Zielumgebung, in der die Software anschließend zum Einsatz gebracht wird, zu schädigen oder unter seine Kontrolle zu bringen. Der Angriff kann auf dem Transport- bzw. Übertragungsweg geschehen oder auch auf die Bereitstellungsquelle selbst ausgeübt werden. Entsprechend erleichtert wird ein Angriff, falls Software nicht über offizielle und kontrollierte Quellen bezogen wird oder eine Integritätsprüfung ausgelassen wird.

Besonderes Risiko zeigt sich für Software, die aus öffentlichen Registries bezogen wird, da diese jedermann für die

Bereitstellung von Software-Projekten offenstehen. Perfide Angriffsmethoden sind inzwischen bekannt, in denen der Angreifer zunächst eine Zeitlang sicherheitstechnisch völlig unauffällige, funktionale Software bereitstellt und sobald diese sich etabliert und eine gewisse Verbreitung gefunden hat, in zukünftigen Versionen gezielt versteckten Schadcode integriert. Andere Methoden setzen auf ähnlich klingende Projektnamen zu weit verbreiteten Bestandsprojekten oder überstimmende Versionsnummern, um manipulierte Software in darauf aufbauende Lösungen zu injizieren.

Umsetzungsbeispiel: Bezug der Software über die offiziellen Bereitstellungs Kanäle des Herstellers. Nach Erhalt der Software umgehend Prüfung auf Integrität mittels kryptografischer Checksummen, wie vom Hersteller bereitgestellt, sowie Freiheit von bekannter Schadsoftware mittels Anti-Malware- / Anti-Virus-Scanner. Ablage der geprüften Software auf einer internen, geschützten Dateiablage und weitere Nutzung (z. B. Rollout auf die Zielsysteme) nur noch von dort.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Modifikation von Daten
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.01-2/9.0

Req 4 Auf dem System darf ausschließlich nur benötigte Software eingesetzt werden.

In den Hersteller-seitig bereitgestellten Installationsroutinen für Software sind oftmals Komponenten oder einzelne Bestandteile der Software als Standard-Installation vorausgewählt, die für den Betrieb und die Funktion eines spezifischen Systems nicht notwendig sind. Hierzu zählen auch Teile einer Software, die als Anwendungsbeispiele (z. B. Default-Web-Seiten, Beispieldatenbanken, Testdaten) mit installiert, aber typischerweise im Anschluss nicht verwendet werden.

Solche Komponenten müssen bei der Installation des Systems gezielt abgewählt (nicht mit installiert) werden oder - falls eine Abwahl während der Installation nicht möglich ist - unmittelbar im Anschluss entfernt werden.

Des Weiteren darf grundsätzlich keine Software auf einem System eingesetzt sein, die für den Betrieb, die Wartung oder die Funktion des Systems nicht erforderlich ist.

Motivation: Schwachstellen in der Software eines Systems sind Einfallstore für Angreifer. Durch die Deinstallation nicht benötigter Komponenten können die potentiellen Angriffsflächen deutlich reduziert werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Nutzung von Diensten oder Ressourcen
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.01-3/9.0

Req 5 Es muss die Windows Server Core Installation verwendet werden.

Windows Server Core unterstützt diverse Server-Rollen, die unter nachfolgend aufgeführten Link eingesehen werden kann. Wenn technisch möglich, sollte Windows Server mit den aufgeführten Server-Rollen als Windows Server Core installiert werden:

- <https://learn.microsoft.com/de-de/windows-server/administration/server-core/what-is-server-core>

Motivation: Windows Server Core ist eine Installationsoption von Windows Server, die die Angriffsfläche signifikant reduziert, da sie keine grafische Benutzeroberfläche und nur die nötigsten Systemdateien und Dienste installiert.

Umsetzungsbeispiel: Bei der Installation von Windows Server mithilfe des Installations-Assistenten kann zwischen den Installationsoptionen „Server Core“ und „Server mit Desktopdarstellung“ gewählt werden.

Bei Server Core ist die standardmäßige grafische Benutzeroberfläche (Desktopdarstellung) nicht installiert. In der Server Core Variante verwaltet man den Server über die Befehlszeile mithilfe von PowerShell, dem Serverkonfigurations-tool (SConfig) oder mittels Remotemethoden.

Der Installations-Assistent listet die folgenden Installationsoptionen auf. In dieser Liste stellen Editionen ohne Desktopdarstellung die „Server Core“-Installationsoptionen dar:

- Windows Server Standard
- Windows Server Standard mit Desktopdarstellung
- Windows Server Datacenter
- Windows Server Datacenter mit Desktopdarstellung

Für Server Core sind die Optionen ohne den Zusatz "mit Desktopdarstellung" auszuwählen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.15-5/10.0

Req 6	Das Windows Server-Betriebssystem muss mit dem Minimum der zum Betrieb erforderlichen Komponenten, Serverrollen und Features installiert sein.
-------	--

Bei Windows Server sind damit die Funktionen und Rollen gemeint, die man über den Server-Manager verwalten kann. Serverrollen stellen Basisdienste bereit und Features erweitern die Serverinstallation um zusätzliche Funktionen. In vielen Fällen sind Serverrollen abhängig von Features oder ergänzen diese optional durch weitere Merkmale.

Weitere Informationen zu den einzelnen Serverrollen:

- [Rollen, Rollendienste und Features, die in Windows Server & Server Core enthalten sind](#)
- [Rollen, Rollendienste und Features, die in Windows Server, aber in Server Core nicht enthalten sind.](#)

Motivation: Jede Windows Server-Komponente bietet eine Angriffsfläche – nicht verwendete und daher nicht installierte Komponenten minimieren die Angriffsfläche. Dadurch wird die Sicherheit erhöht, weil immer nur die Anwendungen, die auch tatsächlich benötigt werden, auf dem Server installiert sind.

Umsetzungsbeispiel: Siehe die Beschreibungen im [Microsoft Artikels "Installieren oder Deinstallieren von Rollen, Rollendiensten oder Features"](#):

- [Installieren von Rollen, Rollendiensten und Features mit dem Assistenten zum Hinzufügen von Rollen und Features](#)
- [Installieren von Rollen, Rollendiensten und Features mit Windows PowerShell-Cmdlets](#)
- [Entfernen von Rollen, Rollendiensten und Features mit dem Assistenten zum Entfernen von Rollen und Features](#)
- [Entfernen von Rollen, Rollendiensten und Features mit Windows PowerShell-Cmdlets](#)

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit

ID: 3.15-6/10.0

Req 7	Es müssen alle Partitionen mit dem New Technology File System (NTFS) betrieben werden.
-------	--

Windows Server bietet aus Gründen der Kompatibilität die Möglichkeit, alternative Dateisysteme zu verwenden. Es

darf nur das Dateisystem NTFS eingesetzt werden. Auch eine Datenpartition, die einem Windows Failover Cluster im SAN zugeordnet ist, muss mit NTFS betrieben werden. Alternativ kann ReFS (Resilient File Systems) für eine Datenpartition verwendet werden, sofern diese die Semantik von NTFS abbildet.

Motivation: Nur NTFS bietet Sicherheitseinstellungen wie beispielsweise Berechtigungen oder Überwachungseinstellungen.

Umsetzungsbeispiel: Während der Windows Server-Installation wird im Regelfall die Option angeboten, das Dateisystem NTFS auszuwählen.

Es gibt zwei Möglichkeiten, ein Laufwerk für die Installation zu partitionieren und das NTFS-Dateisystem auszuwählen: Entweder über die grafische Benutzeroberfläche (GUI) während der Installation durch Auswahl von "Laufwerkoptionen (Erweitert)" und dann "Neu" für die Partitionierung, oder durch die Verwendung des Tools DiskPart in der Eingabeaufforderung mit dem Befehl `format fs=ntfs`.

Methode 1: Über die grafische Benutzeroberfläche (GUI)

1. Vom Windows Server-Installationsmedium booten.
2. Im Installationsassistenten "Benutzerdefiniert (Erweitert)" auswählen.
3. "Laufwerkoptionen (Erweitert)" auswählen.
4. Eine neue System- und Datenpartition erstellen, indem man auf "Neu" klickt, eine Größe festlegt und "Übernehmen" auswählt.
5. Die Partition wird automatisch mit NTFS formatiert: (dies ist die Standardoption)

Methode 2: Über DiskPart (Befehlszeile)

1. Den Server über die Eingabeaufforderung während des Installationsprozesses (z. B. über Shift + F10) starten.
2. `diskpart` eingeben und Enter drücken, um das Tool zu starten.
3. `list disk` eingeben, um die verfügbaren Festplatten anzuzeigen.
4. Mit `select disk <Nummer>` die gewünschte Festplatte auswählen.
5. Mit `create partition primary size=XXX` (XXX durch die gewünschte Größe in MB ersetzen) eine Partition erstellen.
6. Mit dem Befehl `format fs=ntfs label=<Name>` (z. B. `format fs=ntfs label=System`) die Partition mit NTFS formatieren.
7. Mit `assign letter=<Buchstabe>` einen Laufwerksbuchstaben zuweisen.
8. `exit` eingeben, um DiskPart zu verlassen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten

ID: 3.15-7/10.0

2.2. Konfiguration

Req 8	Nicht benötigte Funktionen in der eingesetzten Software und Hardware müssen deaktiviert werden.
-------	---

Während der initialen Installation von Software können zunächst Funktionen standardmäßig aktiviert worden sein, die für den Betrieb und die Funktionalität des konkreten Systems nicht notwendig sind. Funktionen sind meistens ein fester Bestandteil der Software, der nicht einzeln gelöscht oder deinstalliert werden kann.

Solche Funktionen müssen unmittelbar nach der initialen Installation über die Konfigurationseinstellungen der Software deaktiviert werden, so dass sie auch nach einem Neustart des Systems dauerhaft deaktiviert bleiben.

Bereits vor der Auslieferung oder während der initialen Inbetriebnahme sind möglicherweise auch in der Hardware zunächst Funktionen standardmäßig aktiviert worden, die für den Einsatz des konkreten Systems nicht benötigt werden. Solche Funktionen, wie beispielsweise nicht benötigte Schnittstellen, müssen ebenfalls unmittelbar nach der initialen Inbetriebnahme dauerhaft deaktiviert werden.

Motivation: Die Hardware oder Software eines Systems enthält oft aktivierte Funktionen, die nicht genutzt werden. Solche Funktionen können eine unnötige Angriffsfläche für Manipulationen darstellen. Des Weiteren entsteht darüber ein Potential, dass unautorisiert auf Bereiche oder Daten des Systems zugegriffen werden kann.

Umsetzungsbeispiel: [Beispiel 1]

Deaktivierung von Debugging-Funktionen in einer Software, die im Falle der Entstörung genutzt werden, aber während des normalen Betriebs nicht aktiv sein müssen.

[Beispiel 2]

Deaktivierung von ungenutzten Netzwerk-Schnittstellen eines Servers.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Nutzung von Diensten oder Ressourcen
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.01-4/9.0

2.3. Konfiguration (alt)

Ab hier alte Struktur des vorherigen Requirementreleases.

Req 9 Nicht benötigte Dienste müssen deaktiviert werden.

Nach der Installation von Systemen und Softwareprodukten sind häufig herstellerseitig voreingestellte, lokale oder aus dem Netz erreichbare Dienste aktiv, die für den Betrieb und die Funktionalität des konkreten Systems im vorgesehenen Einsatzumfeld nicht erforderlich sind.

Auf einem System dürfen jedoch grundsätzlich nur die tatsächlich benötigten Dienste aktiv sein.

Entsprechend müssen unmittelbar nach der Installation sämtliche auf einem System nicht erforderliche Dienste vollständig deaktiviert werden. Es muss sichergestellt werden, dass diese Dienste auch nach einem Neustart des Systems weiterhin deaktiviert bleiben.

Motivation: Aktive Dienste, die nicht benötigt werden, vergrößern unnötig die Angriffsfläche eines Systems und in unmittelbarer Folge das Risiko einer erfolgreichen Kompromittierung. Dieses Risiko kann zusätzlich nochmals erhöht sein, falls - wie bei nicht benötigten Diensten häufig beobachtet - eine gezielte Betrachtung und Optimierung der Konfiguration hinsichtlich Sicherheit nicht ausreichend stattfindet.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Nutzung von Diensten oder Ressourcen
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.01-5/9.0

Req 10 Die Erreichbarkeit von aktivierten Diensten muss eingeschränkt werden.

Ein bereitgestellter Dienst muss grundsätzlich auf allen Schnittstellen des Systems vollständig deaktiviert werden, über die eine Erreichbarkeit des Dienstes für den ordnungsgemäßen Betrieb des Systems nicht erforderlich ist. Die Deaktivierung ist primär durch eine entsprechende Konfiguration des Dienstes bzw. Betriebssystems umzusetzen. In Fällen, in denen die zu Verfügung stehenden Konfigurationsoptionen eine Deaktivierung auf einzelnen Schnittstellen nicht ermöglichen, darf stattdessen auch ein lokaler Filter ("Host Firewall") auf dem System eingesetzt werden, um Zugriffe auf den Dienst über nicht erforderliche Schnittstellen zu blockieren.

Die Erreichbarkeit eines Dienstes über die erforderlichen Schnittstellen muss zudem auf legitime Kommunikationspartner eingeschränkt werden. Die Einschränkung ist durch eine entsprechende Konfiguration des Dienstes bzw. Be-

triebssystems oder mittels eines lokalen Filters ("Host Firewall") umzusetzen. Alternativ darf diese Aufgabe an ein netzseitiges Filterelement ausgelagert werden, sofern sich das System in einem separaten Netzwerk-Segment befindet und die Kommunikation mit diesem Segment ausschließlich über das netzseitige Filterelement möglich ist.

Motivation: Mittels Deaktivierung von Diensten auf Schnittstellen, über die eine Erreichbarkeit nicht notwendig ist, sowie durch die Einschränkung möglicher Kommunikationspartner, kann die Angriffsfläche, die ein System bietet, stark reduziert werden.

Umsetzungsbeispiel: Ein SNMP-Dienst, über den ein System gemonitort wird, ist ausschließlich auf der dedizierten Management-Netzwerk-Schnittstelle des Systems aktiviert. Über eine Firewall ist zusätzlich reglementiert, dass einzig das legitime Monitoring System der Infrastruktur-Umgebung diesen Dienst erreichen kann.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Nutzung von Diensten oder Ressourcen
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.01-6/9.0

Req 11	Die Berechtigungen von Prozessen, Diensten und Anwendungen müssen auf ein für deren Aufgaben notwendiges Minimum reduziert werden.
--------	--

Die Berechtigungen für Prozesse und Dienste müssen so eingeschränkt werden, dass diese nur Zugriffsrechte auf benötigte Systemressourcen haben. Minimale Zugriffsberechtigungen sind auch für Dateien zu vergeben, die Bestandteil des Betriebssystems oder von Anwendungen sind oder von diesen erzeugt werden (z. B. Konfigurations- und Protokollierungsdateien).

Auch die Ausführung von Anwendungen oder Bestandteile davon müssen mit möglichst niedrigen Berechtigungen erfolgen. Anwendungen sollten nicht mit Administrator- oder Systemberechtigungen ausgeführt werden. Insbesondere sind Mechanismen zu vermeiden, die es Prozessen erlauben während der Laufzeit erhöhte Rechte zu erlangen.

Motivation: Werden einem Prozess zu weitreichende Berechtigungen auf einem System gewährt, kann dieser ggf. auf Daten oder Teile anderer Dienste/Anwendungen zugreifen, deren Einsicht oder Nutzung ihm nicht erlaubt sind. Hierdurch besteht die Möglichkeit der Offenlegung oder Veränderung von vertraulichen Daten oder der Manipulation von Systemdateien. Anwendungen, die über zu weitreichende Berechtigungen verfügen, können von einem Benutzer genutzt werden, um seine eigenen Berechtigungen zu erweitern und damit Zugriff auf Daten und Systemteile zu erlangen, auf die er unter normalen Bedingungen mit seinen Berechtigungen keinen Zugriff hätte.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten

ID: 3.37-6/9.0

Req 12	Es müssen Maßnahmen zur Härtung des System-Kernels aktiviert sein.
--------	--

Implementierung von Kernel-Hardening-Techniken: Diese Methoden modifizieren die Kernelkonfiguration oder das Kernelverhalten, um die Angriffsfläche zu verringern und die Widerstandsfähigkeit gegen Angriffe zu erhöhen. Dazu müssen unnötige Kernel-Funktionen, -Module oder -Dienste deaktiviert oder entfernt werden. Es müssen Sicherheitsfunktionen wie die Randomisierung des Adressraumlayouts (ASLR), Schutz vor Stapelzertrümmerung (SSP) oder Verhinderung der Datenausführung (DEP) aktiv sein.

Motivation: Maßnahmen wie ASLR schützen insbesondere das System vor der Ausführung von schadhaftem Code bei sogenannten Pufferüberläufen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

ID: 3.37-8/9.0

Req 13 Das automatische Starten von Anwendungen auf Wechseldatenträgern muss abgeschaltet werden.

Wechseldatenträger - etwa CD-, DVD-, USB-Sticks oder USB-Laufwerke - dürfen darauf enthaltene Anwendungen nicht automatisch starten.

Motivation: Das automatische Starten von Anwendungen könnte versehentlich Schadsoftware starten.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unbemerkt durchführbare Angriffe

ID: 3.37-9/9.0

Req 14 Das System muss über eine Kennzeichnung verfügen, die eine eindeutige Identifizierung ermöglicht.

Der Hostname und eine IP-Adresse reichen häufig nicht aus, die Identität der Betriebssysteminstanz zweifelsfrei festzustellen. Bei maschineller Kommunikation mit anderen Systemen wird eine zuverlässigere Prüfung der Identität benötigt, z. B. beim Zugriff auf zentrale Managementsysteme. Hierfür wird für jeden Host individuell generiertes Schlüsselmaterial, i. d. R. ein Zertifikat, benötigt. Dies ist der Standard in Active Directory Umgebungen.

In Fällen, in denen nur eine Identifizierung aber keine Vertraulichkeit oder Integritätsschutz benötigt wird, können Daten zusammen mit einem Unique Identifier gesendet werden, z. B. eine UUID (RFC4122), die auf der Gegenseite bekannt ist.

Motivation: Eine starke Authentifizierung der Maschine anhand von Schlüsseln und/oder Zertifikaten ist gegenüber einer einfachen Identifizierung anhand des Hostnamen oder einer IP-Adresse zu bevorzugen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.37-28/9.0

Req 15 Das Windows Server System muss entsprechend der Härtingsrichtlinien von Microsoft oder "Security Best Practices" konfiguriert sein.

Allgemeine Sicherheitsanleitungen von Microsoft findet sich unter <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/windows-security-baselines> & <https://techcommunity.microsoft.com/t5/microsoft-security-baselines/bg-p/Microsoft-Security-Baselines>

Die Security Benchmarks des Centers for Internet Security (CIS) können ebenfalls angewendet werden: https://www.cisecurity.org/benchmark/microsoft_windows_server/

Motivation: Die Anwendung von Härtingsrichtlinien des Herstellers wie auch von „Security Best Practices“ reduzieren Schwachstellen durch restriktive Konfigurationseinstellungen.

Umsetzungsbeispiel: Umsetzen der unter den Langtext verlinkten Best Practices.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

Req 16	Für das setzen von Securityeinstellungen müssen administrative Templates (ADMX) verwendet werden.
--------	---

ADMX-Dateien sind XML-basierte Dateien, die registrierungsbasierte Einstellungen für den Gruppenrichtlinien-Editor bereitstellen. Sie ermöglichen es, die spezifischen Gruppenrichtlinieneinstellungen auszuwählen, die implementiert werden sollen.

Motivation: Manuelle Konfigurationen von Windows Server über GUI, etc. können insbesondere bei größeren Systemverbünden zu Fehlern führen. Die Konfiguration über zu importierenden administrative Templates hat den Vorteil, das über alle Server die identische Konfiguration ausgerollt wird.

Zusätzlich ermöglicht die Konfiguration über ADMX-Templates ein hohes Maß an Automatisierung, was das automatisierte testen & auditieren mittels CIS-Benchmarks, Taste OS, etc, einschließt.

Umsetzungsbeispiel: Windows Server 2012R2: <https://www.microsoft.com/de-de/download/details.aspx?id=41193>
Windows Server 2016 (beinhaltet 2012R2): <https://www.microsoft.com/de-DE/download/details.aspx?id=53430>
Windows Server 2019 (beinhaltet 2012R2 & 2016): <https://www.microsoft.com/en-us/download/details.aspx?id=57576>
Windows Server 2022 (beinhaltet 2012R2, 2016 & 2019): <https://www.microsoft.com/en-us/download/details.aspx?id=104003>

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

Req 17	Backup-Server und in im Internet exponierte Server dürfen nicht Mitglied einer Active Directory Domäne sein.
--------	--

Sollte das Active Directory übernommen werden, wird durch die Angreifer versucht über das Active Directory erreichbare Backups zu verschlüsseln (Ransomware-Angriffe). Zusätzlich können aus vorher kopierten bzw. extrahierten Daten von Backups Informationen zwecks Erpressung veröffentlicht werden (Double Extortion). Deshalb müssen Backup-Server unabhängig von einer Active Directory Domäne betrieben werden.

Speziell für Backup-Server der Active Directory Domain Controller auf Domain- wie auch Forest-Ebene, müssen die Backup-Server unabhängig von einer Mitgliedschaft einer Domäne betrieben werden.

Motivation: Active Directories bzw. Domain Controller sind besonders im Fokus von Attacken. Dabei wird versucht, das komplette Active Directory zu übernehmen. Sind im Internet exponierte Windows Server Mitglied einer Active Directory Domäne, sind diese ein möglicher Einstieg um das Active Directory zu penetrieren.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

Req 18	NTLM darf nicht als Authentifizierungsprotokoll genutzt werden.
--------	---

NTLM bietet keine Mechanismen zur Verschlüsselung der Authentifizierungssitzung, was die Vertraulichkeit der über-

tragenen Daten gefährdet. Aufgrund dieser Schwäche müssen sichere Authentifizierungsprotokolle wie Kerberos genutzt werden, das stärkere Verschlüsselungs- und Authentifizierungsmethoden bietet.

Motivation: Als Authentifizierungsprotokoll wurde NTLM im Jahre 2000 durch Kerberos ersetzt. Trotz seiner weiten Verbreitung zeigt NTLM erhebliche Sicherheitslücken, die es für Cyberattacken anfällig machen. Die Anfälligkeit von NTLM resultiert primär aus seinem Design, das auf Challenge-Response-Mechanismen basiert, ohne eine ausreichende Verifizierung der Kommunikationspartner zu gewährleisten. Angreifer können verschiedene Techniken wie Pass-the-Hash, Man-in-the-Middle-Angriffe oder Brute-Force-Attacken nutzen, um NTLM-Authentifizierungsprozesse auszunutzen.

Ein Beispiel für Cyberattacken auf NTLM ist der PetitPotam-Angriff, der Schwachstellen im NTLM-Protokoll ausnutzt, um die Kontrolle über Domain Controller in Windows-Netzwerken zu erlangen. Durch Ausnutzung dieser Schwachstelle in Kombination mit AD-CS Relay-Angriffen können Angreifer eine vollständige Domänen-Kompromittierung herbeiführen. Microsoft veröffentlichte Patches, um PetitPotam zu beheben, jedoch bleiben Herausforderungen bestehen, da die Patches nicht alle Probleme lösen und neue Authentifizierungszwangsmethoden aufgetaucht sind, wie DFS-Coerce, die weiterhin Sicherheitsrisiken darstellen.

Umsetzungsbeispiel: Im Pfad "Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Sicherheitsoptionen" die Policies wie folgt konfigurieren:

Einstellung	Wert
Network security: Restrict NTLM: Incoming NTLM traffic	Deny all accounts
Network security: Restrict NTLM: NTLM authentication in this domain	Deny all
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Deny all

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.15-18/10.0

2.4. Netzwerk

Req 19	Der Zugang zur Administration des Betriebssystems muss über eine vom Produktionsnetz unabhängige Schnittstelle erfolgen.
--------	--

Der administrative Zugang auf einen Server oder vergleichbares System darf nicht über die Netzschnittstelle erfolgen, auf der Dienste für Benutzer oder andere Systeme erbracht werden (Produktionsnetz). Weiterhin muss der Zugang auf legitime Systeme eingeschränkt werden. Über diesen Weg kann auch die Anwendungsadministration erfolgen.

Eine Einschränkung des Zugangs kann z. B. durch einen Filtermechanismus, lokale Access-Listen oder eine lokale Firewall realisiert werden. Die Beschränkung ist hierbei möglichst restriktiv auf einzelne IPs oder zumindest kleine IP-Adressbereiche zu setzen.

Motivation: Ein Angreifer kann im Falle eines erfolgreichen Angriffs auf vertrauliche Informationen oder sogar auf das komplette System zugreifen. Durch eine Einschränkung der netzseitigen Erreichbarkeit auf legitimierte Systeme kann der Kreis potentieller Angreifer verkleinert werden. Zudem müssen Systeme immer verwaltet werden können, auch wenn kundenseitige Netze gestört sind.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System

- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.37-10/9.0

Req 20 Administrative Dienste und Zugänge dürfen nur an die Schnittstellen gebunden werden, die für die Administration vorgesehen sind.

Die Dienste zur Administration (interaktiv durch Personen oder Maschinen-Kommunikation, z. B. per SSH, HTTPS, RDP), müssen an die dafür vorgesehene(n) Schnittstelle(n) gebunden werden. Auf Grund der Trennung des Managementverkehrs vom Nutzdatenverkehr, ist dies üblicherweise die IP-Adresse der Management-Schnittstelle. Wird das System - oder Teile davon - über mehrere Schnittstellen administriert, so sind diese Dienste an die entsprechende geringstmögliche Anzahl Schnittstellen zu binden.

Je nach Erfordernissen des jeweiligen Dienstes ist der Zugriff darauf auf wenige, vertrauenswürdige, notwendige Ziel- bzw. Quell-Adressen einzuschränken.

Motivation: Mit Umsetzung dieser Maßnahme ist klar definiert, unter welcher Adresse diese Managementdienste erreichbar sind. Eine eindeutige Adresse ist wichtig für die Implementierung von Filtern und Firewall-Regeln, die den Zugriff auf diese Managementdienste auf legitime Adressen beschränken.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.37-11/9.0

Req 21 Zugänge über das Netz zur Administration des Betriebssystems müssen integritätsgeschützt, verschlüsselt und sicher authentifiziert erfolgen.

Der Zugang darf nur mittels sicherer Protokolle (z. B. SSHv2, HTTPS, SNMPv3) erfolgen. Der Administrator muss sicherstellen, dass jede Netzverbindung zwischen dem Arbeitsplatzsystem oder einem Managementsystem und dem zu verwaltenden Betriebssystem sicher authentifiziert, verschlüsselt und manipulationsgeschützt ist.

Motivation: Überträgt der Administrator Änderungen an Konfigurationseinstellungen über unverschlüsselte oder unsichere Verbindungen, besteht die Gefahr, dass Unberechtigte durch Abhören Erkenntnisse gewinnen (Konfigurationseinstellungen, Zugangskennungen, etc.), die das Ausnutzen von Schwachstellen begünstigen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Abstreiten von durchgeführten Aktionen

ID: 3.37-12/9.0

Req 22 Falls sich Dienste nicht durch Konfiguration auf die minimal erforderlichen Schnittstellen beschränken lassen, muss ein lokaler (Paket-)Filter die Erreichbarkeit reglementieren.

Manche Software lässt sich nicht auf bestimmte Schnittstellen binden. Ein lokaler Paketfilter oder ein TCP Wrapper stellen sicher, dass Dienste, insbesondere Management-Dienste, nur an den erforderlichen Schnittstellen erreichbar sind.

Motivation: Paketfilter sind ein effektiver Schutz, um einen Missbrauch von Diensten aus anderen Netzen zu verhindern.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System

- Unberechtigte Nutzung von Diensten oder Ressourcen
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.37-3/9.0

Req 23 Falls es keine alternative Firewall für das System gibt, muss die Windows Server Firewall zum Filtern nicht benötigter Ports konfiguriert sein.

Die Windows Firewall filtert den TCP/IP-Datenverkehr anhand verschiedener TCP/IP-Attribute (etwa TCP-Port, Quell- und Zieladresse) und verhindert so unerwünschten Datenverkehr. Der Einsatz der Windows Server Firewall erübrigt sich, falls man den Windows Server in einem ohnehin durch eine Firewall geschützten Internet-Protokoll (IP)-Teilnetz betreibt oder eine Software-Firewall eines Drittherstellers nutzt, die die gleichen Filterregeln anwendet.

Motivation: Eine durch die Server des Teilnetzes gemeinsam genutzte Komponente kann das Filtern des TCP/IP-Datenverkehrs durchführen. Dies ist beispielsweise dann möglich, wenn mehrere Datei- und Druckserver eines Internet-Protokoll (IP)-Teilnetzes in einem Verbund zusammengefasst sind, der für die gleichen Arbeitsplatzsysteme Dienste zur Verfügung stellt. Es ist auch zugelassen, dass die Windows Firewall TCP/UDP-Ports filtert und eine zusätzliche Komponente Teilnetze filtert, die eine Verbindung herstellen dürfen.

Der Einsatz von Filterregeln unterbindet effektiv unerwünschten Datenverkehr, und erschwert somit gegebenenfalls auch die unkontrollierte Ausbreitung von Schad-Software.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit

ID: 3.15-23/10.0

Req 24 Die IPv4- und IPv6-Adressen aller Schnittstellen eines Servers müssen fest konfiguriert sein.

IP-Adressen, auf denen Dienste angeboten werden, dürfen nicht durch äußere Einflüsse verändert werden können, auch nicht bei einem erzwungenen Reboot. Eine automatische Zuweisung von IP-Adressen, z. B. mittels DHCPv4/v6 oder IPv6-Autokonfiguration, ist nur dann zulässig, wenn sie nach initialer Vergabe der Adresse(n) abgeschaltet oder anderweitig abgesichert wird. IPv6 Router Advertisements müssen ignoriert werden.

Es wird empfohlen den Host-Anteil der IPv6-Adressen zufällig zu bilden, da auf Grund des sehr großen Adressbereiches von IPv6 ein Auffinden von Systemen für einen Angreifer durch Scans sehr aufwändig ist.

Motivation: Ein Angreifer im gleichen Netzsegment kann durch vorgetäuschte DHCP-/RA-Pakete den Netzverkehr auf seinen Server umleiten (Man-In-The-Middle) und so die gesamte Kommunikation abhören.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Störung der Verfügbarkeit

ID: 3.37-24/9.0

Req 25 Netzfunktionen im Betriebssystemkern, die für den Betrieb als Server nicht benötigt werden, müssen abgeschaltet werden.

Wird IPv6 nicht benötigt, so ist es zu deaktivieren. Ein Server braucht nicht zu routen, daher muss die Routing-Funktion abgeschaltet sein. Ebenso muss das Antworten auf Broadcast ICMP Pakete abgeschaltet sein. Diese und weitere Netzfunktionen sollten normalerweise bereits im Auslieferungszustand korrekt gesetzt sein.

Motivation: Die Router-Funktion kann missbraucht werden, eingehende Pakete an andere angeschlossene Netze zu routen. Dies wird durch diese Maßnahme verhindert.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 3.37-7/9.0

Req 26	Es muss ausschließlich das TCP/IP-Protokoll installiert und verwendet werden.
--------	---

Administratoren sollten alternative Netzwerkprotokolle deinstallieren beziehungsweise deaktivieren.

Motivation: Alternative Netzwerkprotokolle sind weniger weit verbreitet und werden meist nicht mehr weiter entwickelt. Zudem stellen einige ein Risiko dar, so ermöglicht NetBIOS das Auffinden von potentiellen Schwachstellen erleichtern und lässt sich für Angriffe verwenden. Außerdem kann ein aktiviertes NetBIOS über TCP/IP, insbesondere in verteilten Umgebungen, zu einer deutlichen Reduktion der Antwortzeiten führen.

TCP/IP ist das Standard-Netzwerkprotokoll des Windows Server-Betriebssystems. Web-Anwendungen benötigen die NetBIOS-Erweiterung zu TCP/IP nicht.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.15-26/10.0

3. Systemaktualisierung

Req 27	Bekannte Schwachstellen in der Software oder Hardware des Systems müssen behoben oder gegen Missbrauch abgesichert werden.
--------	--

Vor der Installation einer Software- oder auch Hardware-Komponente muss überprüft werden, ob bereits Schwachstellen in der einzusetzenden Version gefunden und veröffentlicht wurden. Sollte die entsprechende Komponente von einer Schwachstelle betroffen sein, darf sie nicht installiert oder verwendet werden. Eine Ausnahme hiervon sind Komponenten, für die bereits eine Maßnahme zum Beheben der Schwachstelle wie z. B. ein Patch, ein Update oder ein Workaround vom Hersteller zur Verfügung gestellt wurde. In diesem Fall muss diese Maßnahme auf dem System umgesetzt werden.

Hinweis: Für das Management von Schwachstellen ist ein kontinuierlicher Prozess für den kompletten Life-Cycle des Systems notwendig, um auftretende Schwachstellen zeitnah beheben zu können.

Motivation: Die Veröffentlichung von Schwachstellen erhöht das Risiko einer erfolgreichen Ausnutzung durch einen Angreifer. Dies wird oftmals dadurch begünstigt, dass detaillierte Informationen und Werkzeuge, die eine Ausnutzung der Schwachstelle möglich machen, veröffentlicht werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Störung der Verfügbarkeit
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.37-16/9.0

Req 28	Falls erforderlich, müssen benötigte, aktivierte, Lizenzen zur Sicherstellung von Sicherheits-Updates für das System hinterlegt sein.
--------	---

Motivation: Einige Hersteller von Betriebssystemen lizenzieren ihre Produkte und fordern den Erwerb von Lizenzen. Diese ermöglichen den Zugriff auf (Sicherheits-) Updates. Ohne Update-Möglichkeiten darf ein System nicht betrieben werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.37-17/9.0

Req 29	Das Betriebssystem muss über eine Endpoint Detection and Response (EDR) Lösung verfügen, die an eine zentrale Security Incident Detection und Response Lösung angebunden ist.
--------	---

Das Betriebssystem muss eine aktuelle Endpoint Detection and Response (EDR) Lösung einsetzen. Eine EDR-Lösung sammelt sicherheitsrelevante Aktivitätsdaten von Prozessen und wertet diese zentral aus. Alarmer können aus maliziosen Verhalten von Prozessen erzeugt werden oder auch durch eine bestimmte Signatur (wie klassische Virens Scanner). Das EDR muss dabei an eine zentrale Security Incident Detection und Response Lösung angebunden sein, so dass Alarmer und Meldungen 7/24 unter Berücksichtigung von Security überwacht werden und Incident Prozesse zeitnah angestoßen werden. Zusätzlich ist es über eine zentrale Konsole möglich, direkt auf verdächtiges Programmverhalten zu reagieren. Das Betriebssystem bzw. der Client kann beispielsweise isoliert oder der maliziose Prozess beendet werden. Darüber hinaus wird eine Übersicht der Schwachstellen aller eingesetzten Betriebssysteme an eine zentrale Stelle geleitet.

Motivation: Normale Virens Scanner verlassen sich rein auf Signaturen, während eine EDR-Lösung auch nach Anomalien im Prozessverhalten sucht. Signaturen haben dabei den Nachteil, dass für neue Virenvarianten erst neue Signaturen geschrieben werden müssen, bevor sie erkannt werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Störung der Verfügbarkeit

ID: 3.37-18/9.0

Req 30	Ein Windows Server-Betriebssystem muss vor Ende des Extended Supports auf ein Betriebssystem im Mainstream Support migriert werden.
--------	---

Motivation: Durch den Hersteller nicht mehr unterstützte Betriebssystemversionen enthalten Designfehler, kritische Fehler und Sicherheitslücken. Solche Lücken sind bekannt und lassen sich mit der Absicht ausnutzen, Viren oder ähnliche Schad-Software in den Server einzuschleusen oder den Server zu missbrauchen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.15-30/10.0

4. Schutz von Daten und Informationen

Req 31	Falls sich das System nicht in einem abgesicherten Raum mindestens der Schutzklasse "hoch" (SK3) befindet, müssen das BIOS und, sofern vorhanden, andere lokale Management-Zugänge vor nicht autorisierten Zugriffen geschützt werden.
--------	--

Die Schutzklassen (SK) sind in der Sicherheitsanforderung "Physische Sicherheit" (Anlage zur Konzernrichtlinie "Sicherheit", siehe <https://richtlinien.telekom.de/>) definiert. Rechenzentren erfüllen in der Regel die Anforderungen nach SK3.

Servers, die öffentlich oder in Räumlichkeiten von Kunden installiert sind, müssen besonders vor unautorisiertem Zugriff und Veränderungen geschützt werden: Es müssen die Einstellungen des BIOS' gegen Auslesen und Manipulation geschützt werden. Sind weitere Zugriffsmöglichkeiten auf die Systemkonfiguration möglich, z. B. durch Intel AMT, iLO, LOM u. ä., müssen diese ebenso geschützt werden. Bei Verwendung eines Passworts muss dieses exklusiv für den einzelnen Server sein und darf keine Rückschlüsse auf ein Unterscheidungsmerkmal des Servers ermöglichen.

Das BIOS muss so konfiguriert sein, dass sich darüber ausschließlich das vorgesehene Betriebssystem von der dafür vorgesehenen Partition starten lässt.

Motivation: Das Ändern von BIOS-Einstellungen kann Angriffe begünstigen. Da beispielsweise dezentrale Technikräume selten einen Zugangsschutz zu Servern bieten, könnten Angreifer beim Starten des Servers im BIOS – ohne den beschriebenen Passwortschutz – die Startreihenfolge der Datenträger verändern. So ließe sich ein alternatives Betriebssystem starten, das die Sicherheitsmechanismen des implementierten Betriebssystems umgeht.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten

ID: 3.37-20/9.0

Req 32	Falls sich das System nicht in einem abgesicherten Raum mindestens der Schutzklasse "hoch" (SK3) befindet, müssen verwendete Datenträger vollständig verschlüsselt werden.
--------	--

Die Schutzklassen (SK) sind in der Sicherheitsanforderung "Physische Sicherheit" (Anlage zur Konzernrichtlinie "Sicherheit", siehe <https://richtlinien.telekom.de/>) definiert. Rechenzentren erfüllen in der Regel die Anforderungen nach SK3.

Als Datenträger gelten insbesondere alle in den Systemen befindliche Festplatten und Flash-Speicher.

Motivation: Der Zutritt zu Geräten, die außerhalb von Rechenzentren mit geschützten Zugängen betrieben werden, ist verhältnismäßig einfach möglich. Damit lassen sich dort vorhandene Datenträger leicht entwenden.

Umsetzungsbeispiel: Bei Windows Server 2008 kann der Administrator die Laufwerksverschlüsselung mittels BitLocker und Schlüsselspeicherung auf einem TPM aktivieren.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten

ID: 3.37-21/9.0

Req 33	In Ausgaben und Meldungen dürfen keine Informationen über interne Strukturen des Systems preisgegeben werden.
--------	---

Informationen über die internen Strukturen eines Systems einschließlich der dort verwendeten Komponenten und ent-

sprechende Implementationsdetails gelten grundsätzlich als schutzbedürftig.

Im Allgemeinen betrifft dies Informationen über

- Produktnamen und Produkt-Identifizierer implementierter System-Komponenten
- eingesetzte Betriebssysteme, Middleware, Backend-Software, Software-Bibliotheken und interne Applikationen sowie deren Software-Versionen
- installierte Service-Packs, Patches, Hotfixes
- Seriennummern von Komponenten sowie hinterlegte Produkt-Lizenzen
- Datenbankstrukturen

Typische Beispiele für Ausgaben und Meldungen, in denen eine Preisgabe solcher System-Informationen potenziell auftreten kann:

- Anmelde-Fenster und -dialoge
- Fehlermeldungen
- Statusausgaben
- Banner von aktiven Netzwerk-Diensten
- System-Protokolle und Log Dateien
- Debug-Protokolle, Stack Traces

Soweit es technisch umsetzbar ist, ohne die Funktion und den Betrieb des Systems zu beeinträchtigen, muss die Ausgabe betroffener System-Informationen grundsätzlich deaktiviert sein.

Ein Zugriff auf betroffene System-Informationen darf nur dazu autorisierten Benutzern des Systems möglich sein. In der Regel ist der Kreis autorisierter Benutzer auf Administratoren und Betreiber des Systems zu beschränken. Ebenfalls zulässig ist ein Zugriff für autorisierte Monitoring- und Inventarisierungs-Systeme innerhalb der Einsatzumgebung.

Eine zulässige Ausnahme dieser Einschränkungen besteht für spezifische einzelne System-Informationen, deren Preisgabe für die vorgesehene Funktion des Systems in Verbindung mit dritten Systemen technisch zwingend erforderlich ist; beispielsweise die Präsentation unterstützter Protokolle und deren Versionen während der initialen Parameter-Aushandlung in Sitzungs-Aufbauten zwischen einem Client und einem Server.

Motivation: Informationen über die internen Strukturen eines Systems können von einem Angreifer genutzt werden, um Angriffe auf das System äußerst effektiv vorzubereiten. Beispielsweise kann ein Angreifer aus der Software-Version eventuell bekannte Schwachstellen eines Produktes ableiten, um diese gezielt während des Angriffs auf das System auszunutzen.

Umsetzungsbeispiel: [Beispiel 1]

Deaktivierung der Anzeige des Produktnamens und der installierten Version in den ausgelieferten Fehler-Webseiten eines eingesetzten Web-Servers.

[Beispiel 2]

Entfernung des Produktnamens und des zugehörigen Versions-Strings aus dem Login-Banner eines eingesetzten SSH Servers.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.01-9/9.0

Req 34	Schutzbedürftige Daten müssen bei der Übertragung sowie Speicherung gegen unberechtigte Einsichtnahme und Veränderung geschützt werden.
--------	---

Schutzbedürftige Daten müssen bei der Übertragung sowie bei der Speicherung angemessen geschützt werden. Au-

thentisierungsdaten wie Passwörter, PINs, Zertifikate und kryptografisches Schlüsselmateriale sind in jedem Fall gegen unberechtigte Einsichtnahme und Manipulation zu schützen. Dies betrifft sowohl die Speicherung als auch die Übertragung. Es ist darauf zu achten, dass vertrauliche Daten auch bei temporärer Speicherung (z. B. in einem Temp-Ordner) nicht ungeschützt abgelegt werden.

Dateien, die für die Funktionalität eines Systems notwendig sind, müssen vor Manipulationen geschützt werden. Dies ist notwendig, da die Integrität des kompletten Systems gefährdet sein kann, falls eine unberechtigte Veränderung solcher Dateien möglich ist. Ein Beispiel für den Schutz solcher Dateien sind kryptographische Verfahren (Signaturen, Hashes) zur Validierung der Manipulationsfreiheit von Firmware-Images, Patches, Treibern und Kernel-Modulen.

Schreibzugriff auf Dateien, die mit Systemprivilegien ausgeführt werden, muss auf Benutzer mit Systemprivilegien beschränkt werden. Andere Benutzergruppen dürfen keine Möglichkeit haben, an diesen Dateien Änderungen vorzunehmen. Dies muss insbesondere für Start-/Stopp-/Logfilerotationsskripte beachtet werden.

Bei der Übertragung von schutzbedürftigen Daten dürfen keine Netzwerkprotokolle verwendet werden, die auf Grund mangelnder Sicherheitsfunktionen als unsicher zu bewerten sind. Beispiele hierfür sind: SSLv3, SSHv1, FTP, Telnet, SNMPv1 und 2c. Im Falle solcher Protokolle muss eine neuere Version oder eine sicherere Alternative verwendet werden.

Motivation: Werden schutzbedürftige Daten nicht gegen eine unautorisierte Einsichtnahme und Veränderung geschützt, kann ein Angreifer dies beispielsweise bei der Übertragung über ein Netz ausnutzen, um Daten mitzuschneiden oder während der Übertragung zu manipulieren. Ein Beispiel hierfür ist das Mitschneiden von Benutzernamen und Passwörtern bei der Administration eines Systems über das Klartextprotokoll Telnet. Die Speicherung von Daten ohne einen adäquaten Schutz auf einem System kann dazu führen, dass ein unautorisierter Benutzer solche Daten kopieren oder auch verändern kann. Ein Beispiel hierfür ist das Auslesen von Passwörtern, die unverschlüsselt auf einem System gespeichert sind.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten

ID: 3.37-19/9.0

5. Schutz von Sitzungen

Req 35 Sitzungen müssen gegen eine unautorisierte Übernahme ("Session Hijacking") geschützt werden.

In Schnittstellen, die Funktionen für Sitzungen zum System bereitstellen, müssen technische Maßnahmen implementiert werden, die verhindern, dass die Sitzung eines legitimen Benutzers von einem nicht autorisierten Dritten übernommen und weitergeführt werden kann.

Ein derartiger Schutz kann beispielsweise durch die Umsetzung einer für das spezifische System sinnvollen Kombination aus den folgenden Optionen erreicht werden:

- Auf der Transportschicht: Verwendung des TCP-Protokolls (mit dessen Sequenz-Nummern) und entsprechenden Filterlisten
- Auf der Sitzungsschicht: Verwendung des TLS-Protokolls
- Auf der Applikationsschicht: Aushandlung eines zufälligen geheimen Sitzungsschlüssels zwischen Sender und Empfänger zwecks Autorisierung allen Sitzungsverkehrs (z. B. Session-ID, Session Cookie, Session Token)
- Nutzung kryptographischer Verfahren zum Schutz von Sitzungsschlüsseln vor Ausspähung oder Veränderung

Motivation: Ungeschützte Sitzungen können potenziell von einem Angreifer gekapert und weitergeführt werden, um darüber im Kontext des betroffenen Benutzers unberechtigte Zugriffe auf das System auszuüben.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen

ID: 3.01-16/9.0

Req 36 Das System muss es Benutzern ermöglichen, sich von ihrer laufenden Sitzung abzumelden.

Das System muss über eine Funktion verfügen, die es dem angemeldeten Benutzer ermöglicht, sich jederzeit abzumelden. Die Wiederaufnahme einer abgemeldeten Sitzung darf nicht ohne erneute und erfolgreiche Authentifizierung des Benutzers möglich sein.

Motivation: Ein Benutzer muss die vollständige Kontrolle über von ihm aufgebaute Sitzungen behalten, um jederzeit situationsgerecht seinen Zugriff auf ein System zu beenden und damit über diesen Zugriff exponierte Daten und Funktionen schützen zu können. Zudem muss der Benutzer davon ausgehen können, dass durch ihn gezielt beendete Sitzungen nicht im Anschluss durch unberechtigte Dritte wieder aufgenommen und weitergeführt werden können.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen

ID: 3.01-17/9.0

Req 37 Sitzungen müssen nach einer dem Verwendungszweck angepassten Zeit der Inaktivität automatisch beendet werden.

Es ist notwendig, dass Sitzungen auf einem System nach einer vorgegebenen Zeit der Inaktivität automatisch beendet

werden.

Aus diesem Grund muss ein Time-Out für Sitzungen gesetzt werden. Der hier zu wählende Zeitraum richtet sich nach der Verwendung des Systems und ggf. nach der physischen Umgebung. So ist beispielsweise der Time-Out für eine Anwendung, die in einer ungesicherten Umgebung genutzt wird, kürzer (wenige Minuten) zu wählen als der Time-Out für eine Anwendung, die von Betriebsmitarbeitern für System-Monitoring-Aufgaben in einem zugangsgeschützten Bereich genutzt wird (60 Minuten und länger).

Motivation: Für eine offene, aber ungenutzte Sitzung besteht ein Risiko, dass ein nicht legitimer Benutzer diese unbemerkt übernimmt und weiterführt, um im Namen des betroffenen Benutzers einen nicht autorisierten Zugriff auf das System und enthaltene Daten auszuüben.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen

ID: 3.01-18/9.0

6. Verfügbarkeit und Integrität

Req 38 Das System muss sich gegen Überlastsituationen schützen und berechenbar bleiben.

Ein System muss über Schutzmechanismen verfügen, die Überlastsituationen so weit wie möglich verhindern. Insbesondere ist eine partielle oder komplette Beeinträchtigung der Verfügbarkeit des Systems zu vermeiden. Beispiele für mögliche Schutzmaßnahmen sind:

- Begrenzung des pro Prozess/pro Anwendung verfügbaren Arbeitsspeichers
- Begrenzung von CPU-Ressourcen pro Prozess
- Priorisieren von Prozessen

Falls eine Überlastsituation nicht verhindert werden kann muss sich das System berechenbar verhalten. In einem solchen Fall muss sichergestellt sein, dass das System nicht in einen undefinierten und möglicherweise unsicheren Zustand gerät. Dies kann im Extremfall bedeuten, dass ein kontrolliertes Herunterfahren des Systems eher hinnehmbar ist, als ein unkontrolliertes Versagen der Sicherheitsfunktionen und somit ein Verlust des Systemschutzes.

Hinweis: Gegen Angriffe mit hohen Datenraten - den sogenannten Distributed-Denial-of-Service-Angriffen - kann ein System sich alleine nicht schützen. Um solche Angriffe abzuwehren, muss eine (externe) netzbasierte Lösung eingesetzt werden.

Motivation: Angreifer versuchen oftmals Systeme mittels Denial-of-Service-Angriffen in eine Überlastsituation zu bringen. Ein erfolgreicher Angriff kann zu einer Beeinträchtigung der Verfügbarkeit oder der Verletzung der Integrität des Systems führen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

ID: 3.37-22/9.0

Req 39 Der TCP/IP-Stack muss gemäß aktuellen Erkenntnissen zur Abwehr von Angriffen gegen das System und seiner Netzverbindungen implementiert und konfiguriert sein.

Typische Angriffe gegen den TCP/IP-Stack dürfen die Stabilität und Integrität des Systems nicht gefährden. Dazu gehören Angriffe wie SYN-Attacken, Hijacking von TCP-Verbindungen, Ping-of-Death. Entsprechende Kerneigenschaften und -parameter sind dazu auf für den geplanten Systemeinsatz als für das jeweilige Betriebssystem sicher angemessene, Parameter zu konfigurieren. Dazu gehört bspw. IP-Pakete mit nicht benötigten Optionen oder Erweiterungs-Headern, z. B. Source Routing, nicht zu verarbeiten. Im Regelfall werden keinerlei IP-Optionen und Erweiterungsheader benötigt.

Allgemein gesagt muss das System robust sein gegen fehlerhafte und unerwartete Datenpakete auf der Netz-Schnittstelle. Die im Folgenden aufgelisteten typischen Implementierungsfehler müssen vermieden werden:

- Fehlende Validierung der Längen übergebener Daten
- Unzutreffende Annahmen über das Format von Daten
- Fehlende Validierung empfangener Daten auf Konformität mit der Spezifikation
- Unzureichende Behandlung von Protokollfehlern in empfangenen Daten
- Unzureichende Begrenzung der Rekursion beim Parsing komplexer Datenformate

Motivation: Vermeidung möglicher Denial-of-Service-Angriffe gegen den TCP/IP-Stack durch Ausnutzung von Schwachstellen oder das Erzwingen einer ressourcen-intensiven Bearbeitung von IP-Paketen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

ID: 3.37-25/9.0

Req 40 Zunehmende (dynamische) Inhalte dürfen Systemfunktionen nicht beeinträchtigen.

Zunehmende Logdaten oder Uploads dürfen die Funktionalität des Systems nicht beeinträchtigen. Es ist sicherzustellen, dass dynamisch wachsende Inhalte nicht die Integrität oder Verfügbarkeit des Systems gefährden.

Motivation: Ein volles Dateisystem könnte das System zum Erliegen bringen.

Umsetzungsbeispiel: Einsatz eigener Dateisysteme für variable Daten, Quotas oder zumindest eine Überwachung des Füllstandes der Dateisysteme.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

ID: 3.37-23/9.0

Req 41 Das System darf keine IP-Pakete verarbeiten, deren Absenderadresse nicht über die Schnittstelle erreicht wird, an der das Paket eingegangen ist.

Der TCP/IP-Stack sieht standardmäßig vor, dass IP-Pakete an einem Interface angenommen werden können, das nicht das eigentliche Ziel des IP-Paketes ist. Notwendig ist dafür lediglich, dass eine Route zur Absenderadresse existiert. In bestimmten Fällen (Cluster, Loadbalancer) ist das ein gewollter Effekt, aber nicht der Standardfall.

Es muss darauf geachtet werden, dass ein Server nicht über eine unnötige Defaultroute verfügt, was z. B. der Fall ist, wenn dieser nur intern verwendet werden.

Motivation: In einer solchen Konstellation handelt es sich i. d. R. um Pakete mit gefälschten Absenderadressen oder einen Fehler im Routing. Das eintreffende Paket muss als nicht vertrauenswürdig verworfen werden.

Umsetzungsbeispiel: Verwendung der Funktion "Reverse Path Filter" (RPF), die dafür sorgt, dass genau solche Pakete verworfen werden.

Microsoft beschreibt hier seine Version des "Reverse Path Filtering", genannt "weak host send behavior" und "weak host receive behavior": [https://docs.microsoft.com/de-de/previous-versions/technet-magazine/cc137807\(v=msdn.10\)](https://docs.microsoft.com/de-de/previous-versions/technet-magazine/cc137807(v=msdn.10))

"

FIGURE 4 COMMANDS TO CONFIGURE STRONG AND WEAK SEND AND RECEIVE BEHAVIOR

[...]

```
netsh interface ipv4 set interface [InterfaceNameOrIndex] weakhostsend=disabled
netsh interface ipv4 set interface [InterfaceNameOrIndex] weakhostreceive=disabled
netsh interface ipv6 set interface [InterfaceNameOrIndex] weakhostsend=disabled
netsh interface ipv6 set interface [InterfaceNameOrIndex] weakhostreceive=disabled
```

"

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 3.15-41/10.0

Req 42 Die Verarbeitung von ICMPv4 und ICMPv6 Paketen, die für den Betrieb nicht benötigt werden, muss deaktiviert sein.

Es gibt verschiedene Typen von ICMPv4 und ICMPv6, die in den meisten Netzen nicht verwendet werden, aber ein potentielles Risiko darstellen. Solche Typen müssen deaktiviert oder gefiltert werden.

Hingegen sind folgende ICMP-Typen erlaubt und dürfen genutzt werden:

- Echo Request [Type 8 (v4), Type 128 (v6)]
- Echo Reply [Type 0 (v4), Type 129 (v6)]
- Destination Unreachable [Type 3 (v4), Type 1 (v6)]
- Time Exceeded [Type 11 (v4), Type 3 (v6)]
- Parameter Problem [Type 12 (v4), Type 4 (v6)]
- Packet Too Big [Type 2 (nur v6)]
- Neighbor Solicitation [Type 135 (nur v6)]
- Neighbor Advertisement [Type 136 (nur v6)]

Es besteht die Möglichkeit, dass weitere Typen notwendig sind. Dies ist im Einzelfall zu prüfen. In keinem Fall dürfen die ICMPv4-Typen "Timestamp Reply (14)", "Netmask Reply (18)", "Information Reply (16)" und "Redirect (5)" sowie die ICMPv6-Typen "Router Solicitation" (133), "Router Advertisement" (134) und "Redirect" (137) beantwortet oder verarbeitet werden.

Motivation: ICMPv4 und v6-Pakete können von einem Angreifer genutzt werden, um gezielt Informationen abzufragen, die für die Planung weiterer Angriffe hilfreich sein können. Zudem besteht die Möglichkeit die Verfügbarkeit von betroffenen Systemen zu beeinflussen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.37-27/9.0

7. Authentifizierung und Autorisierung

Req 43	Es muss eine Authentifizierungsmethode verwendet werden, die eine eindeutige Identifizierung der Benutzer ermöglicht.
--------	---

Benutzer müssen eindeutig von einem System identifiziert werden können. Dies wird typischerweise dadurch erreicht, dass für jeden Benutzer ein individuelles Benutzerkonto verwendet wird.

Es können rollenbasierte Konten (funktionales Konto) genutzt werden, bei denen individuelle Authentisierungsmerkmale (z. B. Zertifikate, kryptografische Schlüssel) verwendet werden. Einsatzzweck ist bspw. das Administrationskonto für eine Datenbank oder einen Webserver, da hier üblicherweise mehrere Administratoren Zugang zu diesem Account benötigen.

Sogenannte Gruppenkonten, bei denen die Authentifizierung mit einem allen Beteiligten bekannten "Geheimnis", z. B. Passwort, erfolgt, dürfen nicht verwendet werden.

Sogenannte Maschinenkonten werden zur Identifizierung und Autorisierung von Systemen untereinander oder von Anwendungen auf einem System genutzt und können nicht einer einzelnen Person zugewiesen werden. Solche Konten müssen individuell pro System oder pro Anwendung vergeben werden. Hierbei ist sicherzustellen, dass eine missbräuchliche Nutzung nicht möglich ist. Möglichkeiten, dies zu verhindern, sind:

- Konfiguration eines - den Sicherheitsanforderungen entsprechenden - Passwortes, das nur den notwendigen Administratoren bekannt ist.
- Konfiguration des entsprechenden Kontos, so dass dies nur lokal verwendet werden kann und eine interaktive Anmeldung nicht möglich ist.
- Verwendung eines Verfahrens mit öffentlichem und privatem Schlüssel oder Zertifikaten für die Authentifizierung des entsprechenden Benutzerkontos.
- Einschränkung des Zugriffs auf legitimierte Systeme.

Weitere Lösungen sind im Einzelfall auf ihre Verwendbarkeit zu prüfen.

Motivation: Die eindeutige Identifizierung eines Benutzers ist Voraussetzung, um einem Benutzer Berechtigungen zuweisen zu können, die für die Durchführung seiner Aufgaben auf dem System notwendig sind. Nur so kann eine adäquate Zugriffskontrolle auf Daten und Dienste erreicht und der missbräuchliche Zugriff verhindert werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen

ID: 3.37-29/9.0

Req 44	Konten müssen gegen unautorisierte Nutzung durch Verwendung mindestens eines Authentisierungsmerkmals geschützt werden.
--------	---

Alle Benutzer-, Rollen- und Maschinenkonten eines Systems müssen vor missbräuchlicher Nutzung geschützt werden. Hierfür wird typischerweise ein Authentisierungsmerkmal verwendet, dass in Kombination mit dem Kontonamen eine eindeutige Authentifizierung von legitimierten Benutzern ermöglicht.

Authentisierungsmerkmale sind z. B.: Kryptographischer Schlüssel, Token, Passwort, PIN.

Dies bedeutet auch, dass eine Authentifizierung von Benutzern mittels eines unsicheren Parameters nicht zulässig ist. Ausgenommen hiervon sind Attribute, die von einem Angreifer nicht gefälscht oder vorgetäuscht werden können. Um eine höhere Sicherheit zu erreichen, können zwei oder mehr der genannten Möglichkeiten miteinander kombiniert werden (2-Faktor-Authentifizierung).

In Unternehmen der Deutschen Telekom Gruppe, in denen die MyCard oder eine vergleichbare Smartcard verfügbar

ist, ist diese Lösung zu favorisieren.

Motivation: Konten, die nicht entsprechend geschützt sind, können von einem Angreifer genutzt werden, um unrechtmäßig auf ein System und die darauf gespeicherten Daten und Anwendungen zuzugreifen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen

ID: 3.37-30/9.0

Req 45	Die Nutzung von schutzbedürftigen Funktionen des Systems sowie der Zugriff auf interne oder vertrauliche Daten darf nicht ohne vorhergehende Authentifizierung und Autorisierung ermöglicht werden.
--------	---

Die Nutzung von schutzbedürftigen Funktionen des Systems sowie der Zugriff auf Daten, die als intern oder vertraulich eingestuft sind, darf erst nach einer eindeutigen Identifizierung und erfolgreichen Authentifizierung des Benutzers anhand eines Benutzerkontos ermöglicht werden. Ein Benutzerkonto besteht aus einem eindeutigen Benutzernamen und zugehörigen Authentisierungsmerkmalen. Zudem muss verifiziert werden, dass der Benutzer innerhalb der ihm im System zugeordneten Benutzerrolle für den Zugriff auf die betroffenen Funktionen und Daten legitimiert ist.

Eine Ausnahme hiervon sind Funktionen und Daten, die uneingeschränkt öffentlich genutzt werden dürfen; beispielsweise der Bereich einer Web-Seite im Internet, in dem nur öffentliche Informationen bereitgestellt werden.

Beispiele für Funktionen, die eine vorhergehende Authentifizierung erfordern:

- Fernzugriff auf Netzdienste (wie SSH, SFTP, Web-Dienste)
- lokaler Zugriff auf die Management-Konsole
- lokale Nutzung von Betriebssystem und Anwendungen

Diese Anforderung gilt ohne Einschränkung auch für jegliche maschinellen Zugriffe auf das System (Hier erfolgt die Umsetzung in der Regel durch den Einsatz von sogenannten "technischen Benutzerkonten", auch "Machine-2-Machine" oder "M2M"-Konten genannt).

Motivation: Die eindeutige Authentifizierung und Autorisierung von Zugriffen auf ein System sind elementar, um Funktionen und Daten vor Missbrauch zu schützen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen

ID: 3.01-19/9.0

Req 46	Benutzerkonten müssen mit mindestens zwei Authentisierungsmerkmalen aus unterschiedlichen Faktoren geschützt werden.
--------	--

Sämtliche Benutzerkonten des Systems müssen vor einer unberechtigten Nutzung geschützt werden. Dies ist durch Verwendung von Authentisierungsmerkmalen umzusetzen, die eine eindeutige Identifizierung des legitimen Benutzers ermöglichen.

Authentisierungsmerkmale werden in übergeordneten Gruppen, sogenannten "Faktoren", differenziert:

- Faktor WISSEN: "etwas, das nur der legitime Benutzer weiss"
- Faktor BESITZ: "etwas, das nur der legitime Benutzer besitzt"
- Faktor INHÄRENZ: "etwas, das nur der legitime Benutzer ist"

Es müssen mindestens zwei Authentisierungsmerkmale miteinander kombiniert werden.

Diese müssen aus unterschiedlichen Faktoren stammen ("Multi-Faktor-Authentisierung"; kurz: "MFA").

Eine Kombination von Authentisierungsmerkmalen desselben Faktors (Beispiel: zwei unterschiedliche PINs) ist nicht zulässig.

Beispiele für zulässige Authentisierungsmerkmale

- aus dem Faktor WISSEN: PINs, Passphrases (Passwörter*)
- aus dem Faktor BESITZ: Smartcards, FIDO2 Level 2 Security Keys, Device-bound Passkeys, in einem TPM/HSM gespeicherte kryptografische Schlüssel, OTPs (One-Time Passwords) generiert in einer zum Einsatz in der Deutschen Telekom freigegebenen Authenticator App
- aus dem Faktor INHÄRENZ: biometrische Merkmale wie Fingerabdrucke, Iris- bzw. Retina-Scans, Gesichtserkennung

***) Wichtiger Hinweis zum Einsatz von Passwörtern**

Passwörter müssen als Authentisierungsmerkmal strikt vermieden werden.

Sie sind nur dann zulässig, falls sicherere Alternativen nicht umgesetzt werden können.

Grundsätzlich nicht zulässig sind Authentisierungsmerkmale, die leicht gefälscht oder manipuliert werden können.

Dazu gehören:

- Rufnummern und Anrufer-IDs
- IP-Adressen
- geografische Standorte
- VPN-Zugehörigkeiten und Netzwerkinformationen
- Status von Clients, etwa von Arbeitsplatzsystemen oder mobilen Endgeräten

Hinweis zu technischen Benutzerkonten

Für den maschinellen Zugriff eingesetzte technische Benutzerkonten (auch unter dem Begriff "Machine-to-Machine" bzw. "M2M"-Konten bekannt) sind von der Verpflichtung zur Multi-Faktor-Authentisierung ausgenommen, da eine solche dort i.d.R. nicht umsetzbar ist.

Motivation: Benutzerkonten, die nicht über angemessene Authentisierungsmerkmale geschützt sind, können von einem Angreifer missbraucht werden, um unberechtigt auf ein System und die darauf gespeicherten Daten und Anwendungen zuzugreifen. Aufgrund vielfältiger gängiger Angriffsmethoden ist der Schutz von Benutzerkonten durch ein einzelnes Authentisierungsmerkmal mittlerweile als schwach zu bewerten, insbesondere, falls hier das klassische Passwort zum Einsatz kommt. Eine Kombination von Authentisierungsmerkmalen aus unterschiedlichen Faktoren erhöht die Sicherheit für Benutzerkonten signifikant.

Umsetzungsbeispiel: Beispiele für MFA

MFA Kombination	Beschreibung	Anmerkung zur Anwendung
Telekom "myCard" plus PIN-Eingabe	1. Faktor: in Hardware implementiertes Zertifikat ("Besitz") 2. Faktor: PIN ("Wissen")	(keine)

FIDO2 Level 2 Security Key plus Fingerabdruck	1. Faktor: in Hardware gespeicherter Crypto-Schlüssel ("Besitz") 2. Faktor: Biometrisches Merkmal ("Inhärenz")	Die Biometrie-Funktion muss vorab konfiguriert werden, da der Biometrie-Sensor sonst nur als "Ta- ste" funktioniert und somit der 2. Faktor ("Inhärenz") nicht gege- ben wäre.
Device-bound Passkey in WH4B* auf Nucleus PC plus PIN	1. Faktor: in Hardware gespeicherter Crypto-Schlüssel ("Besitz") 2. Faktor: PIN ("Wissen")	(keine)
Device-bound Passkey in Secure Enclave auf iOS Device plus FaceID	1. Faktor: in Hardware gespeicherter Crypto-Schlüssel ("Besitz") 2. Faktor: Biometrisches Merkmal ("Inhärenz")	(keine)
Passwort plus freigegebene OTP App (z. B. MS Authenticator)	1. Faktor: Passwort ("Wissen") 2. Faktor: spezifisch generiertes One Time Password ("Besitz")	Passwörter sind nur dann zulässig, falls sicherere Alternativen nicht umgesetzt werden können. Die Synchronisation der Authentica- tor App über einen Clouddienst sowie das Teilen (z. B. über einen Passwortmanager) des OTP ist nicht zulässig.

*) WH4B: "Windows Hello for Business"

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen

ID: 3.01-20/9.0

Req 47 Privilegierte Benutzerkonten müssen mit mindestens zwei Authentisierungsmerkmalen geschützt werden, die aus unterschiedlichen Faktoren stammen und erhöhte Resilienz gegen Phishing-Angriffe bieten.

Ein privilegiertes Benutzerkonto ist ein Benutzerkonto, welches über erweiterte Berechtigungen innerhalb eines Systems verfügt. Erweiterte Berechtigungen ermöglichen einen Zugriff auf Konfigurationseinstellungen, Funktionen oder Datenbestände, der regulären Benutzern des Systems nicht zu Verfügung steht. In direkter Abhängigkeit zu den besonderen Aufgaben, die mittels eines privilegierten Benutzerkontos innerhalb eines Systems wahrgenommen werden, können die zugewiesenen erweiterten Berechtigungen spezifisch limitiert sein oder einen vollständig uneingeschränkten Systemzugriff umfassen.

Beispiele für privilegierte Benutzerkonten:

- Konten für Administrations-, Wartungs- oder Entstörungsaufgaben
- Konten für Benutzer-Verwaltungsaufgaben (z. B. Anlegen/Löschen von Benutzern; Zuweisen von Berechtigungen; Passwort-Rücksetzungen)
- Konten, die zur Freigabe, Auslösung oder Unterbindung von geschäftskritischen Vorgängen berechtigt sind
- Konten mit Zugriff auf Daten, die im Interesse des DTAG-Konzerns, dessen Kunden oder der Öffentlichkeit als

SCD (Sensitive Customer Data) eingestuft sind

- Konten, die in hohem Umfang auf lt. EU-DSGVO als „personenbezogen“ definierte Daten zugreifen können (z. B. Massenabruf von größeren Teilen oder des vollständigen Datenbestands)

Zum Schutz privilegierter Konten müssen mindestens zwei Authentisierungsmerkmale miteinander kombiniert werden.

Diese müssen aus unterschiedlichen Faktoren ("WISSEN", "BESITZ" oder "INHÄRENZ") stammen.

Eine Kombination von Authentisierungsmerkmalen desselben Faktors ist nicht zulässig.

Mindestens eines der Authentisierungsmerkmale darf nicht anfällig gegenüber Phishing-Angriffen sein.

Bei einem Phishing-Angriff wird der legitime Nutzer trickreich manipuliert, um seine Anmeldedaten dem Angreifer offenzulegen, beispielsweise mittels gefälschter Anmelde-Seiten. Ein Phishing-Angriff kann auch gegen eine Kombination aus mehreren Authentisierungsmerkmalen erfolgen.

Phishing-resiliente Authentisierungsmerkmale verhindern Angriffe anhand ihrer technischen Umsetzung. Diese Authentisierungsmerkmale nutzen kryptographische Verfahren und stellen eine starke Bindung zwischen dem Nutzer, dem Gerät und dem Dienst her. Sie erfordern während der Authentisierung zusätzlich eine manuelle Nutzerinteraktion, die nicht automatisiert werden kann; beispielsweise, einen Fingerabdruck-Scan an einem Hardware Token abzugeben.

Als nicht anfällig gegenüber Phishing-Angriffen gelten

- FIDO2 Level 2 Security Keys
- in Hardware implementierte Zertifikate

Wichtiger Hinweis zum Einsatz von Passwörtern

Passwörter müssen als Authentisierungsmerkmal strikt vermieden werden.

Sie sind nur dann zulässig, falls sicherere Alternativen nicht umgesetzt werden können.

Hinweis zu technischen Benutzerkonten

Für den maschinellen Zugriff eingesetzte technische Benutzerkonten (auch unter dem Begriff "Machine-to-Machine" bzw. "M2M"-Konten bekannt) sind von der Verpflichtung zur Multi-Faktor-Authentisierung ausgenommen, da eine solche dort i.d.R. nicht umsetzbar ist.

Motivation: Privilegierte Benutzerkonten stellen ein erhöhtes Risiko für die Sicherheit eines Systems dar. Kompromittiert ein Angreifer erfolgreich ein solches Benutzerkonto, erhält er weitreichende Berechtigungen, mit denen er das System oder Systemanteile unter seine Kontrolle bringen, die Systemfunktionen stören, verarbeitete Daten einsehen/manipulieren oder geschäftskritische Vorgänge beeinflussen kann. Die Kombination von mehreren Authentisierungsmerkmalen unterschiedlicher Art minimiert das Risiko der Kompromittierung eines Benutzerkontos bereits signifikant, jedoch muss für privilegierte Benutzerkonten in besonderem Maße auf Resilienz gegen Phishing-Angriffe geachtet werden. Die zu beobachtenden Phishing-Angriffe werden zunehmend trickreicher und für Nutzer schwerer zu erkennen, so dass eine Multifaktor-Authentifizierung ohne erhöhte Resilienz gegen Phishing nicht mehr als ausreichend für privilegierte Benutzerkonten zu bewerten ist.

Umsetzungsbeispiel: Beispiele für MFA mit erhöhter Resilienz gegen Phishing-Angriffe

MFA Kombination	Beschreibung	Anmerkung zur Anwendung
Telekom "myCard" plus PIN-Eingabe	1. Faktor: in Hardware implementiertes Zertifikat ("Besitz") 2. Faktor: PIN ("Wissen")	(keine)

FIDO2 Level 2 Security Key plus Fingerabdruck	1. Faktor: in Hardware gespeicherter Crypto-Schlüssel ("Besitz") 2. Faktor: Biometrisches Merkmal ("Inhärenz")	Die Biometrie-Funktion muss vorab konfiguriert werden, da der Biometrie-Sensor sonst nur als "Ta- ste" funktioniert und somit der 2. Faktor ("Inhärenz") nicht gege- ben wäre.
FIDO2 Level 2 Security Key plus PIN-Eingabe	1. Faktor: in Hardware gespeicherter Crypto-Schlüssel ("Besitz") 2. Faktor: PIN ("Wissen")	(keine)

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen

ID: 3.01-21/9.0

Req 48 Benutzerkonten müssen die eindeutige Identifizierung des Benutzers sicherstellen.

Benutzer müssen eindeutig von einem System identifiziert werden können.

Dies wird typischerweise dadurch erreicht, dass für jeden Benutzer ein individuelles Benutzerkonto genutzt wird.

Sogenannte Gruppenkonten, die sich dadurch auszeichnen, dass sie von mehreren Personen gemeinsam genutzt werden, dürfen nicht verwendet werden. Dies gilt uneingeschränkt auch für privilegierte Benutzerkonten. Die meisten Systeme verfügen nach der Grundinstallation zunächst nur über ein einzelnes Benutzerkonto mit administrativen Berechtigungen. Soll das System von mehreren Personen administriert werden, muss jede dieser Personen ein persönliches, individuelles Benutzerkonto verwenden, dem entsprechende administrative Berechtigungen bzw. Rollen zugewiesen sind.

Eine Besonderheit stellen sogenannte technische Benutzerkonten dar. Diese werden für Authentifizierung und Autorisierung von Systemen untereinander oder von Anwendungen auf einem System genutzt und können damit nicht einer konkreten Person zugewiesen werden. Solche Benutzerkonten müssen individuell pro System oder pro Anwendung vergeben werden. Hierbei ist allerdings sicherzustellen, dass eine missbräuchliche Nutzung solcher Benutzerkonten nicht möglich ist.

Möglichkeiten, um eine missbräuchliche Nutzung solcher Benutzerkonten durch Personen zu verhindern, sind:

- Konfiguration eines den Sicherheitsanforderungen entsprechenden Passwortes, dass nur einem kleinstmöglichen Kreis von Administratoren bekannt ist.
- Konfiguration des entsprechenden Benutzerkontos, so dass dieses nur lokal verwendet werden kann und eine interaktive Anmeldung nicht möglich ist.
- Verwendung eines Verfahrens mit öffentlichem und privatem Schlüssel oder Zertifikaten für die Authentifizierung des entsprechenden Benutzerkontos.
- Einschränkung des Zugriffs über ein Netz auf legitimierte Systeme.

Weitere Lösungen sind im Einzelfall auf ihre Verwendbarkeit zu prüfen.

Motivation: Die eindeutige Identifizierung eines Benutzers ist Voraussetzung, um einem Benutzer Berechtigungen zuweisen zu können, die für die Durchführung seiner Aufgaben auf dem System notwendig sind. Nur so kann eine adäquate Zugriffskontrolle auf Daten und Dienste eines Systems erreicht und der missbräuchliche Zugriff verhindert werden. Des Weiteren wird hierdurch ermöglicht, dass Tätigkeiten und Aktionen auf einem System protokolliert und einem Benutzer zugeordnet werden können.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen

ID: 3.01-22/9.0

Req 49	Es darf keine privilegienerweiternde Mechanismen geben, die es ermöglichen, von einem Benutzerkonto aus vollständige Administrator-/Root-Rechte zu erlangen, ohne eine ausreichend starke, erneute, Authentifizierung durchzuführen.
--------	--

Methoden zur Rechte-Erweiterung wie su, sudo und runas bieten eine hohe Gefahr, dass mehr Rechte als benötigt erlangt werden können. Die Anzahl der Exploits in solchen Mechanismen zeigt die hohe Komplexität und Fehleranfälligkeit dieser Lösungen, denen daher nicht vertraut werden kann.

Eine Anmeldung mit erweiterten Rechten muss stets mit zwei Authentisierungsmerkmalen erfolgen.

Motivation: Wenn ein Angreifer ein Konto kompromittieren kann, für das die Möglichkeit einer Privilegiererweiterung eingerichtet ist, besteht die Gefahr, dass er auf weite Teile des Systems und den darauf gespeicherten Daten zugreifen kann.

Umsetzungsbeispiel: Abschalten per se unsicherer privilegienerweiternder Mechanismen, so dass Benutzer sich (erneut) direkt an dem Konto, das für die Arbeiten benötigt wird, anmelden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Abstreiten von durchgeführten Aktionen

ID: 3.37-32/9.0

Req 50	Vordefinierte Authentisierungsmerkmale müssen geändert werden.
--------	--

Nach der Übernahme oder Erstinstallation eines Systems existieren üblicherweise vordefinierte Authentisierungsmerkmale (z. B. Passwörter, SSH Keys, SSL/TLS Zertifikate) im System, wie sie durch Hersteller, Entwickler, Lieferanten oder automatisierte Installationsroutinen vergeben wurden.

Solche vordefinierten Authentisierungsmerkmale müssen unmittelbar nach der Übernahme bzw. Installation des Systems auf neue, individuelle Werte geändert werden.

Motivation: Von Dritten vordefinierte Werte in Authentisierungsmerkmalen können nicht als vertrauenswürdig angesehen werden, da sie kein kontrolliertes Geheimnis darstellen. Betroffene Authentisierungsmerkmale können von Unbefugten dafür missbraucht werden, um auf Systeme zuzugreifen und diese zu kompromittieren. Dieses Risiko ist signifikant erhöht, falls für Authentisierungsmerkmale allgemein bekannte Standard-Werte verwendet werden (z. B. ein Standardpasswort für das Administrator-Benutzerkonto in einem bestimmten Software-Produkt).

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.01-8/9.0

Req 51	Die Berechtigungen von Konten müssen auf ein für deren Aufgaben notwendiges Minimum reduziert werden.
--------	---

Die Berechtigungen von Konten müssen so eingeschränkt werden, dass ein Benutzer nur auf Daten zugreifen und Funktionen nutzen kann, die er im Rahmen seiner Rolle benötigt. Entsprechende minimale Rechte sind auch für den Zugriff auf Dateien, die Bestandteil des Betriebssystems oder von Anwendungen sind, einzurichten.

Motivation: Werden einem Benutzer zu weitreichende Berechtigungen auf einem System gewährt, kann er ggf. auf Daten und Anwendungen zugreifen, deren Einsicht oder Nutzung ihm in seiner Rolle nicht erlaubt sind. Hierdurch besteht die Möglichkeit der Offenlegung oder Veränderung von vertraulichen Daten oder der Manipulation von Systemdateien.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.37-34/9.0

Req 52	Es müssen zur technischen Verwaltung von Domänen-Mitgliedern Active Directory-Konten verwendet werden.
--------	--

Windows Server-Betriebssysteme sind meist Mitglieder einer Active Directory-Domäne, die eine zentrale Verwaltung von Benutzerkonten ermöglicht. Der Administrator kann einem Benutzerkonto des Active Directory beispielsweise über die Mitgliedschaft in der lokalen Gruppe der Administratoren auf dem zu verwaltenden Server die Berechtigung einräumen, den Server vollständig zu verwalten.

Motivation: Die Verwendung von Konten des zentralen Verzeichnisdienstes erlaubt die Zuordnung eines Kontos zu einer Person und die Durchsetzung von Sicherheitsrichtlinien (wie: Anmeldung mit Smartcard erforderlich) zu diesen zentral verwalteten Konten.

Umsetzungsbeispiel: Ein Mitarbeiter, der die Dateifreigaben eines Verbundes mehrerer Datei- und Drucker-Server regelmäßig verwalten möchte, erhält ein Konto im Active Directory, welches Mitglied der lokalen Gruppe der Drucker-Administratoren auf allen Servern des Verbundes ist.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen

ID: 3.15-52/10.0

Req 53	Die Anzahl lokaler, zum Betrieb notwendiger, Konten muss minimiert werden.
--------	--

Für lokale Konten gelten bei allen Betriebssystemen erhöhte Sicherheitsanforderungen. Der Administrator muss gewährleisten, dass alle nicht genutzten lokalen Konten wirksam deaktiviert sind.

Für nicht-vermeidbare (System-)Konten, bei denen eine Anmeldung in gewissen Fällen auch per Passwort möglich sein muss (root, lokaler Administrator), müssen diese Passwörter für jede Maschine und jedes Konto individuell und ohne erkennbare Bildungsregel gewählt werden.

Motivation: Lokale Accounts sind zusätzliche Angriffspunkte, die durch Angreifer beziehungsweise unbefugte Personen missbraucht werden könnten. Dies erfordert das nur für den Betrieb unbedingt notwendige lokale Konten im Betriebssystem vorhanden sind.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System

Req 54 Vordefinierte, nicht benötigte Benutzerkonten müssen gelöscht oder zumindest deaktiviert werden.

Auf vielen Systemen existieren nach der initialen Installation vordefinierte, aber nicht genutzte Benutzerkonten (z. B. "Gast").

Diese vordefinierten Benutzerkonten müssen unmittelbar nach der initialen Installation gelöscht oder zumindest deaktiviert werden; sollten diese Maßnahmen nicht umsetzbar sein, muss das entsprechende Benutzerkonto für einen Fernzugriff gesperrt werden. In jedem Fall müssen auch deaktivierte oder gesperrte Benutzerkonten mit einem Authentisierungsmerkmal (z. B. einem Passwort oder einem SSH Key) versehen werden, so dass im Fall einer Fehlkonfiguration die unberechtigte Nutzung eines solchen Benutzerkontos verhindert wird.

Ausgenommen von der Anforderung, vordefinierte Benutzerkonten zu löschen oder zu deaktivieren, sind Benutzerkonten, die ausschließlich der internen Nutzung auf dem entsprechenden System dienen und die für die Funktionalität einer oder mehrerer Anwendungen des Systems notwendig sind. Auch für ein solches Benutzerkonto muss sichergestellt werden, dass ein Fernzugriff oder eine lokale Anmeldung nicht möglich ist und dass ein Benutzer des Systems ein solches Benutzerkonto nicht missbräuchlich nutzen kann.

Motivation: In einem Produkt standardmäßig vordefinierte Benutzerkonten sind typischerweise allgemein bekannt und können von einem Angreifer sehr gezielt für Brute-Force- und Wörterbuchangriffe ausgewählt werden. Werden diese Benutzerkonten in einem konkreten System gar nicht benötigt, stellt deren Existenz dann eine unnötige Angriffsfläche dar. Ein besonderes Risiko stellen vordefinierte Benutzerkonten dar, die ohne Passwort oder mit einem weithin bekannten Standardpasswort vorkonfiguriert sind. Solche Benutzerkonten können unmittelbar von einem Angreifer missbraucht werden, falls ihre Absicherung aufgrund der nicht weiter vorgesehenen Nutzung im konkreten System versäumt wurde.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

Req 55 Es muss bei Betriebssysteminstallationen, die Mitglieder einer Active Directory-Domäne sind, das erste lokale Administratorenkonto des Betriebssystems gesperrt sein.

Alle Windows Server-Betriebssysteme werden mit einem ersten lokalen Administratorenkonto ausgeliefert, dessen technische Sicherheitskennung (SID) auf allen Windows Server-Betriebssystemen identisch ist. Dieses muss der Verantwortliche deaktivieren, um jegliche Verwendung des Kontos effektiv zu verhindern.

Hinweis: Sollte sich das Betriebssystem nicht mehr mittels eines Domänenkontos verwalten lassen, müsste der Administrator den Betrieb des Servers unterbrechen und das Betriebssystem im abgesicherten Modus starten. Dabei wird dieses lokale Konto automatisch wieder aktiviert.

Motivation: Das erste lokale Administratorkonto eines Windows Servers stellt eine Schwachstelle dar, da es auf allen Systemen die gleiche technische Sicherheitskennung (SID) trägt. Es wird nicht automatisch gesperrt, falls ein Angreifer versucht, das Passwort durch ständige Anmeldeversuche zu erraten.

Umsetzungsbeispiel: Der Administrator kann das lokale Administratorkonto beispielsweise durch eine Gruppenrichtlinie deaktivieren.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen

Req 56 Es muss das vordefinierte lokale Gäste-Konto gesperrt sein.

Alle Windows Server-Betriebssysteme werden mit einem vordefinierten lokalen und deaktivierten Gäste-Konto ausgeliefert. Dieses Konto muss der Administrator deaktivieren, um jegliche Verwendung des Kontos effektiv zu verhindern.

Motivation: Das vordefinierte lokale Gäste-Konto stellt eine Schwachstelle dar, da sich mit dessen Identität gegenüber dem Betriebssystem Erkenntnisse gewinnen lassen, die Angriffe begünstigen.

Umsetzungsbeispiel: Der Administrator kann das vordefinierte Gäste-Konto beispielsweise durch eine Gruppenrichtlinie deaktivieren.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen

Req 57 Falls Passwörter zur Authentifizierung genutzt werden, müssen Vorkehrungen getroffen worden sein, die die mit dem Einsatz von Passwörtern verbundenen Risiken minimieren.

Werden Passwörter verwendet, müssen die folgenden Kriterien erfüllt werden:

(1) Ein System darf nur Passwörter akzeptieren, die die folgende Komplexität erfüllen:

- Mindestlänge 12 Zeichen
- Bestehend aus min. drei der vier Kategorien: Kleinbuchstaben, Großbuchstaben, Ziffern, Sonderzeichen

Das System muss bei der Vergabe sicherstellen, dass ein Passwort diesen Mindestregeln entspricht.

(2) Passwörter dürfen nicht im Klartext angezeigt werden.

(3) Passwörter dürfen nur so auf dem System gespeichert werden, dass

- der Zugriff auf Dateien, die Passwörter enthalten, nur Administratoren möglich ist und
- es nach aktuellem Stand der Technik nur mit unverhältnismäßig großem Aufwand möglich wäre, sie aus dem gespeicherten Wert zurückzurechnen (Nutzung einer für diesen Zweck als sicher eingestuften, kryptografischen, Einwegfunktion mit mehrfachem Hashing, z. B. bcrypt, und "Salzen" der Hashes als Schutz gegen Rainbowtable-Angriffe).

Dies verringert zudem das Risiko von Wörterbuch- und Brute-Force-Angriffen gegen die Inhalte einer Passwortdatei.

In expliziter Deutlichkeit ist als NICHT ZULÄSSIG hervorzuheben:

- jegliche Speicherung von Passwörtern im Klartext
- jegliche Speicherung von Passwörtern in direkt rückrechenbaren Formaten, z. B. base64 (kein weiteres Wissen benötigt)
- jegliche Speicherung von Passwörtern mittels umkehrbarer Verschlüsselung (Symmetrische Verfahren mit einem Schlüssel)

(4) Um das Erraten von Passwörtern, Wörterbuch- und Brute-Force-Attacken beim Login zu verhindern, können verschiedene Maßnahmen oder eine Kombination daraus umgesetzt werden, z. B.:

- Ansteigende zeitliche Verzögerung vor einer erneuten Eingabe eines Passwortes nach einem Fehlversuch („Teergrube“, z. B. durch Verdopplung der Wartezeit nach jeder Falsch-Eingabe oder Verwendung der Fibonacci-Folge 2,3,5,8,13,21,34, ... als Wert der Erhöhung der Wartezeit).
- Temporäres oder dauerhaftes Sperren des Kontos nach einer vorgegebenen Anzahl an Fehlversuchen (typischerweise 5). Sperrdauer typischerweise größer 10 Minuten. Damit ein Angreifer dies nicht nutzen kann, um gezielt Konten unbrauchbar zu machen, sollte eine solche zeitliche Sperrung auch nicht zu lang sein (typischerweise 1h). Zudem wird ein Entsperrprozess für legitime Nutzer vollständig gesperrter Konten benötigt.

Bei der Verwendung eines zentralen Systems für die Authentifizierung der Benutzer können diese Funktionen dorthin weitergereicht oder ausgelagert werden.

Motivation: Passwörter mit der genannten Komplexität bieten eine hohe Robustheit gegen Angriffe bei gleichzeitig akzeptabler Benutzerfreundlichkeit. Triviale, zu kurze oder schlecht gespeicherte Passwörter sind anfällig gegen Brute-Force- und Wörterbuch-Angriffe und sind von einem Angreifer ermittelbar. Ein einmal ermitteltes Passwort kann dann von einem Angreifer für den unautorisierten Zugriff auf das System und dessen Daten genutzt werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.37-36/9.0

8. Authentisierungsmerkmal Passwort

Req 58	Falls Passwörter als Authentisierungsmerkmal genutzt werden, darf deren Darstellung während der Eingabe nicht im Klartext erfolgen.
--------	---

Passwörter dürfen während deren Eingabe nicht in lesbarem Klartext auf Bildschirmen oder sonstigen Ausgabegeräten dargestellt werden. Eine Darstellung während der Eingabe darf keine Rückschlüsse auf die tatsächlich im Passwort verwendeten Zeichen ermöglichen.

Diese Anforderung gilt für jegliche Arten von Eingabemasken und -feldern für Passwörter.

Beispiele hierfür sind Dialoge zur Passwort-Vergabe, zur Passwort-basierenden Anmeldung an Systemen oder zur Änderung von bestehenden Passwörtern.

Ausnahmeregelungen:

- Innerhalb eines Eingabefelds ist eine optionale Klartext-Darstellung eines Passworts zulässig, sofern diese Klartext-Darstellung einem validen Zweck dient, nur temporär anhält, dazu fallbezogen durch den legitimen Benutzer explizit zu aktivieren ist und von diesem umgehend auch wieder deaktiviert werden kann. Ein valider Zweck wäre beispielsweise, dem legitimen Benutzer bei Bedarf eine unkomplizierte visuelle Überprüfung zu ermöglichen, sein Passwort in einem Anmelde-Dialog korrekt eingegeben zu haben, bevor er die Anmeldung letztendlich final vollzieht. Eine solche optionale Klartext-Darstellung eines Passworts muss vollständig in der Kontrolle des legitimen Benutzers verbleiben, damit er über deren Aktivierung/Deaktivierung situationsgerecht entscheiden kann. In der Standard-Einstellung des Systems muss die Klartext-Darstellung deaktiviert sein.
- Das auf vielen mobilen Endgeräten (Smartphones) typische Verhalten, jedes einzelne Zeichen bei der Eingabe eines Passworts sehr kurz im Klartext anzuzeigen, um dem Benutzer die Eingabekontrolle zu erleichtern, ist dort grundlegend zulässig. Allerdings darf dabei niemals das vollständige Passwort im Klartext auf dem Bildschirm dargestellt werden.

Motivation: Im Fall einer Klartext-Darstellung besteht das Risiko, dass dritte Personen ein Passwort während der Eingabe zufällig oder gezielt über die Bildschirm-Ausgabe ausspähen können.

Umsetzungsbeispiel: In der Darstellung auf dem Bildschirm wird während der Eingabe eines Passworts jedes einzelne Zeichen einheitlich durch ein "*" ersetzt.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.01-31/9.0

Req 59	Falls Passwörter als Authentisierungsmerkmal genutzt werden, muss eine Änderung des eigenen Passwortes jederzeit durch den Benutzer möglich sein.
--------	---

Das System muss eine Funktion bieten, die es einem Benutzer ermöglicht, sein Passwort jederzeit zu ändern.

Bei der Verwendung eines zentralen Systems darf die Funktion auf dieses System weitergereicht oder ausgelagert werden.

Motivation: Nur durch die Möglichkeit, dass ein Benutzer sein Authentisierungsmerkmal jederzeit selbsttätig ändern

kann, ist ein zeitnahe Änderung möglich, wenn der Benutzer den Verdacht hat, dass dieses in den Besitz Dritter gelangt sein könnte.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.01-29/9.0

Req 60	Falls Passwörter als Authentisierungsmerkmal genutzt werden, muss nach spätestens 12 Monaten ein Passwort-Wechsel erfolgen.
--------	---

Die maximal zulässige Nutzungsdauer für Passwörter beträgt 12 Monate.
Erreicht ein Passwort die maximal zulässige Nutzungsdauer, muss es geändert werden.

Das System muss hierzu den Benutzer automatisch bei dessen nächster Systemanmeldung auf die abgelaufene Nutzungsdauer hinweisen und ihn unmittelbar durch einen Passwort-Änderungsdialog führen. Der Zugriff auf das System darf ohne eine erfolgreich abgeschlossene Passwort-Änderung nicht weiter zugelassen werden.
Für technische Benutzerkonten (M2M bzw. Machine-2-Machine), die für die Authentifizierung und Autorisierung von Systemen untereinander oder von Anwendungen auf einem System genutzt werden, müssen ebenfalls automatisierte Lösungen zur Einhaltung der zulässigen Nutzungsdauer für Passwörter implementiert werden.

Falls eine automatisierte Abbildung des Prozesses zur Passwort-Änderung nicht umsetzbar ist, muss ersatzweise eine wirksame organisatorische Maßnahme angewendet werden, die eine verbindliche manuelle Passwort-Änderung bei Ablauf der zulässigen Nutzungsdauer sicherstellt.

Motivation: Passwörter sind im Gegensatz zu moderneren Authentisierungsmerkmalen leichter angreifbar. Ohne spezifische Maßnahmen einer verlässlichen technisch automatisierten Kompromittierungserkennung kann das Risiko, dass ein Passwort von einem Angreifer ermittelt oder gebrochen wird, über die Zeit deutlich steigen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.01-30/9.0

Req 61	Falls Passwörter als Authentisierungsmerkmal verwendet werden, muss die Wiederverwendung bereits eingesetzter Passwörter unterbunden werden.
--------	--

Für jedes Benutzerkonto muss eine Historie der bisher genutzten Passwörter aufgezeichnet werden. Wird eine Passwort-Änderung für ein Benutzerkonto initiiert, ist das neue Passwort gegen diese Passwort-Historie abzugleichen. Bei erkannter Wiederverwendung eines Passworts muss die Passwort-Änderung abgelehnt werden. Die Umsetzung dieses Validierungsvorgangs muss im System auf Basis von technischen Maßnahmen erfolgen. Bei Verwendung eines zentralen IAM Systems für die Authentisierung der Benutzer darf die Umsetzung an das zentrale IAM System weitergereicht bzw. dorthin ausgelagert werden [vgl. Wurzel-Anforderungsdokument "3.69 IAM (Identity Access Management) - Framework"].

Generell soll mittels der Passwort-Historie sichergestellt werden, dass ein schon einmal verwendetes Passwort niemals erneut einsetzbar ist.

Aufgrund technischer Limitierungen kann eine Passwort-Historie jedoch in vielen IT/NT-Produkten nicht unbe-

schränkt aufgezeichnet werden. In diesem Fall ist die folgende Grundregelung zu berücksichtigen:

- ein bereits genutztes Passwort darf für den Zeitraum von mindestens 60 Tagen nicht erneut einsetzbar sein (gemessen ab dem Zeitpunkt, an dem das betroffene Passwort durch ein anderes ersetzt wurde)
- in Systemen, in denen der Zeitraum von mindestens 60 Tagen nicht abgebildet werden kann, muss der längst mögliche Zeitraum konfiguriert werden. Zusätzlich muss durch einen Project Security Manager (PSM) bestätigt werden, dass der konfigurierte Zeitraum im Gesamtkontext des Systems noch ausreichend im Sinne der Sicherheitsanforderung ist.

Anmerkung:

Einige IT/NT-Produkte bieten keinen technischen Konfigurationsparameter an, mit dem die Passwort-Historie direkt an einen Zeitraum gebunden werden kann, sondern ermöglichen nur, die Anzahl der aufzuzeichnenden Passwörter zu definieren. In solchen Fällen darf der Zeitraum alternativ durch eine Verknüpfung der folgend beschriebenen, i. d. R. breit verfügbaren Konfigurationsparameter sichergestellt werden. Innerhalb der resultierenden Policy kann ein Benutzer nur einmal pro Tag sein Passwort ändern und aufgrund der Anzahl der aufgezeichneten Passwörter effektiv nach frühestens 60 Tagen ein altes Passwort erneut einsetzen.

- Minimum Passwort-Alter: 1 Tag
- Passwort-Historie: Aufzeichnung der letzten 60 benutzten Passwörter

In dieser Umsetzungsvariante ist zu beachten, dass das Minimum Passwort-Alter nicht mehr als einen Tag betragen sollte, um den Benutzer nicht unangemessen hinsichtlich der grundsätzlichen Notwendigkeit einzuschränken, das Passwort jederzeit selbstständig ändern zu können.

Motivation: Benutzer favorisieren in der Regel Passwörter, die sie sich gut merken können und verwenden diese in Folge oft wiederkehrend über lange Zeiträume, falls das System dies zulässt. Aus Sicht des Benutzers ist das Verhalten nachvollziehbar, führt aber effektiv zu einer erheblichen Reduzierung der Schutzwirkung dieses Authentisierungsparameters. Mit etwa entsprechenden Kenntnissen über den Benutzer oder erbeuteten Informationen aus zurückliegenden System-Kompromittierungen kann ein Angreifer so Zugriff auf vermeintlich geschützte Benutzerkonten erlangen. Insbesondere auch in Situationen, in denen im Rahmen einer akuten Risikobehandlung zentral neue Initialpasswörter vergeben werden, die Benutzer diese jedoch unmittelbar aus Bequemlichkeit auf ein vorheriges Passwort zurückändern, bestünde hohe Gefahr, dass ein Angreifer seinen illegalen Zugriff erneut aufnehmen kann. Es ist daher wichtig zu vermeiden, dass Benutzer alte Passwörter erneut einsetzen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.01-28/9.0

Req 62	Falls Passwörter als Authentisierungsmerkmal genutzt werden, muss ein Schutz gegen Online-Angriffe wie Wörterbuch- und Brute-Force-Attacken vorhanden sein, der das Erraten von Passwörtern stark erschwert.
--------	--

Online Wörterbuch- und Brute-Force Angriffe haben zum Ziel, durch automatisiertes Ausprobieren an einer regulären Zugangsschnittstelle des Systems die Passwörter von Benutzerkonten zu erraten.

Um dies zu verhindern, muss eine der folgenden Maßnahmen oder eine Kombination aus diesen umgesetzt werden:

- mittels technischer Maßnahmen abgebildete Erzwingung einer Wartezeit nach einem fehlgeschlagenen Anmeldeversuch, bevor eine erneute Anmeldung ermöglicht wird. Die Wartezeit sollte sich zudem mit jedem weiteren fehlgeschlagenen Anmeldeversuch automatisch deutlich erhöhen (z. B. durch Verdopplung).
- automatisiertes Sperren des Benutzerkontos nach einer vorgegebenen Anzahl von aufeinanderfolgenden fehl-

geschlagenen Anmeldeversuchen (typischerweise 5). Allerdings ist bei dieser Lösung zu bedenken, dass diese einen Entsperrungs-Prozess erforderlich macht und ein Angreifer dies gezielt nutzen kann, um Konten zu sperren und somit vorübergehend unbrauchbar zu machen.

- Verwendung von CAPTCHA ("Completely Automated Public Turing test to tell Computers and Humans Apart"), um automatisierte Anmeldeversuche von Maschinen ("Robots" oder "Bots") bestmöglich zu unterbinden. Ein CAPTCHA stellt dazu eine kleine Aufgabe, i. d. R. basierend auf grafischen oder akustischen Elementen, die von einer Maschine nur schwer zu lösen ist. Es ist entsprechend zu berücksichtigen, dass CAPTCHA problematisch bzgl. der Barrierefreiheit sein können.

Um eine höhere Sicherheit zu erreichen, ist es oftmals sinnvoll, zwei oder mehrere der genannten Maßnahmen miteinander zu kombinieren. Dies ist abhängig vom Einzelfall zu prüfen und entsprechend umzusetzen.

Motivation: Ohne entsprechenden Schutz kann ein Angreifer durch bloßes Durchprobieren von Wörterbuchlisten oder automatisch erzeugten Zeichenkombinationen versuchen ein Passwort zu ermitteln, um so das entsprechende Benutzerkonto missbräuchlich zu nutzen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen

ID: 3.01-25/9.0

Req 63	Falls Passwörter als Authentisierungsmerkmal genutzt werden, muss deren Speicherung unter Einsatz eines für diesen Zweck als ausreichend sicher anerkannten "Password Hashing"-Verfahrens erfolgen, um Offline-Angriffe wie Wörterbuch- und Brute-Force-Attacken stark zu erschweren.
--------	---

Diese Anforderung bezieht sich auf die Speicherung von Passwörtern in sämtlichen Arten von Benutzerdatenbanken, die im vorliegenden System eingesetzt werden, um darüber eingehende Zugriffe (lokal oder aus der Ferne) von Benutzern oder anderen Systemen zu authentisieren.

Gelingt es einem Angreifer, die Kopie einer Benutzerdatenbank des Systems in seinen Besitz zu bringen, kann er diese in einer unabhängigen Umgebung einem automatisierten Wörterbuch- oder Brute-Force-Angriff aussetzen, um enthaltene Passwörter zu ermitteln. Durch Einsatz spezialisierter Werkzeuge in Kombination mit hoher Rechenleistung können bei unzureichenden Schutzmaßnahmen hierbei hohe Erkennungsraten in verhältnismäßig kurzer Zeit erreicht werden. Aufgrund der Unabhängigkeit vom Quellsystem bleibt ein solcher Offline-Angriff auf eine Benutzerdatenbank zudem unbemerkt.

Folgende Maßnahme ist umzusetzen, da diese den größtmöglichen Schutz bei Offline-Angriffen gewährleistet:

- Passwörter müssen unter Verwendung einer für diesen Zweck anerkannt wirksamen, zum aktuellen Stand der Technik als sicher eingestuften, kryptografischen Einwegfunktion gespeichert werden (bekannt als "Password-Hashing" Verfahren)

Hinweis: Zulässige Passwort-Hashing-Verfahren sind im Sicherheitsanforderungsdokument "3.50 / Kryptographische Algorithmen und Sicherheitsprotokolle" beschrieben.

In expliziter Deutlichkeit ist als NICHT ZULÄSSIG hervorzuheben:

- jegliche Speicherung von Passwörtern im Klartext
- jegliche Speicherung von Passwörtern in direkt rückrechenbaren Formaten
- jegliche Speicherung von Passwörtern mittels umkehrbarer Verschlüsselung

Hinweis:

"direkt rückrechenbare Formate" bezieht sich in diesem Kontext auf Formate, die ein Passwort lediglich kodieren, also ohne Einbeziehung eines geheimen Schlüssels transformieren. Da ein Passwort bei Anwendung eines solchen Formats nicht mehr in seinem originalen Klartext lesbar bleibt, werden diese Formate leicht als Schutzmaßnahme missverstanden. Effektiv bieten sie jedoch keinen Schutz, da die dahinterliegende Kodierung fest definiert ist und von einem Angreifer sehr leicht für die Rückrechnung der Inhalte in den ursprünglichen Klartext genutzt werden kann.

Beispiele für direkt rückrechenbare Formate sind: "base64", "rot13"

"Umkehrbar" sind alle Verfahren der Verschlüsselung, die unter Verwendung des passenden Schlüssels ermöglichen, einen verschlüsselten Inhalt zurück in den originalen Inhalt zu transformieren. Entsprechend stellt sich bei umkehrbarer Verschlüsselung stets die Herausforderung, den Schlüssel sicher aufzubewahren und vor unberechtigtem Zugriff zu schützen. Die Umkehrbarkeit ist auf vielen Einsatzgebieten der Verschlüsselung, z. B. für den Transport von vertraulichen Nachrichten, eine benötigte Grundeigenschaft, für das Speichern von Passwörtern jedoch kontraproduktiv: ein gespeichertes Passwort muss zwar mittels technischer Methoden vergleichbar bleiben, aber darf nicht mehr in seinen Klartext rückwandelbar sein, um es vor unberechtigter Einsicht bestmöglich zu schützen.

Beispiele für umkehrbare Verschlüsselung sind: "AES", "CHACHA20", "3DES", "RSA"

Motivation: Ohne entsprechenden Schutz kann ein Angreifer im Besitz der Benutzerdatenbank durch bloßes Durchprobieren von Wörterbuchlisten oder automatisch erzeugten Zeichenkombinationen versuchen, massenhaft Passwörter zu ermitteln, um so entsprechende Benutzerkonten missbräuchlich zu nutzen. Passwörter, die im Klartext oder direkt rückrechenbaren Formaten gespeichert werden, sind bei einem Offline-Angriff vollkommen schutzlos.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.01-24/9.0

Req 64	Falls Passwörter als Authentisierungsmerkmal für technische Benutzerkonten genutzt werden, müssen diese mindestens 30 Zeichen lang sein und drei der folgenden Zeichenkategorien beinhalten: Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen.
--------	--

Technische Benutzerkonten zeichnen sich dadurch aus, dass sie nicht von Personen verwendet werden. Stattdessen werden sie für die Authentifizierung und Autorisierung von Systemen untereinander oder von Anwendungen auf einem System genutzt.

Ein System darf für technische Benutzerkonten nur Passwörter verwenden, welche die folgende Komplexität erfüllen:

- Mindestlänge 30 Zeichen
- Bestehend aus mindestens drei der folgenden vier Zeichenkategorien:
 - Kleinbuchstaben
 - Großbuchstaben
 - Ziffern
 - Sonderzeichen

Motivation: Technische Benutzerkonten sind aufgrund ihrer Verwendung in Machine-to-Machine (M2M) Kommunikations-Szenarien oft mit Berechtigungen ausgestattet, die für einen Angreifer von hohem Interesse sein können, um Infrastrukturen zu kompromittieren. Ohne Mechanismen einer umfassenden Kompromittierungserkennung kann dann das Risiko, dass ein Passwort von einem Angreifer ermittelt oder gebrochen wird, über die Zeit deutlich ansteigen. Eine signifikante Erhöhung der Passwort-Länge wirkt diesen Risiken entgegen und lässt sich zudem in M2M Szenarien besonders leicht umsetzen, da die Handhabung eines sehr langen Passworts für eine Maschine (im Gegensatz zu einer Person) keine besondere Herausforderung darstellt.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen

ID: 3.01-27/9.0

9. Protokollierung

Req 65 Die Systemzeit muss zu einer exakten Referenzzeit (Zeitnormal) synchronisiert werden.

Als Zeitnormal ist eine Zeitgeber-Quelle heranzuziehen, die ein Zeitsignal auf Basis der koordinierten Weltzeit ("UTC" = "Universal Time Coordinated") liefert.

Anmerkung: die anhand der Zeitgeber-Quelle zu UTC synchronisierte Systemzeit darf auf dem lokalen System mittels entsprechender Zeitzone-Konfiguration bei der Ausgabe von Zeitinformationen in die Ortszeit transformiert werden, sofern die so stattfindende Zeitzoneanpassung eindeutig erkennbar und nachvollziehbar ist.

Systeme, die zu einer gemeinsamen Sicherheits-Domäne gehören, müssen sich einheitlich an derselben Zeitgeber-Quelle synchronisieren.

Motivation: Zeitsynchronisation kann auf einem System eine technische Voraussetzung sein, um zeitkritische Abhängigkeiten in beispielsweise der Nutzung von Zertifikaten oder Authentisierungsmechanismen korrekt bedienen zu können. Dringend erforderlich sind außerdem exakte Zeitstempel in Protokollierungseinträgen, damit diese bei Sicherheitsvorfällen oder Problemanalysen in eindeutiger zeitlicher Relation auswertbar sind.

Umsetzungsbeispiel: Einige zulässige Zeitgeber-Quellen:

- vertrauenswürdig eingestuftes NTP ("NetworkTimeProtocol") Server im IP-Netzwerk
- DCF77-Funksignal über physisch angebundenes Empfängermodul
- GPS-Funksignal über physisch angebundenes Empfängermodul

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.01-32/9.0

Req 66 Sicherheitsrelevante Windows Server Events müssen mit genauem Zeitstempel und einer eindeutigen Systembezeichnung protokolliert werden.

Windows Server müssen das Auftreten von sicherheitsrelevanten Ereignissen protokollieren. Um die Auswertung und Klassifizierung der auftretenden Ereignisse zu ermöglichen, müssen diese zusammen mit einer eindeutigen Systembezeichnung (z. B. Hostname, IP- oder MAC-Adresse) und dem genauen Zeitpunkt des Auftretens protokolliert werden.

Bei der Protokollierung sind die geltenden gesetzlichen, tariflichen und betrieblichen Bestimmungen zu beachten. Diese Bestimmungen legen unter anderem fest, dass die Protokollierung von Ereignissen nur für einen bestimmten Zweck durchgeführt werden darf. Die Protokollierung zum Zweck der Arbeitskontrolle von Mitarbeitern ist nicht gestattet.

Typische Ereignisse sind:

Ereignis	Zu protokollierende Daten des Ereignisses
----------	---

Erfolgreiche Anmeldung/Verwendung von allen Accounts (Im Falle von Domaincontrollern nur privilegierte Accounts)	- Konto - Quelle (IP-Adresse) bei entferntem Zugriff - LogonType - Art des Log-ons (Prozess und LogonType, beides enthalten in Event-ID 4624) - Berechtigung des Log-ons (Event-ID 4672) - Session ID
Ereignisse des Antivirensystems	- Update der Signaturen - Aktivieren/Deaktivieren des Virenschutzes - Identifikation von Bedrohungen - Reaktion auf die Bedrohung
Erstellung von Autostart Funktionen soweit möglich wie (Services, Scheduled Tasks, Autostart in der Registry (Run, RunOnce))	- Gestartetes Programm - Startbedingung - Rechte des Prozesses
Logmanipulationen	- Löschung der Logdateien (Event ID 1102)
Verwendung von Remotekommandos; eingehend und ausgehend	- WMI Remoting - PowerShell Remoting - PSEXEC
Ausführen von Befehlen/Start von Prozessen wie u. A. durch Defender ATP abgedeckt	- Startparameter - Rechte des Prozesses - sofern verfügbar: Hash der ausgeführten Binary - sofern verfügbar: Durch Prozess aufgebaute Netzwerkverbindungen
Logoff eines Accounts	- Session ID - Account

Motivation: Die Protokollierung von sicherheitsrelevanten Ereignissen ist eine Grundvoraussetzung, um laufende Angriffe oder auch Angriffe im Nachhinein erkennen zu können. Nur so ist es möglich, sinnvolle Maßnahmen zur Erhaltung oder auch Wiederherstellung der Systemsicherheit durchzuführen. Des Weiteren dienen die Protokollierungsdaten der Beweissicherung, um rechtlich gegen Angreifer vorgehen zu können.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.15-66/10.0

Req 67 Sicherheitsrelevante Protokollierungsdaten müssen umgehend nach deren Erzeugung an ein separates System weitergeleitet werden.

Sicherheitsrelevante Protokollierungsdaten müssen neben der lokalen Speicherung in den entsprechenden Protokolldateien auch an ein externes System weitergeleitet werden. Standardisierte Protokolle wie Syslog, SNMPv3 müssen hierbei bevorzugt zum Einsatz kommen. Die Übertragung sollte gesichert erfolgen, d. h. verschlüsselt und authentifiziert, wenn schutzbedürftige Daten übertragen werden. Zur Prüfung auf Konsistenz und Vollständigkeit sollen Sequenznummern verwendet werden und die Übertragung möglichst per TCP statt UDP erfolgen.

Hinweis: Mit dem Empfänger der Daten muss abgestimmt werden, wie die gelieferten Daten zu bewerten sind.

Motivation: Werden Protokollierungsdaten nur lokal gespeichert, können diese im Falle einer erfolgreichen Kompromittierung des Systems durch einen Angreifer manipuliert werden, um seinen Angriff und durchgeführte Manipulationen zu verheimlichen.

nen des Systems zu verschleiern. Aus diesem Grund muss die Weiterleitung zeitnah nach dem Auftreten des Ereignisses erfolgen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unbemerkt durchführbare Angriffe

ID: 3.37-43/9.0

Req 68	Für sicherheitsrelevante Protokollierungsdaten, die lokal erfasst werden, müssen geltende Aufbewahrungszeiträume und Löschfristen eingehalten werden.
--------	---

Aus Sicht der IT-Sicherheit wird auf einem System die lokale Erfassung von sicherheitsrelevanten Protokollierungsdaten nicht zwingend gefordert. Da lokal erfasste Protokollierungsdaten bei Systemstörungen beschädigt oder von einem erfolgreichen Angreifer gezielt manipuliert werden können, sind sie für sicherheitstechnische bzw. forensische Analysen nur bedingt belastbar. Entsprechend ist für die IT-Sicherheit relevant, dass Protokollierungsdaten an einen separaten Log Server weitergeleitet werden.

Eine lokale Erfassung kann dennoch erfolgen; beispielsweise falls bei der Erzeugung der Protokollierungsdaten eine lokale Speicherung aufgrund technischer Abläufe zunächst unabdingbar ist oder es begründete betriebliche Interessen gibt, Protokollierungsdaten auch lokal vorzuhalten.

Folgende Grundregelung ist bei einer lokalen Erfassung von Protokollierungsdaten zu berücksichtigen:

- Sicherheitsrelevante Protokollierungsdaten müssen für einen Zeitraum von 90 Tagen aufbewahrt werden.
(Diese Anforderung gilt nur, falls auf dem System keine zusätzliche Weiterleitung an einen separaten Log Server umgesetzt ist und Protokollierungsdaten daher ausschließlich lokal erfasst werden.)
- Nach Ablauf von 90 Tagen muss eine umgehende Löschung von gespeicherten Protokollierungsdaten erfolgen.

Abweichungen

Abweichende Aufbewahrungszeiträume und Löschfristen können durch gesetzliche oder regulatorische Anforderungen (insbesondere im Zusammenhang mit personenbezogenen Daten) bestehen oder durch vertragliche Vereinbarungen definiert sein. In diesen Fällen sind die geltenden Zeiträume individuell mit einem Project Security Manager (PSM) bzw. Datenschutzberater (DSB) abzustimmen oder werden durch diesen vorgegeben.

Motivation: Protokollierungsdaten sind ein immens wichtiges Werkzeug der IT-Sicherheit zur Abwendung, Detektierung und Aufklärung von Systemstörungen, Sicherheits- und Datenschutzvorfällen. Auf der anderen Seite unterliegt die Erfassung von Protokollierungsdaten wie jede andere Datenverarbeitung auch gesetzlichen und regulatorischen Auflagen. Entsprechend müssen Richtlinien eingehalten werden, die beides in Einklang bringen.

Umsetzungsbeispiel: Unter Berücksichtigung der gültigen Gesetzeslage und zutreffenden Datenschutz-Regularien werden folgende Löschfristen für lokal erfasste sicherheitsrelevante Protokollierungsdaten auf einem beispielhaften TK-System umgesetzt:

- Standard System Logs: Löschung nach spätestens 90 Tagen
- Protokollierungen von öffentlichen IP-Adressen: Löschung (oder Anonymisierung) nach spätestens 7 Tagen
- Protokollierungen der Vergabe von dynamischen öffentlichen IP-Adressen durch die TK-Lösung: Löschung nach spätestens 7 Tagen
- Protokollierungen nicht abrechnungsrelevanter Call Detail Records: Löschung nach spätestens 7 Tagen
- Protokollierungen der Kommunikations-Inhalte von E-Mail und SMS: Löschung nach spätestens 24 Stunden
- Protokollierungen der behandelten Domain-Abfragen des DNS-Servers der TK-Lösung: Löschung nach spätestens 24 Stunden

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten

- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.01-34/9.0

Req 69	Für sicherheitsrelevante Protokollierungsdaten, die an den Log Server weitergeleitet werden, muss die Einhaltung geltender Aufbewahrungszeiträume und Löschfristen sichergestellt werden.
--------	---

Folgende Grundregelung ist zu berücksichtigen:

- sicherheitsrelevante Protokollierungsdaten müssen auf dem Log Server für einen Zeitraum von 90 Tagen aufbewahrt werden.
- nach Ablauf von 90 Tagen muss eine umgehende Löschung der auf dem Log Server gespeicherten Protokollierungsdaten erfolgen.

Abweichungen

Abweichende Aufbewahrungszeiträume und Löschfristen können durch gesetzliche oder regulatorische Anforderungen bestehen (insbesondere im Zusammenhang mit personenbezogenen Daten) oder durch vertragliche Vereinbarungen definiert sein. In diesen Fällen sind die geltenden Zeiträume individuell mit einem Project Security Manager (PSM) bzw. Datenschutzberater (DSB) abzustimmen oder werden durch diesen vorgegeben.

Log Server in Verantwortung eines Dritten

Sollte der ausgewählte Log Server nicht innerhalb derselben operativen Verantwortung liegen wie das Quellsystem der Protokollierungsdaten, muss sichergestellt werden, dass dem verantwortlichen Betreiber des Log Servers die gültigen Parameter für die zu empfangenden Protokollierungsdaten bekannt sind und durch diesen im Sinne der hier genannten Regelungen eingehalten werden.

Motivation: Protokollierungsdaten sind ein immens wichtiges Werkzeug der IT-Sicherheit zur Abwendung, Detektierung und Aufklärung von Systemstörungen, Sicherheits- und Datenschutzvorfällen. Auf der anderen Seite unterliegt die Erfassung von Protokollierungsdaten wie jede andere Datenverarbeitung auch gesetzlichen und regulatorischen Auflagen. Entsprechend müssen Richtlinien eingehalten werden, die beides in Einklang bringen.

Umsetzungsbeispiel: Unter Berücksichtigung der gültigen Gesetzeslage und zutreffenden Datenschutz-Regularien werden folgende Löschfristen für ausgeleitete sicherheitsrelevante Protokollierungsdaten eines beispielhaften TK-Systems auf dem separaten Log Server umgesetzt:

- Standard System Logs: Löschung nach spätestens 90 Tagen
- Protokollierungen von öffentlichen IP-Adressen: Löschung (oder Anonymisierung) nach spätestens 7 Tagen
- Protokollierungen der Vergabe von dynamischen öffentlichen IP-Adressen durch die TK-Lösung: Löschung nach spätestens 7 Tagen
- Protokollierungen nicht abrechnungsrelevanter Call Detail Records: Löschung nach spätestens 7 Tagen
- Protokollierungen der Kommunikations-Inhalte von E-Mail und SMS: Löschung nach spätestens 24 Stunden
- Protokollierungen der behandelten Domain-Abfragen des DNS-Servers der TK-Lösung: Löschung spätestens nach 24 Stunden

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.01-36/9.0

Req 70	Sicherheitsrelevante Protokollierungsdaten müssen echtzeitnah an eine Erkennungs- und Reaktionslösung für Sicherheitsvorfälle bereitgestellt werden.
--------	--

Eine zulässige Erkennungs- und Reaktionslösung im Sinne dieser Anforderung muss die folgenden Kriterien erfüllen:

- Es erfolgt eine kontinuierliche Analyse bzw. Korrelation der aus angebundenen IT/NT-Systemen bereitgestellten Protokollierungsdaten.
- Die Identifizierung bedrohlicher Aktivitäten und laufender Angriffe findet auf Basis einer fortlaufend aktuell gehaltenen Erkennungsmuster-Datenbank statt.
- Integrierte Alarmierungsprozesse lösen im Fall eines Fundes die Einleitung von Gegenmaßnahmen aus.
- Sicherheitsexperten sind aktiv involviert in den Betrieb der Lösung sowie die Auswertung von Alarmen.

Eine solche Lösung ist in ihrer Funktion nicht mit einem Log Server gleichzusetzen. Entsprechend muss die Bereitstellung an eine Erkennungs- und Reaktionslösung stets zusätzlich zu einer vorhandenen Weiterleitung an einen Log Server erfolgen. Eine Ausnahme besteht, falls der genutzte Log Server seinerseits die Protokollierungsdaten umgehend nach Erhalt zusätzlich an eine Erkennungs- und Reaktionslösung bereitstellt. In diesem Fall ist es ausreichend, dass das System die Protokollierungsdaten nur an den Log Server weiterleitet.

Die Protokollierungsdaten müssen ab dem Zeitpunkt ihrer Erzeugung im System innerhalb von 5 Minuten an die Erkennungs- und Reaktionslösung bereitgestellt werden ("echtzeitnah").

Die konkret zu unterstützenden technischen Schnittstellen und Protokolle für die Bereitstellung werden durch die im Einsatzumfeld des Systems verfügbare Erkennungs- und Reaktionslösung sowie die technische Basis des Systems bestimmt.

Motivation: IT/NT-Systeme sind permanent sicherheitstechnischen Bedrohungen und Angriffen ausgesetzt. Mittels einer zentralen Analyse und der Korrelation erfasster System-Ereignisse ganzer IT-Landschaften in nahezu Echtzeit können aktuelle Bedrohungen und laufende Angriffe auch über Systemgrenzen hinaus erkannt und zeitnah passende Gegenmaßnahmen eingeleitet werden. Die unverzügerte Bereitstellung von Protokollierungsdaten an die Erkennungs- und Reaktionslösung ist essenziell für deren Effektivität.

Umsetzungsbeispiel: **Beispiel 1:** Ein System auf Basis eines klassischen Servers erfasst sicherheitsrelevante Protokollierungsdaten im lokalen Syslog oder Windows Event Log des Betriebssystems. Die Protokollierungsdaten werden kontinuierlich zur weiteren Analyse, Angriffserkennung und Alarmbehandlung an ein SIEM (Security Information and Event Management) weitergeleitet.

Beispiel 2: Auf einem System wird ein EDR ("Endpoint Detection and Response") Agent ausgeführt. Der EDR-Agent leitet die von ihm auf dem System erfassten sicherheitsrelevanten Protokollierungsdaten kontinuierlich an das zentrale Backend der EDR-Lösung aus, auf dem die weitere Analyse, Angriffserkennung und Alarmbehandlung erfolgt.

Beispiel 3: Netzwerk-Komponenten stellen Ereignisse an ein SIEM bereit, die es ermöglichen, verdächtiges Kommunikationsverhalten wie Netzwerk-Scans, unzulässige Datenflüsse zwischen Netz-Segmenten oder aktive Verbindungen bzw. Verbindungsversuche zu verdächtigen Zielen im Internet zu entdecken. Im speziellen liefern Gateway Router aus dem CNDTAG "Netflow" Logs, während Forward Proxies Zugriffe auf Domänen und/oder IP-Adressen melden und Firewalls blockierte Verbindungsversuche loggen.

Beispiel 4: Auf Basis von Cloud-nativen Funktionen entwickelte Systeme erzeugen Protokollierungsdaten mittels der Cloud-eigenen Protokollierungs- und Überwachungsinfrastruktur direkt aus diesen Funktionen heraus. In einem solchen System wird die Erzeugung sicherheitsrelevanter Protokollierungsdaten in den entsprechenden Konfigurationsoptionen der eingesetzten Cloud-nativen Funktionen gezielt aktiviert. Die entstehenden Protokollierungsdaten werden kontinuierlich zur weiteren Analyse, Angriffserkennung und Alarmbehandlung an ein SIEM (Security Information and Event Management) übertragen. Einige Cloud-Anbieter leisten eine gewisse Angriffsmustererkennung bereits in der Cloud-eigenen Überwachungsinfrastruktur und erzeugen daraus spezifische Cloud-Alarme. Diese werden zusätzlich an das SIEM übertragen.

Beispiel 5: Ein System basiert auf einer SaaS ("Software as a Service") Applikation eines Cloud-Anbieters. Typischerweise verantwortet im SaaS Modell der Cloud-Anbieter alle operativen Aspekte der Applikation, inkl. des Sicherheitsmanagements. Der Cloud-Kunde selbst hat keinen Einfluss auf die zugrunde liegende technische Infrastruktur oder den Betrieb der Applikation. Anhand von Vertragsvereinbarungen, anerkannten Zertifikaten und dokumentierten Selbstauskünften des Cloud-Anbieters wird formell überprüft, dass der Cloud-Anbieter eine Erkennungs- und Reaktionslösung für Sicherheitsvorfälle implementiert hat. Einige Cloud-Anbieter erzeugen zusätzlich dedizierte Protokollierungsdaten über sicherheitsrelevante Aktivitäten innerhalb der separaten Kunden-Mandanten ihrer SaaS Applikation (beispielsweise zu Änderungen von Konfigurationseinstellungen, Berechtigungsvergaben oder Benutzer-Konten innerhalb der Mandanten) und stellen diese den Cloud-Kunden zu Verfügung. Diese sogenannten Audit-Logs werden

kontinuierlich zur weiteren Analyse, Angriffserkennung und Alarmbehandlung an ein SIEM (Security Information and Event Management) übertragen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unbemerkt durchführbare Angriffe

ID: 3.01-37/9.0