

Sicherheitsanforderung

Client Computer

Deutsche Telekom Gruppe

Version	7.0
Datum	01.07.2025
Status	Freigegeben

Impressum

Herausgeber
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Deutschland

Dateiname	Dokumentennummer 3.19	Dokumententyp Sicherheitsanforderung
Version 7.0	Stand 01.07.2025	Status Freigegeben
Fachlicher Ansprechpartner Telekom Security psa.telekom.de	Gültigkeitsdauer 01.07.2025 - 30.06.2030	Freigegeben von Stefan Pütz, Leiter SEC-T-TST

Zusammenfassung
Anforderungen zur Absicherung von Client Computern.

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.	Systemhärtung	5
3.	Hardware	12
4.	Systemaktualisierung	14
5.	Schutz von Daten und Informationen	17
6.	Verfügbarkeit und Integrität	24
7.	Authentifizierung und Autorisierung	26
8.	Protokollierung	36

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.

Dieses Anforderungspapier bietet die Grundlage welche Mindestanforderungen an einen Client erfüllt sein müssen, um direkt an die interne Backendinfrastruktur des Konzerns Deutsche Telekom AG angebunden zu werden. Abweichungen von Projekten müssen im SDSK entsprechend dokumentiert und durch das Sicherheitsmanagement der Deutschen Telekom AG bewertet werden.

Darüber hinaus dient dieses Anforderungspapier dazu, eine Bewertung zu bekommen welchen Sicherheitsstatus Clients haben, die im Rahmen eines eigenen Betriebes (EVC) an die die interne Backendinfrastruktur angebunden werden sollen.

Damit der Client einen Zugriff auf das Unternehmensnetzwerk erhält, sind jedoch weitere Freigaben oder Vorleistungen nötig (Netzwerk, RAS, VPN etc.).

Als 'Client' oder 'Client Computer' werden hier alle möglichen Geräteklassen und Betriebssysteme bezeichnet, wenn das Gerät im oben genannten Kontext genutzt wird. Allerdings stehen Desktop-Computer, Laptops und Tablets im Fokus dieses Dokuments. Normalerweise handelt es sich dabei um Geräte mit Windows-Betriebssystem, aber auch andere Systeme können relevant sein, wenn sie in diesem Zusammenhang genutzt werden.

2. Systemhärtung

Req 1	Die Sicherheitsmechanismen des BIOS/EFI müssen vorhanden sein und zur sicheren Nutzung konfiguriert werden.
-------	---

Zu den BIOS/EFI-Sicherheitsmechanismen gehören im Einzelnen:

- Schreibschutz-Option
- Passwortschutz durch ein Passwort das den Passwortrichtlinien des Konzerns Deutsche Telekom AG entspricht (siehe SiAnf Technischer Basisschutz)
- Boot-Reihenfolge
- Virenschutz, Virus-Warnfunktion
- Secure Boot
- etc.

So ist z.B. in der Bootreihenfolge festzulegen, dass ein Booten der Workstation von einem Wechseldatenträger unterbunden wird.

Motivation: Manipulationen am BIOS/EFI des Clients sind schwer zu detektieren bzw. ermöglichen den unberechtigten Zugriff auf schützenswerte Informationen des Clients. So lässt sich z.B. mit Booten von einem Wechseldatenträger bzw. USB-Stick vor dem Start von Windows/macOS die Software Kon-Boot starten, die einem volle Rechte eines Administrators auf dem Client verschafft.

Umsetzungsbeispiel: Ist die Schreibschutz-Option des BIOS im Client aktiviert, lässt sich der BIOS-Code im Flash-Speicher nicht überschreiben. Sicherheitsrelevante BIOS-Einstellungen lassen sich durch ein spezielles Administrator-kennwort vor Veränderung schützen, welches dem Workstation-Benutzer nicht bekannt ist. Der unberechtigte Zugriff auf installierte Datenträger und somit die unberechtigte Einsichtnahme von schützenswerte Informationen lässt sich bei bestimmten Angriffsmethoden verhindern, wenn die Bootreihenfolge eindeutig festgelegt und nicht unberechtigt veränderbar ist.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.19-1/7.0

Req 2	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 Download validiert werden, um die Identität des Bereitstellungs-Servers zu bestätigen; schlägt die Validierung fehl, ist der Download abubrechen 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 Bereitstellungskanäle 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 3 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 4 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

nen 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 5 Die Nutzung nicht freigegebener Software auf dem Client muss verhindert werden.

Das Einspielen bzw. Benutzen nicht freigegebener Anwendungen und Programmcodes (lokal installiert oder portabel ausgeführt) muss verhindert werden. Dies sollte durch technische Möglichkeiten soweit wie möglich verhindert werden oder kann durch die Einschränkung der Benutzerumgebung realisiert werden.

Motivation: Durch das Verwenden von portablen Anwendungen, z.B. Webbrowser lassen sich die Sicherheitseinstellungen des lokal installierten Webbrowsers umgehen und dadurch kann ggf. Schadcode auf den Client gelangen. Damit soll verhindert werden, dass Programme oder Skripte mit unerwünschten Auswirkungen eingebracht werden, die nicht nur lokal wirken sondern auch auf weitere Systeme Auswirkung haben können.

Zusätzlich soll verhindert werden, dass das System über den festgelegten Funktionsumfang hinaus unkontrolliert genutzt wird.

Umsetzungsbeispiel: Als technische Lösung unter Windows-Clients die Nutzung von Applocker bzw. einer 3rd-Party-Lösung wie EgoSecure Application Control, McAfee Application Control, Trendmicro Endpoint Application Control, AppSense Application Manager, etc.

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: 3.19-5/7.0

Req 6 Die Nutzung nicht freigegebener Hardware auf Clients muss verhindert werden.

Die Verwendung nicht freigegebener Hardware (ohne Öffnen des Gehäuses angebunden) muss verhindert werden. Dies sollte durch technische Möglichkeiten soweit wie möglich verhindert werden oder kann durch die Einschränkung der Benutzerumgebung realisiert werden.

Motivation: Durch das Verwenden von externer Hardware kann Schadsoftware auf die Workstation übertragen oder schützenswerte Daten abgegriffen werden.

Umsetzungsbeispiel: Die Installation externer Hardware kann über eine spezielle Gruppenrichtlinie reglementiert wer-

den.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.19-6/7.0

Req 7	Die Workstation muss entsprechend der Härtingsrichtlinien der Betriebssystemhersteller oder -distributoren bzw. gemäß "Security Best Practices" konfiguriert werden.
-------	--

Betriebssystemhersteller bzw. Distributoren, Sicherheitsorganisationen, etc. haben bereits entsprechende Kenntnisse in Härtung einer Workstation und bieten entsprechende Anleitungen, Härtungsskripte, etc. zur Verwendung an. Diese "Security Best Practices" können angewandt werden, sofern nicht diese nicht gegen anderslautende Sicherheitsanforderungen des Konzerns Deutsche Telekom AG oder der jeweiligen Geschäftseinheit verstoßen.

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

Umsetzungsbeispiel: Umsetzung der CIS Security Benchmarks (Stand 04/2015 <http://benchmarks.cisecurity.org/index.cfm>), der jeweiligen Herstellervorgaben wie z.B. von Microsoft (Stand 04/2015 <http://blogs.technet.com/b/secguide/archive/2014/08/13/security-baselines-for-windows-8-1-windows-server-2012-r2-and-internet-explorer-11-final.aspx>, etc.) oder staatlicher Institution wie das Bundesamt für Sicherheit in der Informationstechnik (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi-client-Anleitung_Windows-7.pdf?__blob=publicationFile).

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: 3.19-7/7.0

Req 8	Überflüssige bzw. nicht benötigte Tunneladapter müssen im Betriebssystem des Clients entfernt werden
-------	--

Motivation: Ein Tunneladapter verpackt Datenpakete eines anderen Verbindungsprotokolls in TCP/IP Pakete, um sie auf diese Weise über das Internet an die passende Gegenstelle zu senden. P2P-Netze arbeiten mit diesem Mechanismus, aber auch die Übersetzung von IPv6 zu IPv4 funktioniert so. Dadurch ist Informationsabfluss von der Workstation möglich.

Umsetzungsbeispiel: Die Tunneladapter (6zu4- beziehungsweise ISATAP-Adapter) lassen sich bei Windows-Clients im Gerätemanager sichtbar machen, wenn man unter *Ansicht* den Befehl *Ausgeblendete Geräte anzeigen* wählt. Allerdings kann man sie lediglich einzeln anklicken und löschen. Bequemer geht es mit dem Kommandozeilen-Programm *devcon.exe*, das auch mit neueren Windows-Versionen zusammenarbeitet.

Umsetzung der "Fix it"-Tools bei Windows-Clients unter <https://support.microsoft.com/en-us/kb/929852>.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.19-8/7.0

Req 9 Der Ad-hoc-Modus über die WLAN-Schnittstelle auf Workstations muss verhindert werden.

Motivation: Im Ad-hoc-Modus können Verbindungen zwischen mehreren WLAN-Clients ohne Nutzung eines Zugangspunkts hergestellt werden. Dieser Modus ist damit unsicher, da keine Zugangskontrolle erfolgt.

Umsetzungsbeispiel: Unterbindung unzulässiger und nicht kontrollierbarer Verbindungen zur Workstation.

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
- Unbemerkt durchführbare Angriffe

ID: 3.19-9/7.0

Req 10 Der Client muss über einen hostbasierten Paketfilter verfügen, welcher alle eingehenden Netzverbindungen blockiert und die Verbreitung von Schadcode unterbindet.

Zur Unterbindung der Verbreitung von Schadcode darf der hostbasierte Paketfilter ausschließlich angeforderte und festgelegte Services, wie z.B. SRTP (Secure Realtime Protocol) für Cisco Jabber etc., zulassen. Jedwede sonstige eingehende Kommunikationsverbindung muss blockiert werden.

Motivation: Durch den hostbasierten Paketfilter werden unerwünschte Verbindungsversuche von außen abgeblockt. Das können zum Beispiel sogenannte Portscans sein, bei denen ein potentieller Angreifer die möglichen Kontaktstellen zum Eindringen abprüft. Der hostbasierte Paketfilter soll die Verbreitung von Netz-Schadprogrammen eindämmen und Zugriffe von außen auf den Client kontrollieren.

Umsetzungsbeispiel: Nutzung eines hostbasierten Paketfilters oder Host Intrusion Prevention Systems (HIPS). Konfiguration des hostbasierten Paketfilters bei eingehenden Verbindungsversuchen auf festgelegte Gateways und Dienste wie SCCM, Active Directory, etc.

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: 3.19-10/7.0

Req 11 Remote-Support- und Administrations-Zugriffe auf den Client müssen über eine sichere Lösung erfolgen.

Remote-Support- und Administrations-Zugriffe auf den Client zur Störungsbehebung oder Wartung der Workstation müssen integritätsgeschützt, verschlüsselt und sicher authentifiziert werden. Zusätzlich müssen diese Verbindungen protokolliert werden und dürfen erst nach Genehmigung des Anwenders des Clients aufgebaut werden.

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: 3.19-11/7.0

3. Hardware

Req 12 Die Integrität der Systemkonfiguration des Clients muss festgestellt werden können.

Zur Systemkonfiguration eines Clients gehören Hardwarekomponenten sowie die Firmwareeinstellungen (BIOS/EFI). Deren Integrität muss feststellbar sein.

Motivation: Clients bieten eine Vielzahl von Zugriffsmöglichkeiten auf schutzbedürftige Informationen sowie materielle Werte. Durch eine Manipulation des BIOS/EFI (z.B. Rootkit Lightteater, etc.) könnte ggf. Schadcode im Flashspeicher dauerhaft installiert werden.

Umsetzungsbeispiel: Um das Risiko der Hardware- bzw. Firmwaremanipulation der Workstations zu minimieren, kann der Client hinsichtlich unbefugter Öffnung, mittels Siegeltechnik, Plomben (Laptops, Tablets) oder Schlössern (Desktop-Systeme) abgesichert werden. Alternativ können Geräte verwendet werden, welche den Zugang zu Hard- und Firmware ohnehin nicht ohne Weiteres ermöglichen (z.B. Microsoft Surface, Apple Macbook). Durch den Einsatz von Trusted Platform Modules (TPM) oder Intel AMT (Active Management Technology) kann die Integrität der Systemkomponenten überprüft und überwacht werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.19-12/7.0

Req 13 Nicht benötigte Hardwareschnittstellen müssen deaktiviert werden.

Nicht benötigte Hardwareschnittstellen müssen deaktiviert werden. Dies gilt insbesondere für unsichere Schnittstellen wie FireWire.

Motivation: Über Hardwareschnittstellen können Daten eingelesen, abgezogen und manipuliert werden, häufig auch wenn der Computer gesperrt ist. Über die FireWire-Schnittstelle ist es bspw. möglich per Direct Memory Access (DMA) ohne Authentisierung auf den Inhalt des Hauptspeichers zuzugreifen.

Umsetzungsbeispiel: Die Deaktivierung der betroffenen Schnittstellen im Nutzerkontext (z.B. per Gruppenrichtlinien) oder für das System generell in den BIOS/UEFI-Einstellungen.

ID: 3.19-13/7.0

Req 14 Ein Multimediagerät wie Kamera oder Mikrofon muss standardmäßig deaktiviert sein und darf Remote nicht aktivierbar sein.

Die standortferne, d.h. nicht lokale Steuerung des Multimediagerätes wie Kamera oder Mikrofon an der Workstation darf nicht möglich sein. Ein eindeutiger Hinweis (z.B. Lichtsignal auf dem Mediengerät) muss während der Aufnahme oder des Live-Streamings bemerkbar sein.

Das Mikrofon einer Workstation kann von denjenigen benutzt werden, die Zugriffsrechte auf die entsprechende Gerätedatei (unter Unix zum Beispiel /dev/audio) haben. Unter Windows bestimmen z.B. die Zugriffsrechte auf die entsprechenden Schlüssel der Registrierung (HKEY_LOCAL_MACHINE\HARDWARE\...), wer das Rechnermikrofon aktivieren kann. Die Aktivierung und Steuerung von Mediengeräten wie Kameras oder Mikrofonen muss auf den lokal angemeldeten Benutzer beschränkt werden. Der Betrieb eines Multimediagerätes ist deshalb durch einen eindeutig verifizierbaren Hinweis kenntlich zu machen.

Motivation: Ein Angreifer hat ggf. die Möglichkeit durch die Aktivierung der Multimediageräte, Personen oder Räume unbemerkt zu überwachen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Unbemerkt durchführbare Angriffe

ID: 3.19-14/7.0

4. Systemaktualisierung

Req 15	Das Betriebssystem und jede installierte Anwendung der Workstation muss innerhalb des Produktlebenszyklus betrieben werden.
--------	---

Das Microsoft-Betriebssystem der Workstation sollte innerhalb des Mainstream Supports betrieben werden und darf nicht über das Ende des Extended Supports hinaus betrieben werden. Das Mac-OS-Betriebssystem sollte nicht über die vom Apple Support gestützte Mac-OS-Version und deren ebenfalls durch den Support gestützte Vorgängerversion hinaus betrieben werden. Ein UNIX-/LINUX- und BSD-Betriebssystem darf nicht über den Zeitraum des uneingeschränkten Herstellersupports (z. Z. 7 Jahre bei Novell SuSE Linux und Red Hat Enterprise Linux) betrieben werden.

Motivation: Betriebssysteme enthalten aufgrund ihrer Komplexität sowie Designfehlern, kritische Fehler und Sicherheitslücken. Solche Lücken in älteren Betriebssystemen sind bekannt und können von unberechtigten Personen mit der Absicht ausgenutzt werden, um Viren oder ähnliche Schadsoftware in das Betriebssystem einzuschleusen oder um das Arbeitsplatzsystem für ihre Zwecke zu missbrauchen. Ältere Betriebssysteme bieten durch neue technische Möglichkeiten und Schwachstellen eine erhöhte Angriffsfläche, da durch den Hersteller keine Patches/Bugfixes mehr bereit gestellt werden, die eine bekannt gewordene Schwachstelle beheben.

Umsetzungsbeispiel: Eine Workstation mit Windows-Betriebssystem muss vor Ende des Extended Supports auf ein Betriebssystem im Mainstream Support migriert werden. Alternativ kann der Produktlebenszyklus durch Beschaffung des Custom Support beim Hersteller Microsoft entsprechend verlängert werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.19-15/7.0

Req 16	Bekannte Schwachstellen in der Software oder Hardware des Systems müssen behoben oder gegen Missbrauch abgesichert werden.
--------	--

Bekannte Schwachstellen in Software- und Hardware Komponenten müssen mittels Installation von verfügbaren Systemaktualisierungen des Herstellers (z. B. Patches, Updates/Upgrades) behoben werden. Alternativ ist der Einsatz von Workarounds (Akut-Lösungen, welche die Schwachstelle nicht beheben, aber die Ausnutzung wirksam verhindern) zulässig. Workarounds sollten grundlegend nur temporär Verwendung finden und sobald möglich durch eine reguläre Systemaktualisierung ersetzt werden, um die Schwachstellen vollständig zu schließen.

Komponenten, die bekannte, nicht behebbare Schwachstellen enthalten, dürfen in einem System nicht eingesetzt werden.

Die Behandlung von neu bekannt werdenden Schwachstellen muss zudem für die gesamte Einsatzphase des Systems fortlaufend sichergestellt und in den kontinuierlichen Betriebsprozessen eines Security Patch Managements umgesetzt werden.

Motivation: Der Einsatz von Komponenten ohne eine Behebung enthaltener Schwachstellen erhöht deutlich das Risiko einer erfolgreichen Kompromittierung. Der Angreifer wird zusätzlich dadurch begünstigt, dass i. d. R. nicht nur detaillierte Informationen zu bereits bekannt gewordenen Schwachstellen offen verfügbar sind, sondern oft auch bereits angepasste Angriffswerkzeuge, die eine aktive Ausnutzung erleichtern.

Umsetzungsbeispiel: Im Anschluss an die initiale Installation eines Betriebssystems von einem offiziellen Installationsmedium werden alle aktuell verfügbaren Patches und Sicherheits-Updates eingespielt.

Zusätzliche Informationen:

Primäre Quellen für bereits bekannt gewordene Schwachstellen in einer Software/Hardware sind Auflistungen in den Versionshinweisen sowie die Sicherheitshinweise aus den offiziellen Meldekanälen des Herstellers oder unabhängiger CERTs. Insbesondere die Meldekanäle werden sinnvollerweise fest in kontinuierliche Prozesse des Security Patch Managements für ein System eingebunden, damit neu bekanntwerdende Schwachstellen zeitnah registriert und in

operative Behebungsmaßnahmen geführt werden können.

Als ergänzende Maßnahme zur Aufdeckung von potenziell noch enthaltenen, grundsätzlich bereits bekannt gewordenen Arten von Schwachstellen können gezielte Schwachstellenuntersuchungen des Systems durchgeführt werden. Zu diesem Zweck eignen sich besonders spezialisierte Werkzeuge wie automatisierte Schwachstellen-Scanner. Beispiele hierfür sind: Tenable Nessus, Qualys Scanner Appliance.

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: 3.01-10/9.0

Req 17	Die Workstation muss stets über alle sicherheitsrelevanten Patches und Updates für Betriebssystem & Applikationen verfügen.
--------	---

Alle Updates, Bugfixes und Patches, die seitens des Herstellers / Distributors des Betriebssystems oder der Anwendung herausgegeben und publiziert wurden, müssen **so früh wie möglich** getestet und installiert werden. Für Updates, Bugfixes und Patches, die nach diesem Zeitpunkt durch den Hersteller / Distributor des Betriebssystems oder der Anwendung publiziert und herausgegeben werden muss ein Prozess für den Umgang mit diesen auf organisatorischer Ebene etabliert sein. Analog dazu gilt die identische Vorgehensweise für genehmigte Workarounds, sofern keine Updates, Bugfixes und Patches seitens des Herstellers / Distributors bereitgestellt werden.

Motivation: Nicht beseitigte Fehler im Betriebssystem können zu instabilen Systemzuständen und zu Systemabstürzen führen, bzw. können Sicherheitslücken gezielt für Angriffe auf Unternehmensnetze und –daten genutzt werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.19-17/7.0

Req 18	Eine Aktualisierung des Betriebssystems und der Applikationen der Workstation muss über sichere Updateserver erfolgen.
--------	--

Das Aktualisieren einer Workstation muss über gesicherte Softwareverteilungs- bzw. Updatemechanismen erfolgen. Es ist darauf zu achten, dass eine Aktualisierung von Komponenten der Workstation nicht unkontrolliert erfolgen darf. Gleiches gilt für sogenannte "Add-in-Käufe" bzw. "Nachladen von funktionalen Komponenten".

Motivation: Durch ein manipuliertes Update für das Betriebssystem kann Schadcode im Betriebssystemkernel installiert werden, der Zugriff auf vertrauliche Informationen ermöglicht oder den störungsfreien Betrieb der Workstation behindert, um sie ggf. für böswillige Zwecke zu missbrauchen.

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
- Unbemerkt durchführbare Angriffe

Req 19 Die Workstation muss über eine Endpoint Detection and Response (EDR) Lösung verfügen.

Auf der Workstation muss eine aktuelle EDR Lösung eingesetzt werden. Eine EDR Lösung sammelt sicherheitsrelevante Aktivitätsdaten von Prozessen und wertet diese zentral aus. Alarme können aus maliziösem Verhalten von Prozessen erzeugt werden oder auch durch eine bestimmte Signatur (wie klassische Virens Scanner). Zusätzlich ist es über eine zentrale Konsole möglich, direkt auf verdächtiges Programmverhalten zu reagieren. Der Client kann beispielsweise isoliert oder der maliziöse Prozess beendet werden. Darüber hinaus wird eine Übersicht der Schwachstellen aller Clients 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.

Umsetzungsbeispiel: Ein Beispiel für eine EDR Lösung ist Defender for Endpoint.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

5. Schutz von Daten und Informationen

Req 20 Der Client muss mit einer sicheren Lösung für eine Festplattenvollverschlüsselung ausgestattet sein.

Lösungen, welche eine Multi-Faktor-basierte Benutzer-Authentifizierung vor dem Betriebssystemstart (Pre-Boot-Authentication) erfordern und zentral verwaltet werden, erhöhen die Sicherheit und sollten an hochkritischen Arbeitsplätzen bevorzugt eingesetzt werden. Die Schlüssel zum Entschlüsseln der Festplatte sollten dabei an einem sicheren Ort abgespeichert werden. Als besonders sicher gelten hier externe Devices wie SmartCards oder USB-Sticks (Medientrennung).

Clients, welche auf einen festen Einsatzort beschränkt sind (mindestens SK1) können von der Anforderung ausgenommen werden.

Motivation: Systeme ohne eine Pre-Boot-Authentication sind anfällig gegen DMA- (Direct Memory Access) und Cold-Boot-Attacken, wenn keine weiteren Gegenmaßnahmen (z.B. Sperren der anfälligen Ports) getroffen werden.

Mittels eines Fremdbetriebssystems, welches von einem USB-Stick, einem anderen Wechseldatenträger oder der lokalen Festplatte gebootet wird, kann schreibend und lesend auf die Festplatte der Workstation zugegriffen werden und so unberechtigte Einsichtnahme schützenswerter Informationen möglich sein oder Manipulationen an dem Betriebssystem vorgenommen werden.

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
- Unbemerkt durchführbare Angriffe

ID: 3.19-20/7.0

Req 21 Der Client muss über sichere Tools und Applikationen verfügen, um eine Verarbeitung schutzbedürftiger Informationen entsprechend der Konzernrichtlinien und Schutzklassen zu ermöglichen.

Eine Auflistung von Tools, welche eine Verarbeitung schutzbedürftiger Informationen entsprechend der Konzernrichtlinien und Schutzklassen ermöglichen und für die dienstliche Nutzung freigegeben sind, ist vom zentralen Sicherheitsmanagement publiziert und im Intranet verfügbar: <https://yam-united.telekom.com/pages/informations-drehscheibe-das-portal/apps/content/produktfreigaben-2>

Alternative Tools können vom jeweils zuständigen Sicherheitsmanagement zur dienstlichen Nutzung freigegeben werden.

Motivation: Schutz vor unberechtigtem Zugriff auf schutzbedürftige Informationen auf Clients (auch temporäre Dateien).

Umsetzungsbeispiel: Installation und Nutzung von Container- oder File-Verschlüsselungslösungen. Installation und Nutzung von sicheren Löschmethoden, auch für temporäre Ordern (%TEMP%).

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.19-21/7.0

Req 22 Der Client muss über eine sichere Lösung verfügen, um externe Datenträger (z.B. USB-Sticks) zu verschlüsseln.

Motivation: Mithilfe externer Datenträger können Nutzer auf einfache Weise Daten von einem Client zum anderen transportieren. Dabei kann es schnell zu einem unerwünschten Datenabfluss kommen, wenn Unbefugte Zugang zu schützenswerten Informationen bekommen, bspw. bei Verlust oder Diebstahl des Datenträgers. Durch den Einsatz einer Verschlüsselungslösung für externe Datenträger wird der Zugriff auf die Informationen erschwert.

Umsetzungsbeispiel: Installation und Nutzung von Verschlüsselungslösungen für externe Datenträger.

ID: 3.19-22/7.0

Req 23 Eine Authentifizierungsinformation die über das Netzwerk gesendet wird, muss integritätsgesichert und verschlüsselt übertragen werden.

Motivation: Bei einer unverschlüsselten oder mit schwachen Verschlüsselungsmechanismen abgesicherten Netzwerkverbindung kann z.B. durch eine Man-in-the-Middle-Attacke die Authentifizierungsinformationen abgefangen werden und somit in den Besitz von Unbefugten gelangen. Damit bei der Übertragung über das Netzwerk die Authentifizierungsinformationen nicht abgefangen oder abgehört und verfälscht werden kann, muss die Kommunikation über eine ausreichend sicher verschlüsselte Verbindung erfolgen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten

ID: 3.19-23/7.0

Req 24 Werden Ordnerumleitungen oder Roaming Profiles eingesetzt, müssen schutzbedürftige Informationen verschlüsselt gespeichert und übertragen werden.

Benutzereinstellungen und Benutzerdateien werden in der Regel im lokalen Benutzerprofil im Ordner **Benutzer** gespeichert. Mithilfe der Ordnerumleitung wird der Pfad eines Ordners an einen neuen Speicherort (Ordner auf dem lokalen Computer oder ein Verzeichnis in einer Dateifreigabe im Netzwerk) umgeleitet, so dass die Informationen über jeden Computer im Netzwerk zur Verfügung stehen.

Motivation: Sicherheitsmechanismen der Workstation schützen bei Speicherung auf einer Dateifreigabe im Netzwerk nicht. So ist eine unberechtigte Einsichtnahme von schützenswerten Informationen möglich.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.19-24/7.0

Req 25 Zur Ver- oder Entschlüsselung benötigte Schlüssel müssen vor unberechtigten Zugriff geschützt werden.

Alle zur Ver- oder Entschlüsselung benötigten Schlüssel werden von Clientbetriebssystemen während der Benutzung in einem Hauptspeicherbereich abgelegt, der nicht in die Auslagerungsdatei verlagert wird. Dadurch soll gewährleistet werden, dass die Schlüssel nicht kompromittiert werden können, wenn ein unberechtigter Dritter Zugriff auf die Auslagerungsdatei erhält. Kritisch ist in diesem Zusammenhang die Verwendung des Ruhezustandes (*Hibernation Modus*) bzw. Energiesparmodus, da der gesamte Hauptspeicherbereich in eine Datei gespeichert wird, die dann notwendigerweise auch das Schlüsselmaterial enthält. Aus diesem Grund darf der Hibernation Modus bzw. Energiesparmodus nicht verwendet werden.

Motivation: Zugriff über die USB- bzw. Firewireschnittstelle, etc. auf die Hauptspeicherbereich enthaltenen Schlüssel

zur Ver- oder Entschlüsselung (cold boot attack).

Umsetzungsbeispiel: Vorhalten der Schlüssel zur Ver- oder Entschlüsselung auf sicheren, Verschlüsselungsmodulen wie TPM oder Smartcards, Deaktivierung des Ruhezustandes bzw. des Energiesparmodus.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Abstreiten von durchgeführten Aktionen

ID: 3.19-25/7.0

Req 26	Für Verschlüsselung müssen Protokolle und Algorithmen verwendet werden die als sicher gelten .
--------	--

Als unsicher geltende Protokolle und Algorithmen müssen an der Workstation deaktiviert werden.

Motivation: Unsichere Protokolle und Algorithmen wie LAN Manager, NTLMv¹, SSL 3.0, etc. bieten aufgrund von bekannten Schwachstellen die Möglichkeit eines Man in the Middle Angriffs.

Umsetzungsbeispiel: Als Verschlüsselungsprotokoll für die Datenübertragung muss TLS 1.2 oder höher mit PFS (Perfect Forward Secrecy) genutzt werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.19-26/7.0

Req 27	Bei Inaktivität des Nutzers muss der Client den Bildschirm nach einer angemessenen Zeit automatisch sperren und zur Reaktivierung eine Benutzeranmeldung anfordern.
--------	---

Der Benutzer muss den Client sperren (Bildschirmsperre), sobald er diesen unbeaufsichtigt zurücklässt. Nach einer angemessenen Zeit (Empfehlung 15 Minuten) muss das Gerät die Bildschirmsperre automatisch erzwingen. Bei mobilen Geräten und solchen Arbeitsplatzsystemen, die in Bereichen ohne Schutzklassifizierung (z.B. Rezeption, Info-Counter, Messestand, etc.) betrieben werden empfiehlt es sich dafür eine kürzere Zeitdauer zu konfigurieren.

Motivation: Verlässt ein Nutzer kurzzeitig seinen Arbeitsplatz, ist ein ungehinderter Zugriff auf Informationen für die der angemeldete Nutzer Berechtigungen besitzt für unbefugte Dritte möglich. Falls ein Nutzer seinen Arbeitsplatz verlässt ohne die Bildschirmsperre zu aktivieren, soll diese Einstellung den Schutz vor unbefugten Zugriff gewährleisten.

Umsetzungsbeispiel: Die automatische Bildschirmsperre lässt sich bei den meisten Betriebssystemen über die Systemeinstellungen konfigurieren und ggf. per Gruppenrichtlinie steuern. Bei Windows Clients empfiehlt sich die Verwendung eines zeitgesteuerten Bildschirmschoners, welcher zur Reaktivierung ein Passwort erfordert.

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
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.19-27/7.0

Req 28	Der Client darf nur über ein bootfähiges Betriebssystem verfügen.
--------	---

Etwaige Dual- oder Multi-Boot-Funktionalitäten des Clients (z.B. Apple Bootcamp) müssen deaktiviert werden. Sollte die Nutzung multipler Betriebssysteme aus betrieblichen Gründen dennoch erforderlich sein, so muss jedes Betriebs-

system die Sicherheitsanforderungen des Konzerns erfüllen und in einer separat verschlüsselten Partition, getrennt von anderen Betriebssystemen installiert sein.

Im Falle einer Festplattenverschlüsselung mit Pre-Boot Authentication gilt das Betriebssystem der Festplattenverschlüsselung als ein startfähiges Betriebssystem, welches ein weiteres Betriebssystem aus der zu entschlüsselnden Partition lädt und im Anschluss startet. Solche Lösungen sind von dieser Anforderung auszunehmen.

Motivation: Mittels einer Dual-Boot- oder Multi-Boot-Konfiguration kann von einer weiteren Partition der lokalen Festplatte ein Betriebssystem gebootet werden. Von diesem kann schreibend und lesend auf die installierte Festplatte der Workstation zugegriffen werden Daten ausgespäht, bzw. Daten oder das Betriebssystem manipuliert werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.19-28/7.0

Req 29	Alle Partitionen der Workstation müssen ein Dateisystem verwenden, welche die Semantik von NTFS abbildet und Access Control Lists verwendet.
--------	--

Windows Betriebssysteme bieten aus Gründen der Kompatibilität die Möglichkeit, alternative Dateisysteme zu verwenden. Es darf nur das Dateisystem NTFS oder gleichwertig/höher eingesetzt werden. Auf anderen Betriebssystemen dürfen dem Sicherheitsstandard von NTFS entsprechende Dateisysteme verwendet werden.

Motivation: FAT32 kann nicht die Sicherheit bieten, die z.B. das NTFS-Dateisystem bereitstellt. Wenn auf dem Client eine FAT32-Partition oder ein FAT32-Volume vorhanden ist, kann jeder Benutzer der auf die Workstation zugreift, auf alle darauf gespeicherten Informationen zugreifen. Nur NTFS oder ein gleichwertiges Dateisystem bietet Sicherheitseinstellungen wie beispielsweise Berechtigungen oder Überwachungseinstellungen.

Umsetzungsbeispiel: Es sollte auf dem Arbeitsplatzsystem ein Dateisystem verwendet werden, welche Access Control Lists und Journaling/Softupdates verwendet. Andere Dateisysteme wie NTFS, ext3, HFS+, JFS, XFS, etc. bieten im Gegensatz zu dem FAT-Dateisystem einen gezielten Zugriffsschutz auf Dateiebene sowie größere Datensicherheit durch Journaling.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.19-29/7.0

Req 30	Ordner bzw. Dateipfade die Auswirkung auf die Schutzfunktionen der Workstation haben, müssen vor Zugriff geschützt werden.
--------	--

Motivation: Es soll verhindert werden das beispielsweise bei Windows-Workstations z.B. durch unberechtigtem Zugriff auf das Verzeichnis %SystemRoot%\system32 ein Schadcode in Form einer dynamischen Programmbibliothek (dll-Datei) platziert werden kann (DLL preloading attack oder auch binary planting attack).

Umsetzungsbeispiel: Einschränkung der Rechte für normale Benutzer z.B. kein Schreibrecht für den Ordner %SystemRoot%\system32. Keine Erteilung von administrativen Rechten für Benutzer auf der Workstation, da diese einen Vollzugriff auf solche Verzeichnisse erlauben.

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
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.19-30/7.0

Req 31 Der selbstständige Aufbau von unkontrollierten Kommunikationsverbindungen durch das Betriebssystem, oder durch installierte Anwendungen der Workstation, muss verhindert werden.

Betriebssysteme, Anwendungen, Browser und Browser-Plugins, etc. bieten ggf. Funktionen wie „automatische Fehlerberichterstattung“, „automatisch fehlende Komponenten nachladen“, etc.. Solche und ähnliche Funktionen (call home) der Workstation, bzw. die daraus resultierende Datenverbindungen zu Parteien/Servern außerhalb des internen Netzwerkes des Konzerns Deutsche Telekom AG, müssen unterbunden werden.

Motivation: Mehrere Betriebssystemdienste und Anwendungen nehmen in der Standardkonfiguration selbsttätig und vom Benutzer unbemerkt Kontakt zu Servern im Internet auf. Dabei werden System- und/oder benutzerspezifische Daten an den Hersteller des Betriebssystems oder andere Anbieter übermittelt. Dabei ist nicht immer offensichtlich was außer seinen Nutz- und Protokollinformationen zusätzlich übertragen wird. Dabei können System- und/oder benutzerspezifische Daten wie. z.B Informationen über das Surfverhalten des Benutzers, etc. gesammelt werden und ohne Initiierung durch den Benutzer an unbefugte Dritte weitergeleitet werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.19-31/7.0

Req 32 Gespeicherte schutzbedürftige Daten müssen vor nicht autorisierter Einsichtnahme, Veränderung und Löschung geschützt werden.

Der Schutzbedarf für gespeicherte Daten ist abhängig von deren Einstufung (beispielsweise nach geltenden gesetzlichen Datenschutzvorgaben, regulatorischen Auflagen, vertraglichen Verpflichtungen), dem Schadenspotential bei deren Missbrauch, sowie weiteren relevanten Faktoren (beispielsweise dem Ort der Speicherung). Art und Umfang von Schutzmaßnahmen müssen entsprechend angemessen gewählt werden.

Gespeicherte Authentisierungsmerkmale wie beispielsweise Passwörter, Private Keys, Tokens oder Zertifikate gelten grundsätzlich als schutzbedürftig. Ebenfalls als grundsätzlich schutzbedürftig gelten Daten, die Funktionalität und sicherheitsrelevantes Verhalten eines Systems bestimmen (z. B. System-Konfigurationsdateien, Betriebssysteme und Kernel, Treiber).

Die Einhaltung der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit muss für gespeicherte schutzbedürftige Daten durchgängig gewährleistet werden. Dies gilt auch während einer lediglich kurzfristigen Speicherung (z. B. bei der Zwischenspeicherung in einem Web Cache oder in einem temporären Ordner innerhalb einer Datenverarbeitungskette).

Grundlegend muss der Zugriff auf schutzbedürftige Daten in einem System auf Basis von technisch implementierten Berechtigungsvergaben und -kontrollen vollumfassend reglementiert werden.

Reicht eine solche technische Zugriffskontrolle allein nicht mehr aus, um den erforderlichen Schutzbedarf gespeicherter Daten zu gewährleisten, oder kann deren Wirksamkeit nicht durchgängig sichergestellt werden, müssen zusätzlich kryptografische Verfahren (z. B. Verschlüsselung, Signierung, Hashing) implementiert werden. Bei der Speicherung von Daten eingesetzte kryptografische Verfahren müssen für diesen Zweck anerkannt wirksam sein und dürfen keine bekannten Schwachstellen aufweisen.

Motivation: Die Speicherung von Daten auf einem System ohne einen adäquaten Schutz ermöglicht es einem Angreifer, diese unberechtigt einzusehen, zu nutzen, zu verbreiten, zu verändern, oder zu vernichten. Dies eröffnet potenziell zusätzliche Angriffsvektoren auf die unmittelbaren sowie angeschlossene weitere Systeme und kann zu erheblichen Ausfällen, Kontrollverlusten und Schäden sowie resultierenden Strafzahlungsforderungen und Reputationsverlusten

gegenüber Kunden und Geschäftspartnern führen.

Umsetzungsbeispiel: [Beispiel 1]

Ein System exportiert Daten für einen Transport auf einen mobilen Datenträger. Da die technische Zugriffskontrolle des Systems auf Dateiberechtigungsebene nicht mehr greift, sobald der mobile Datenträger aus dem System entfernt wird, müssen zusätzliche Maßnahmen zum Schutz der Daten getroffen sein. Bevor das System die Daten auf den mobilen Datenträger schreibt, werden sie entsprechend mit einem passenden Verfahren verschlüsselt. Der zugehörige Schlüssel wird auf einem separaten Kanal ausgetauscht, so dass die Daten im legitimen Zielsystem wieder entschlüsselt und verarbeitet werden können. Ein Angreifer, der den mobilen Datenträger in seinen Besitz bringt, hat hingegen keinen Zugriff auf die Daten.

[Beispiel 2]

In der lokalen Benutzer-Datenbank eines Systems werden nur kryptografische Hashes der Passwörter gespeichert, die mit einem als sicher geltenden Password-Hashing Verfahren erzeugt wurden. Für das System sind diese Hashes ausreichend, um die Benutzer bei einer Anmeldung am System zu authentifizieren. Sollte ein Angreifer die Benutzer-Datenbank kopieren können, gelangt er somit jedoch nicht unmittelbar in den Besitz von Klartext-Passwörtern, mit denen er sich am System im Namen der Benutzer anmelden könnte.

[Beispiel 3]

Auf einem System sind die Konfigurationsdateien des Web-Servers ausschließlich für den legitimen Admin schreibbar, in dem im Dateisystem entsprechende Berechtigungen gesetzt wurden. Die Zugriffskontrolle des Betriebssystem-Kernels verweigert somit allen anderen Benutzern des Systems, Veränderungen an den Konfigurationsdateien des Web-Servers vorzunehmen; einschließlich dem Web-Server Dienste-Konto selbst, was auch die Angriffsfläche von außen bei Schwachstellen im Web-Server verkleinert.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.01-14/9.0

Req 33	Schutzbedürftige Daten müssen während der Übertragung vor nicht autorisierter Einsichtnahme und Veränderung geschützt werden.
--------	---

Der Schutzbedarf von zu übertragenden Daten ist abhängig von deren Einstufung (beispielsweise nach geltenden gesetzlichen Datenschutzvorgaben, regulatorischen Auflagen, vertraglichen Verpflichtungen), dem Schadenspotential bei deren Missbrauch, sowie weiteren relevanten Faktoren (beispielsweise der Übertragung über öffentliche Netze). Art und Umfang der Schutzmaßnahmen müssen entsprechend angemessen gewählt werden.

Authentisierungsmerkmale wie beispielsweise Passwörter oder Tokens gelten grundsätzlich als schutzbedürftige Daten. Ebenfalls grundsätzlich als schutzbedürftig gelten Daten, die Funktionalität und sicherheitsrelevantes Verhalten eines Systems bestimmen (z. B. Updates & Patches, Konfigurationsparameter, Fernwartungen, Steuerung über APIs).

Die Einhaltung der Schutzziele Vertraulichkeit und Integrität muss während der Übertragung von schutzbedürftigen Daten durchgängig gewährleistet werden.

I.d.R. erfordert dies eine Implementation von kryptografischen Verfahren (z. B. Verschlüsselung, Signaturen, Hashes). Kryptografische Verfahren können

- vor der Übertragung direkt auf die Daten angewendet werden, was eine anschließende Übertragung der Daten auch über unsichere Kanäle vertretbar machen kann
- auf dem Übertragungs-Kanal eingesetzt sein, um einen sicheren Kanal zu schaffen und beliebige Daten, die durch diesen geleitet werden, zu schützen
- oder auch als Kombination aus beidem umgesetzt sein.

Bei der Übertragung von Daten eingesetzte kryptografische Verfahren müssen für diesen Zweck anerkannt wirksam sein und dürfen keine bekannten Schwachstellen aufweisen.

Motivation: Die Übertragung von Daten ohne einen adäquaten Schutz ermöglicht es einem Angreifer, diese unberechtigt abzufangen, zu nutzen, zu verbreiten, zu verändern oder aus der Übertragung zu entfernen. Dies eröffnet potenziell weitere Angriffsvektoren auf die unmittelbaren Zielsysteme sowie angeschlossene weitere Systeme und kann zu erheblichen Ausfällen, Kontrollverlusten und Schäden sowie resultierenden Strafzahlungsforderungen und Reputationsverlusten gegenüber Kunden und Geschäftspartnern führen.

Umsetzungsbeispiel: [Beispiel 1]

Vertrauliche Dokumente werden vor dem Versand per E-Mail an den Kunden verschlüsselt.

[Beispiel 2]

Ein Administrator konfiguriert eine neue Cloud-Anwendung über das Internet. Der Zugriff erfolgt über eine TLS-verschlüsselte Verbindung ("https").

[Beispiel 3]

Ein System bezieht automatische Software-Updates von einem Update-Server. Der Update-Server liefert die Software Updates kryptografisch signiert aus. Das System kann die empfangenen Software-Updates somit validieren und sicher ausschließen, dass diese während der Übertragung manipuliert wurden.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.01-15/9.0

6. Verfügbarkeit und Integrität

Req 34	Zum Schutz der Workstation muss ein hostbasiertes Intrusion Prevention System installiert und konfiguriert werden.
--------	--

Das hostbasierte Intrusion Prevention System muss die Infektion mit Schadprogrammen von außerhalb und einen Netzangriff verhindern. Ebenfalls muss es die Verbreitung von Schadcode durch eine infizierte Workstation verhindern.

Motivation: Um einen potentiellen Angriff gegen und auf dem Arbeitsplatzsystem zu erkennen, nutzt ein hostbasiertes Intrusion Prevention System detaillierte Daten über Systemprozesse, Ressourcenverwendung und Geräteaktivität, die netzbasierten Sensoren fehlen um ggf. den Datenpakete zu verwerfen, die Verbindung zu unterbrechen oder die übertragenen Daten zu ändern. Der Einsatz eines hostbasierten Paketfilters ist hinsichtlich der Funktionalität und der Widerstandsfähigkeit grundsätzlich begrenzt. Ziel ist es, durch einen kombinierten Einsatz von hostbasierten Paketfiltern und Intrusion Prevention System bestehende Restrisiken auf ein tragbares Maß zu reduzieren.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.19-34/7.0

Req 35	Die Funktion der Anzeige von Dateinamenserweiterungen in der Workstation muss aktiviert sein.
--------	---

Motivation: Windows blendet häufig die Datei-Endung aus, das birgt jedoch eine Sicherheitsfalle! Angreifer können eine schädliche Datei umbenennen von „harmlos.exe“ in „harmlos.jpg.exe“. Der Anwender erkennt nur „harmlos.jpg“ und erwartet eine Bild-Datei, allerdings wird mit dem Doppelklick bzw. der Bestätigung durch den Anwender die gewünschte .exe ausgeführt.

Umsetzungsbeispiel: Im Windows Explorer die „Ordneroptionen“ aufrufen und den Reiter „Ansicht“ auswählen. Entfernung vom Häkchen bei „Erweiterungen bei bekannten Dateitypen ausblenden“ und Änderung übernehmen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 3.19-35/7.0

Req 36	Ein mobiles Speichermedium/-gerät muss beim Zugriff durch die Workstation auf Schadcode überprüft werden.
--------	---

Motivation: Durch so genannte Shared Executable Files verbreitet sich Malware heimlich über portable Geräte wie USB-Sticks oder externe Festplatten. Anwender geben den Schadcode manuell an andere weiter, so wie sie es früher mit Disketten taten. Schadcode wird verstärkt über mobile Speichermedien/-geräte verbreitet um Workstations zu infizieren.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 3.19-36/7.0

Req 37	Sicherheitsfunktionen der Workstation wie DEP, ASLR, etc. müssen konfiguriert und durch das Betriebssystem und die Anwendungen genutzt werden.
--------	--

Im Jahr 2013 fand Secunia in den 50 meistgenutzten Anwendungen 1208 Sicherheitslücken. Nur 24 Prozent davon steckten in Programmen von Microsoft. Installierte Anwendungen müssen daher mit einem Zusatzschutz gegen Sicherheitslücken ausgestattet werden.

Zu diesen Sicherheitsfunktionalitäten zählen unter anderem:

- DEP (Data Execution Prevention)
- ASLR (Address Space Layout Randomization)
- ASR (Attack Surface Reduction)
- etc.

Motivation: Erst wenn neue Viren oder Trojaner auftreten, können die Hersteller von Antivirensoftware Gegenmaßnahmen ergreifen. Dies ist umso gefährlicher, wenn Sicherheitslücken bekannt werden, deren Behebung über Updates lange dauert oder Updates/Patches aufgrund interner Tests nur mit großer Verzögerung ausgerollt werden können.

Im Fall solcher „Zero-Day-Exploits“ und bei allgemeinen Bedrohungen kann die Nutzung der Sicherheitsfunktionalitäten helfen, die Gefahren zu reduzieren. Diese Technologien stellen spezielle Schutzmechanismen bereit und richten Hindernisse ein, die ein Angreifer überwinden muss, um Sicherheitslücken in der Software ausnutzen zu können.

Umsetzungsbeispiel: Bei Windows-Workstations die Installation und Konfiguration des Enhanced Mitigation Experience Toolkit (EMET).

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: 3.19-37/7.0

7. Authentifizierung und Autorisierung

Req 38 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 39 Der automatische Login (AutoLogon) an der Workstation muss verhindert werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.19-39/7.0

Req 40 Auf mobilen Endgeräten (z.B. Laptops, Tablets) ohne direkte Anbindung an das Unternehmensnetzwerk muss die Authentifizierung am Client mit mindestens zwei Faktoren geschehen.

Ist ein Client nicht direkt mit dem Unternehmensnetzwerk verbunden, so muss sich der Nutzer am Client mit mindestens zwei Faktoren authentifizieren.

Dazu gehören die Faktoren

- Wissen (Passwort, PIN, ...)
- Besitz (Zertifikat, Mobiles Endgerät, ...)

- Biometrie (Fingerabdruck, Irismuster, ...)

von denen beliebig viele Authentisierungsmerkmale genutzt und kombiniert werden können. Als besonders sicher gelten Verfahren bei denen die Authentisierungsmerkmale getrennt voneinander gehalten werden (Medientrennung), bspw. Zertifikat auf SmartCard + PIN-Eingabe auf dem Client.

Geräte, welche an einem Unternehmensstandort direkt mit dem Unternehmensnetzwerk verbunden sind (über VLAN Office oder CWLAN Office), können hiervon ausgenommen werden.

Motivation: Das Kurzzeitgedächtnis des menschlichen Gehirns kann lediglich zwischen fünf und neun zufällige Zeichen speichern (der Durchschnitt liegt bei sieben Zeichen). Da sich ein Großteil der Benutzer ein Kennwort mit mehr als acht Zeichen nicht einprägen kann, notieren sich ggf. viele das Kennwort an einer Stelle die potentiellen Angreifern die Möglichkeit gibt, sich die Anmeldeinformationen anzueignen.

Ein langes Kennwort mit mehr als 14 Zeichen, das sich aus zufällig ausgewählten Buchstaben, Zahlen und Sonderzeichen zusammensetzt, kann sehr schwer zu entschlüsseln sein, Rainbow Tables sind nach aktuellem Stand (Mai 2015) ebenfalls nicht berechnet. Leider ist das menschliche Gehirn nicht immer in der Lage, sich solche Kennwörter einzuprägen. Eine Zwei-Faktoren-Authentifizierung reduziert die Wahrscheinlichkeit des unberechtigten Zugriffs auf den Client deutlich.

Mittels Single Sign On - Mechanismen des installierten Betriebssystems ist es nach Anmeldung mittels eines ermittelten Kennwortes möglich auf weitere Dienste zuzugreifen und so unberechtigt auf schützenswerte Informationen zuzugreifen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.19-40/7.0

Req 41	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 "Taste" funktioniert und somit der 2. Faktor ("Inhärenz") nicht gegeben 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 42 Das lokale Administratorenkonto der Workstation muss deaktiviert sein.

Motivation: An einer Workstation mit Windows-Betriebssystem wird der geänderte Kontoname des integrierten Administrators anhand seiner eindeutigen SID ermittelt und mittels Brute-Force-Attacke können mehrere Anmeldeversuche an der Workstation durchgeführt werden. Alle Windows-Betriebssysteme werden mit einem ersten lokalen Administratorenkonto ausgeliefert, dessen technische Sicherheitskennung (SID) in allen Windows-Betriebssystemen stets identisch ist. Dieses Konto kann nicht gesperrt werden, wenn ungültige Anmeldeversuche ausgeführt werden. Eine Umbenennung dieses Kontos erhöht die Sicherheit nicht.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.19-42/7.0

Req 43 Das vordefinierte lokale Gäste-Konto muss deaktiviert sein.

Motivation: Mittels eines Exploits ist es möglich, dass ein Angreifer auf der Windows-Workstation das Gäste-Konto der Gruppe Administratoren hinzufügt oder dem Konto weitere Rechte verschafft. Das vordefinierte lokale Gäste-Konto stellt eine Schwachstelle dar, da mit dessen Identität gegenüber dem Betriebssystem Erkenntnisse gewonnen werden könnten, die Angriffe begünstigen.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.19-43/7.0

Req 44 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 45	Das Prinzip der minimalen Rechte bzw. „need to know“ Prinzip muss für Accounts, Anwendungen und Schnittstellen angewendet werden.
--------	---

Es muss ermittelt werden, welche Aufgaben der Benutzer auf der Workstation hat und es muss bestimmt werden, welche Mindestrechte sich daraus ableiten. Die Workstation muss von den Rechten so eingeschränkt werden, dass diese nichts beinhalten, was über die abgeleiteten Mindestrechte hinausgeht. Ein Zugriff durch lokal angemeldete Nutzer auf schützenswerte Verzeichnisse der Workstation (Verzeichnisse anderer Nutzer, System- und Programmverzeichnisse des Betriebssystems, etc.) muss verhindert werden. Ebenso muss verhindert werden, dass ein Nutzer unberechtigt Funktionen, Programme bzw. Schnittstellen aktiviert/deaktiviert.

Anwendungen bzw. Dienste auf der Workstation müssen mit so wenigen Rechten wie möglich installiert werden. Schreib- und Leseberechtigungen für schutzbedürftige Informationen und Verzeichnisse müssen z.B. mittels ACLs so restriktiv wie möglich gesetzt werden.

Motivation: Wird z.B. der Webbrowser mit einer noch nicht geschlossenen Schwachstelle mit Administratorenrechten gestartet und eine manipulierte Web-Seite aufgerufen, nutzt diese ggf. die Schwachstelle ohne Interaktion des Benutzers und installiert Schadcode auf der Workstation. Arbeitet ein Nutzer an der Workstation mit erweiterten Rechten, erhöht dies das Risiko bei der Einwirkung von Programmen, die im Rechtekontext des Benutzers ausgeführt werden.

Umsetzungsbeispiel: Ein Konto mit erweiterten Rechten wie z.B. als Mitglieder der Gruppe „Administratoren“ oder „Hauptbenutzer“ darf nicht für den normalen Tätigkeitsbetrieb genutzt werden. Ein Nutzer auf der Workstation muss für die normale tägliche Arbeit ein Konto mit eingeschränkten Rechten verwenden.

Schutzbedürftige Dateien und Verzeichnisse wie %systemroot% oder %programfiles% müssen ebenso wie relevante Anteile der Registry vor dem Zugriff durch den Anwender geschützt werden. Diese dürfen in diesen Verzeichnissen oder diese Daten weder schreiben, ändern noch löschen können. Deshalb sollten z.B. die Standard-Windows-ACLs (Access Control Lists) nicht verändert werden.

Installierte Anwendungen können vor Rollout mittels des Microsoft Attack Surface Analyzer auf Rechte bzw. Funktionen überprüft werden (<https://www.microsoft.com/en-us/download/details.aspx?id=24487>).

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: 3.19-45/7.0

Req 46	Es muss verhindert werden, dass sicherheitskritische Einstellungen der Workstation oder der installierten Anwendungen durch den Benutzer geändert werden können.
--------	--

Die Bedienungsfelder oder Zugriffsmöglichkeiten für die Veränderung sicherheitskritischer Einstellungen bei Betriebssystemen und Anwendungen auf der Workstation müssen für den angemeldeten Benutzer deaktiviert sein und/oder durch andere technische Maßnahmen für den Benutzer nicht bedienbar sein. Dies gilt gleichermaßen für andere relevante Mechanismen (Registry, API-Call, etc.).

Motivation: Beispielsweise durch die Veränderung der Einstellungen für die Funktion „Vertrauenswürdige Sites“ im Internet Explorer kann eine manipulierte Webseite mit Schadcode als vertrauenswürdig eingestuft werden, die dann ggf. auf der lokalen Workstation Manipulationen vornimmt. Benutzer könnten damit etablierte Sicherheitseinstellungen unbewusst deaktivieren und somit eine potentielle Sicherheitslücke für Schadcode öffnen.

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
- Abstreiten von durchgeführten Aktionen

Req 47	Für die Administration und den Support der Workstation muss ein Domänenkonto des Active Directory Verzeichnis des Konzerns Deutschen Telekom AG verwendet werden.
--------	---

Ein erforderlicher Administrationsvorgang und/oder eine Fehlerbehebung im Supportfall darf nicht über ein lokales Administratorkonto erfolgen. Das zu verwendende Domänenkonto darf nicht Mitglied der Domänenbenutzerkonten sein, die für die tägliche Arbeit verwendet werden. Ferner darf kein einheitliches oder ableitbares Masterpasswort für alle Workstations genutzt werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Abstreiten von durchgeführten Aktionen

Req 48	Falls Passwörter als Authentisierungsmerkmal genutzt werden, müssen diese mindestens 12 Zeichen lang sein und drei der folgenden Zeichenkategorien beinhalten: Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen.
--------	--

Ein System darf nur Passwörter akzeptieren, welche die folgende Komplexität erfüllen:

- Mindestlänge 12 Zeichen
- Bestehend aus mindestens drei der folgenden vier Zeichenkategorien:
 - Kleinbuchstaben
 - Großbuchstaben
 - Ziffern
 - Sonderzeichen

Die maximal mögliche Länge für Passwörter sollte 25 Zeichen oder mehr betragen. Dies unterstützt Endbenutzer bei Bedarf mit mehr Freiraum, um individuelle merkbare Passwörter bilden zu können, und hilft so, unerwünschte Verhaltensweisen im Umgang mit Passwörtern zu vermeiden, welche durch stark eingeschränkte maximale Passwortlängen provoziert werden können.

Das System muss bei der Vergabe eines Passwortes sicherstellen, dass das Passwort diesen Bildungsregeln entspricht; vorzugsweise mittels technischer Maßnahmen, falls solche aber nicht umsetzbar sein sollten, ersatzweise mittels organisatorischer Maßnahmen.

Bei Verwendung eines zentralen Systems für die Authentisierung der Benutzer [vgl. Wurzel-Anforderungsdokument "[I]3.69 IAM (Identity Access Management) - Framework"] darf diese Aufgabe an das zentrale System weitergereicht bzw. dorthin ausgelagert werden.

Zulässige Abweichung in der Passwort-Mindestlänge

Unter sicherheitsbezogenen Kriterien lassen sich für ein System potenziell Bedingungen identifizieren, die eine Reduzierung der Passwort-Mindestlänge ermöglichen:

- Allgemein zulässig ist eine Reduzierung der Passwort-Mindestlänge für Systeme, die innerhalb des Authentisierungsprozess zusätzlich zum Passwort weitere unabhängige Authentisierungsmerkmale verwenden (Umsetzung von 2-Faktor oder Multi-Faktor Authentisierung).
- Eine Reduzierung der Passwort-Mindestlänge muss grundsätzlich durch einen fachlichen Sicherheitsberater (z. B. ein PSM der Telekom Security) individuell bewertet und als zulässig bestätigt werden. In der Bewertung müssen umgebende technische, organisatorische und gesetzliche Rahmenparameter berücksichtigt sowie der systemspezifische Schutzbedarf und die potenzielle Schadenshöhe bei Sicherheitsvorfällen einbezogen werden.
- Der absolute Mindestwert von 8 Zeichen Länge darf für Passwörter grundsätzlich nicht unterschritten werden.

Motivation: Passwörter mit der genannten Komplexität bieten eine zeitgemäße Robustheit gegen Angriffe bei gleichzeitig akzeptabler Benutzerfreundlichkeit. In der Praxis haben sich Passwörter mit dieser Komplexität bewährt. Triviale und zu kurze Passwörter sind anfällig für Brute-Force- und Wörterbuch-Angriffe und von einem Angreifer leicht zu ermitteln. Ein 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
- Abstreiten von durchgeführten Aktionen

ID: 3.01-26/9.0

Req 49	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 50	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 fehlgeschlagenen 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 51	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

Req 52	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 uneingeschränkt 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 längstmögliche 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

8. Protokollierung

Req 53 Sicherheitsrelevante Windows Betriebssystem Events müssen mit genauem Zeitstempel und einer eindeutigen Systembezeichnung protokolliert werden.

Windows Betriebssystem Events müssen das Auftreten von sicherheitsrelevanten Ereignissen protokollieren. Um eine Auswertbarkeit und Zuordnung 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 müssen die jeweils geltenden gesetzlichen, tariflichen und betrieblichen Bestimmungen beachtet werden. Diese besagen unter anderem, dass die Protokollierung von Ereignissen nur zweckgebunden erfolgen darf. Eine Protokollierung zum Zwecke der Arbeitskontrolle von Mitarbeitern ist nicht zulässig.

Typische Ereignisse sind:

Ereignis	Zu protokollierende Daten des Ereignisses
Erfolgreiche Anmeldung/Verwendung von Accounts	- Konto - Quelle (IP-Adresse) bei entferntem Zugriff - LogonType - Art des Log-ons (Prozess und LogonType, beides enthalten in 4624) - Berechtigung des Log-ons (4672) - Session ID
Log-off eines Accounts	- Session ID - Account
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))	- Betroffene Event IDs (Keine vollständige Liste): • Scheduled TasksSecurity.evtx: 4624, 4672, 4698, 4702, 4699, 4700, 4701Microsoft-Windows-Task-Scheduler%4Operational.evtx: 106, 140, 141, 200, 201 • ServicesSecurity.evtx: 4624 Logon Type 3, 4697system.evtx: 7034, 7035, 7036, 7040, 745 • WMI\Security.evtx: 4624 Logon Type 3, 4672Microsoft-Windows-WMI-Activity%4Operational.evtx: 5857, 5860, 5861 - Grundsätzlich sollten folgende Informationen in den Logs für Autostartdienste enthalten sein • Gestartetes Programm • Startbedingung • Rechte des Prozesses
Logmanipulationen	- Löschung der Logdateien (Event ID 1102)

Verwendung von Remotekommandos; eingehend und ausgehend	- WMI Remoting • Security.evtx: 4624, 4672 • Microsoft-Windows-WMI-Activity%4Operational.evtx: 5857, 5860, 5861 - PowerShell Remoting • Security.evtx: 4624, 4672 • Microsoft-Windows-PowerShell%4Operational.evtx: 4103, 4104, 53504 • Windows PowerShell.evtx: 400, 403, 800 • Microsoft-Windows-WinRM\$4Operational.evtx: 91, 168
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

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: 3.19-53/7.0

Req 54 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 angebotenen 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

Req 55	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 Abhän-

gigkeiten 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 56	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 57	Sicherheitsrelevante Protokollierungsdaten müssen umgehend nach deren Erzeugung an einen Log-Server weitergeleitet werden.
--------	--

Die sicherheitsrelevanten Protokollierungsdaten des Systems müssen umgehend nach deren Erzeugung an einen Log-Server weitergeleitet werden.

Im Sinne der Anforderung muss der dafür genutzte Log-Server die folgenden Kriterien erfüllen:

- Der Log-Server muss dediziert für die Vorhaltung von Protokollierungsdaten eingesetzt sein. Er darf keine weiteren Funktionen oder Dienste abbilden, die nicht in Relation zu dieser Aufgabe stehen. Eine zulässige Ausnahme ist die Kombination eines Log Servers mit einer SIEM (Security Information and Event Management) Lösung.
- Der Log-Server muss vom System separiert sein. Er darf nicht als zusätzliches Modul unmittelbar mit auf dem System betrieben werden.
- Der Log-Server muss zentral für die Einsatzumgebung bereitstehen, zu der auch das System gehört.

Zur Übertragung der Protokollierungsdaten an den Log-Server sollten bevorzugt auf diesen Zweck spezialisierte Standard-Protokolle (z. B. Syslog oder SNMPv3) zum Einsatz kommen.

Motivation: Werden Protokollierungsdaten nur lokal gespeichert, können diese im Fall einer erfolgreichen Kompromittierung des Systems durch einen Angreifer manipuliert werden, um dessen Angriff und auf dem System durchgeführte Aktionen zu verschleiern. Aus diesem Grund muss die Weiterleitung von Protokollierungsdaten an einen Log-Server sehr zeitnah nach dem Auftreten eines sicherheitsrelevanten Ereignisses im Quell-System erfolgen. So stehen die angefallenen Protokollierungsdaten separiert vom Quell-System und unabhängig von dessen Zustand jederzeit für Analysen bereit. Die Verwendung eines zentralen Log-Servers für eine Einsatzumgebung stellt sicher, dass auf die Logs sämtlicher IT/NT-Systeme dieser Einsatzumgebung schnell und einheitlich zugegriffen und der Zugriff selbst optimal in die Incident-Prozesse der Umgebung integriert werden kann.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Modifikation von Daten
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.01-35/9.0

Req 58	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 auf-

bewahrt 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 59	Die Workstation muss über zentrale Richtlinien konfiguriert, gesteuert und deren Einhaltung überwacht werden.
--------	---

Motivation: Mittels zentraler Richtlinien lassen sich mehrere Workstations, die einer Domäne angehören, gleich konfigurieren. Eine Verletzung durch Angreifer bzw. bösartigen Code gegenüber diesen Richtlinien, kann durch geeignete Protokollierungsmechanismen erfasst werden, um entsprechende Maßnahmen zu ergreifen.

Umsetzungsbeispiel: Über Gruppenrichtlinien oder Group Policy Objects (GPOs) lassen sich ähnlich der Registrierungsdatenbank diverse Programmeinstellungen setzen oder Sicherheitseinstellungen anwenden. Hierzu müssen die Gruppenrichtlinien für jedes Betriebssystem bzw. jeden Anwendungsfall entsprechend konfiguriert werden. Eine Übersicht der verfügbaren GPOs bei Windows Systemen findet man unter <https://www.microsoft.com/en-us/download/details.aspx?id=25250> oder auch online unter <http://gpsearch.azurewebsites.net/>.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.19-59/7.0