

Sicherheitsanforderung

Hyper-V Server

Deutsche Telekom Gruppe

Version	8.0
Datum	01.07.2025
Status	Freigegeben

Impressum

Herausgeber
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Deutschland

Dateiname	Dokumentennummer 3.49	Dokumententyp Sicherheitsanforderung
Version 8.0	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
Hyper-V Server

Copyright © 2025 by Deutsche Telekom AG.

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

Inhaltsverzeichnis

1.	Einleitung	4
2.	Abhängigkeiten	5
3.	Systemhärtung	6
4.	Systemaktualisierung	14
5.	Schutz von Daten und Informationen	17
6.	Schutz der Verfügbarkeit und Integrität	25
7.	Authentifizierung und Autorisierung	29
8.	Schutz von Sitzungen	39
9.	Authentisierungsmerkmal Passwort	40
10.	Protokollierung	47

1. Einleitung

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

2. Abhängigkeiten

Die meisten Anforderungen aus diesem Dokument ergeben sich aus den generellen Sicherheitsanforderungen für Virtualisierungsumgebungen, die in der Sicherheitsanforderung 3.35 „IT Virtualisierungs-Lösungen“ festgelegt werden. Darüber hinaus sind auch für die virtuellen Maschinen (Guests) die Anforderungen aus der Sicherheitsanforderung 3.37 „Betriebssysteme“ und generell die Anforderungen aus dem Dokument 3.1 „Technischer Basisschutz von IT-/NT-Systemen“ und 3.14 „Architekturen für Netzdienste und Rechenzentren“ zu beachten. Für einen Hyper-V Server sind die Anforderungen in diesen Dokumenten verbindlich.

3. Systemhärtung

Req 1 Nicht benötigte Dienste müssen deaktiviert werden.

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

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

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

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

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.01-5/9.0

Req 2 Die Erreichbarkeit von aktivierten Diensten muss eingeschränkt werden.

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

Die Erreichbarkeit eines Dienstes über die erforderlichen Schnittstellen muss zudem auf legitime Kommunikationspartner eingeschränkt werden. Die Einschränkung ist durch eine entsprechende Konfiguration des Dienstes bzw. Betriebssystems oder mittels eines lokalen Filters ("Host Firewall") umzusetzen. Alternativ darf diese Aufgabe an ein netzseitiges Filterelement ausgelagert werden, sofern sich das System in einem separaten Netzwerk-Segment befindet und die Kommunikation mit diesem Segment ausschließlich über das netzseitige Filterelement möglich ist.

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

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

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.01-6/9.0

Req 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 spezifi-

schen 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	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 Bereitstellungskanäle des Herstellers
- dritte Distributoren, sofern sie durch den Hersteller autorisiert und legitimer Bestandteil von dessen Bereitstellungskanälen 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 5	Es muss der Windows Server Core-Installations-Mode verwendet werden.
-------	--

Motivation: Windows Server Core ist eine Installationsoption von Windows Server, welche die Angriffsfläche signifikant reduziert, da sie keine grafische Benutzeroberfläche (GUI) und nur die nötigsten Systemdateien und Dienste installiert. Ein weiterer Vorteil ist die regelmäßig geringere Anzahl an Updates/Patches und die damit verbundene Downtime.

Umsetzungsbeispiel: Der Windows Server Core-Betriebsmodus ist bei Installation von Windows Server 2008 oder Windows Server 2008 R2 während der Installation auszuwählen, da eine nachträgliche Änderung nicht möglich ist. Ab Windows Server 2012 ist ein Wechsel zwischen Core und Vollinstallation nachträglich möglich.

Alternativ lässt sich die Installation ab Windows Server 2012 im Modus „Grafische Verwaltungstools und Infrastruktur“ (Minimal Server Interface) durchführen. Wenn absehbar ist, dass keine lokalen Anpassungen mehr nötig sind, kann man in den vom Hersteller favorisierten Core-Modus wechseln.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.49-5/8.0

Req 6	Von den virtuellen Maschinen nicht benötigte Geräte, sowie Software- und Hardwarekomponenten, müssen auf dem Virtualisierungsserver deaktiviert werden.
-------	---

Um die Angriffsfläche der virtuellen Maschinen möglichst gering zu halten, müssen nicht benötigte Komponenten (virtuelle Netzwerkkarten, Treiber etc.) im Virtualisierungsserver (Host System) für die virtuelle Maschine deaktiviert oder entfernt werden.

Motivation: Jedes zusätzliche Gerät bietet zusätzliche Angriffspunkte auf das virtuelle System.

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
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.35-10/8.0

Req 7	Der Hyper-V Host darf nur über den für die Anforderung notwendigen Funktionsumfang verfügen und muss entsprechend konfiguriert sein.
-------	--

Motivation: Um Beeinflussung der virtuellen Maschinen durch Geräte oder Softwarekomponenten des Hyper-V Systems zu minimieren, sind diese zu deaktivieren. Ferner bieten nicht genutzte Hardwarefunktionalitäten und die dafür installierten Treiber wie auch virtuelle Netzwerkkarten eine vergrößerte Angriffsfläche.

Umsetzungsbeispiel: Deaktivierung der CD-/DVD-Laufwerksfunktionalität auf dem Hyper-V System im Gerätemanager oder die Deaktivierung von nicht verwendeten virtuellen Netzwerkkarten.

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
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.49-7/8.0

Req 8	Das Hyper-V System darf nicht mit einer weiteren Serverrolle als Hyper-V oder mit einer zusätzliche Anwendung installiert sein.
-------	---

Technisch ist es möglich bei der Installation von Windows Server 2008, weitere Serverrollen oder zusätzliche Anwendungen oder Administrationswerkzeuge wie „Virtual Machine Manager“ zu installieren und in der Parent Partition des Hyper-V Systems auszuführen.

Motivation: Jeder Netzwerk- oder Storage-Zugriff (I/O-Zugriff) wird durch die Parent Partition geleitet. Wenn die Parent Partition weitere Dienste ausführen muss, stehen die dafür nötigen Ressourcen den virtuellen Maschinen nicht zur Verfügung. Da die Parent Partition im Hyper-V System eine privilegierte Stellung hat und über den VMBus der gesamte ein- und ausgehende Datenverkehr aller auf dem System betriebenen virtuellen Maschinen steuert, stellt eine zusätzlich betriebene Anwendung eine weitere kompromittierbare Angriffsfläche auch für die virtuellen Maschinen dar.

Umsetzungsbeispiel: Keine weitere Serverrolle bei der Installation von Windows Server und Hyper-V zur Installation auswählen als die Serverrolle Hyper-V sowie keine weitere Anwendung installieren (Ausnahmen können aus betrieblichen Gründen Software-Agenten für Softwareverteilung, Performance-Monitoring, Asset-Management, Anti-Malware etc. sein).

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: 3.49-8/8.0

Req 9	Das Hyper-V System muss entsprechend der Härtingsrichtlinien von Microsoft oder "Security Best Practices" konfiguriert sein.
-------	--

Wenn interne Härtingsrichtlinien der Sicherheitsorganisationen der Deutschen Telekom Gruppe vorhanden sind, sollen die Hyper-V Systeme nach diesen Vorgaben gehärtet werden. Falls entsprechende Härtingsrichtlinien nicht vorhanden sein sollten, ist ein entsprechendes Hardeningkonzept anhand der „Security Best Practices“ vorzunehmen.

Motivation: Durch Umsetzung der, an Telekom Belange angepassten, „Best Practice“ Einstellungen der Hersteller oder anderer Organisation wie Fachverbände, etc. werden Sicherheitseinstellungen erreicht, die auf jahrelanger Praxis-Erfahrung beruhen. So werden auch Einstellungen getroffen die im Rahmen eines einzelnen Projekts eventuell nicht berücksichtigt würden, da Sie keine offensichtliche beziehungsweise aktive Relevanz im Projekt haben.

Umsetzungsbeispiel: Beachtung der Konfigurationshinweise und Anweisungen Microsoft TechNet unter [http://technet.microsoft.com/de-de/library/dd283088\(WS.10\).aspx](http://technet.microsoft.com/de-de/library/dd283088(WS.10).aspx), im Microsoft TechNet-Wiki unter <http://social.technet.microsoft.com/wiki/contents/articles/151.aspx>, der anwendbaren Einstellungen des Microsoft Windows Server 2008 Hyper-V Common Criteria Guides unter <http://www.microsoft.com/download/en/details.aspx?id=14252>, des Hyper-V Security Guides unter <http://technet.microsoft.com/en-us/library/dd569113.aspx> und der Aktivierung von Specialized Security, Limited Functionality (SSLF).

Zusätzlich können durch Tools wie der Microsoft Security Compliance Manager (<http://technet.microsoft.com/en-us/>

library/cc677002.aspx), der Microsoft Best Practices Analyzer (<http://technet.microsoft.com/de-de/library/dd759260.aspx>), dem Microsoft Baseline Security Analyzer (<http://technet.microsoft.com/de-de/security/cc184924>), etc. weiteren Aufschluss über die Sicherheit des Gesamtsystems geben und Vorschläge zur Erhöhung der Sicherheit bereitstellen.

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
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.49-9/8.0

Req 10	Die Integrität der Virtualisierungssoftware (Hypervisor) muss vor der Ausführung geprüft werden.
--------	--

Der Hypervisor ist eine kritische Komponente und sollte vor Manipulation geschützt werden. Eine Prüfung, bei System Neustart, hilft Veränderungen und Manipulationen frühzeitig zu erkennen. Hierbei ist auch der Einsatz von Hardware Techniken zu prüfen.

Eine Sicherstellung der Integrität der Software vor Ausführung (Installation) kann durch das Herunterladen von ausschließlich vertrauenswürdigen Quellen (Hersteller) und anschließender Checksummenprüfung (z. B. MD5, SHA256) erfolgen.

Motivation: Manipulationen der Virtualisierungssoftware haben Auswirkungen auf alle darauf betriebenen virtuellen Maschinen. Daher sollte der Hypervisor regelmäßig überprüft und besonders geschützt werden.

Umsetzungsbeispiel: Eine solche Überprüfung ist mit Hilfe von entsprechenden Tools wie z. B. OSSEC die ein File Integrity Monitoring durchführen, oder auch durch Hardware Techniken, wie z. B. Trusted Platform Module (TPM) realisierbar. Eine Unterstützung des Hypervisors für die entsprechende Lösung sollte im Vorfeld vom Hersteller bestätigt werden.

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: 3.35-9/8.0

Req 11	Das Hyper-V System muss vor und während der Ausführung vor Manipulation geschützt und die Integrität bewahrt sein.
--------	--

Motivation: Manipulationen der Virtualisierungsschicht (Hyper Jacking, Rogue Hypervisor wie SubVirt Virtual Machine Based Rootkit, Blue Pill) und der Parent Partition haben Auswirkungen auf alle auf dem Hyper-V System betriebenen virtuellen Maschinen.

Umsetzungsbeispiel: Setzen von restriktiven Zugriffsrechten mittels ACLs auf die genannten Verzeichnisse im „Hyper-V Attack Surface Reference Workbook“ (<http://download.microsoft.com/download/8/2/9/829bee7b-821b-4c4c-8297-13762aa5c3e4/Windows%20Server%202008%20Hyper-V%20Attack%20Surface%20Reference.xlsx>). Zusätzlich ein Monitoring via System Center Operations Manager mit dem Windows Server Hyper-V Management Pack die Integrität des Hyper-V Systems überprüfen und regelbasierte Aktionen ausführen lassen (<http://technet.microsoft.com/de-de/library/ff621102.aspx>, Überschrift „Überwachen der Integrität und Leistung von Hyper-V“).

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: 3.49-11/8.0

Req 12 Der Kommunikationskanal von einer virtuellen Maschine zum Hyper-V Host und umgekehrt muss eingeschränkt sein.

Hyper-V bietet mit den „Integration Services“ für die virtuellen Maschinen speziell eingerichtete Treiber für synthetische I/O-Geräte am VMBus an, so das Hardwarezugriffe durch die virtuelle Maschine eine vergleichbare Leistung zu physischen Servern erreichen können. Andere Gastbetriebssysteme die keine Anpassung (Enlightenment) für den Hyper-V und den VMBus aufweisen, kommunizieren über emulierte Geräte mit dem Hyper-V System.

Motivation: Die direkte Schnittstelle zwischen den virtuellen Maschinen und dem Hyper-V System kann auf Grund mangelnder Kontrollmöglichkeit Denail-of-Service-Angriffe auf das Hyper-V System oder sonstige kompromittierende Angriffe ermöglichen. Die direkte Schnittstelle zwischen Virtualisierungsserver und virtuellen Maschinen ist besonders kritisch, da sie nur schlecht kontrolliert werden kann. Sie erlaubt Administratoren der Virtualisierungsserver Zugriff auf virtuelle Maschinen, ohne Administratorrechte auf den virtuellen Maschinen besitzen zu müssen. Weiterhin könnte die Schnittstelle von Angreifern genutzt werden. Aktionen über die Schnittstelle werden nicht von den Standardlogging der virtuellen Maschine erfasst. Virtuelle Maschinen sollte daher analog zu physischen Maschinen administriert werden.

Umsetzungsbeispiel: Es sollten nur Gastbetriebssysteme auf dem Hyper-V System virtualisiert werden, die unter [http://technet.microsoft.com/de-de/library/cc794868\(ws.10\).aspx](http://technet.microsoft.com/de-de/library/cc794868(ws.10).aspx) aufgelistet werden oder für die durch Microsoft zertifizierte Gasterweiterungen (Integrationsdienste) angeboten werden. Ferner sollten alle Securityupdates zeitnah installiert werden, die Sicherheitslücken im VMBus beheben.

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
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.49-12/8.0

Req 13 Virtualisierungsumgebung müssen so abgesichert sein, dass sie keine Sicherheitsmechanismen umgehen.

Bei Virtualisierungsumgebung dürfen keine vorhandenen Sicherheitsmechanismen umgangen werden.

Weitere Beispiele bzw. Stichworte zu diesem Requirement sind: lokale Firewall, IDS/IPS, Proxy Restriktionen, lokale ACLs, „Zwang zur Verschlüsselung beim Abspeichern auf Massenspeichern“.

Motivation: Erhöhung der Sicherheit durch ausnutzen aller vorhandenen Sicherheitsschnittstellen, ohne diese durch verkürzung der Kommunikationswege zu umgehen.

Umsetzungsbeispiel: Hierbei sind z. B. Firewalls gemeint, die zwischen zwei Netzen vorhanden sind, jedoch durch eine direkte Kommunikation zwischen virtuellen Maschinen über lokale Schnittstellen umgangen werden könnten.

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

ID: 3.35-12/8.0

4. Systemaktualisierung

Req 14 Das Hyper-V System muss innerhalb des Unterstützungs-Supports des Herstellers betrieben werden.

Das Hyper-V System sollte innerhalb des Mainstream Supports betrieben werden und darf nicht über das Ende des Extended Supports hinaus betrieben werden. Ein Hyper-V System welches sich im Extended Support befindet, darf nicht mehr für neu konzipierte Produktionssysteme eingesetzt werden

Motivation: Ältere Hyper-V Systeme bieten aufgrund neuer Angriffsmöglichkeiten und technischer Schwachstellen eine erhöhte Angriffsfläche, da durch den Hersteller keine Patches/Bugfixes mehr bereit-gestellt werden, die ein potenti-elles Problem beheben.

Umsetzungsbeispiel: Für Hyper-V Server 2008 R2 endet der Mainstream Support am 14.01.2014. Bis zum Ende des Extended Supports am 08.01.2019 muss das Hyper-V System auf ein Produkt im Mainstream Support migriert werden.

Siehe hierzu: <http://support.microsoft.com/lifecycle/?ln=de>.

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: 3.49-14/8.0

Req 15 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 16 Es muss eine Anti-Malware Software auf dem Hyper-V System betrieben werden.

Motivation: Schadcode kompromittiert das Hyper-V System und gefährdet die Sicherheit wie auch die Stabilität des Gesamtsystems. Ein installiertes Anti-Malware-Programm kann diese Angriffsfläche weiter minimieren

Umsetzungsbeispiel: Installation einer Anti Malware Software auf dem Hyper-V System (Host).

Damit ein Hyper-V System einwandfrei mit einer installierten Anti Malware Software betrieben werden kann, sind folgende Verzeichnisse vom Virensan (Realtime und Scheduled) auszuschließen:

- Virtual Machine Configuration Files
 - Default "C:\ProgramData\Microsoft\Windows\Hyper-V"
- Virtual Machine VHD Files
 - Default "C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks"
 - Default bei Cluster "C:\ClusterStorage"
- Snapshot Files
 - Default "C:\ProgramData\ProgramData\Microsoft\Windows\Hyper-V\Snapshots"
- Virtual Machine Prozesse
 - Vmms.exe
 - Vmwp.exe

Hinweis: Bei Microsoft Forefront Endpoint Protection (FEP) kann dazu sehr einfach auf eine vordefinierte Richtlinie zurückgegriffen werden. Siehe hierzu: <http://technet.microsoft.com/de-de/library/gg412475.aspx>

Hinweis: Sofern die Standard-Verzeichnispfade während der Installation oder in der anschliessenden Konfiguration geändert werden, sind diese in der gewählten Anti-Malware Software entsprechend anzupassen.

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: 3.49-16/8.0

Req 17	Es müssen ausgeschaltete virtuelle Maschinen mit aktuellen Patches des Betriebssystems und der installierten Anwendungen sowie den aktuellen Anti-Malware-Pattern versorgt werden.
--------	--

Virtuelle Maschinen, die offline sind, können nicht über automatische Updatemechanismen wie Windows Update oder Windows Software Update Services (WSUS) auf einem aktuellen Stand gehalten werden

Motivation: Eine über längere Zeit ausgeschaltete virtuelle Maschine kann aufgrund fehlender Aktualität der virtuellen Maschinen anfällig für Angriffe sein und damit andere virtuelle Maschinen, Netzlaufwerke, etc. ggf. kompromittieren

Umsetzungsbeispiel: „Offline Virtual Machine Servicing Tool“ von Microsoft integriert System Center Virtual Machine Manager (SCVMM) mit den Windows Server Update Services oder der ConfigMgr Patching-Infrastruktur. Es startet automatisch einen Software-Update-Zyklus bei abgeschalteten virtuellen Maschinen, die nach dem Update auch wieder offline abgelegt werden

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.49-17/8.0

5. Schutz von Daten und Informationen

Req 18 Die Systempartition einer virtuellen Maschine sowie deren Kopien müssen verschlüsselt sein.

Virtuelle Maschinen werden häufig in Dateien auf dem Virtualisierungsserver oder einem SAN gespeichert. Es ist sicherzustellen, dass keine Kopien (z. B. Snapshots) oder Sicherungen existieren, welche nicht verschlüsselt sind. Die Verschlüsselung der Datenpartition wird durch die Schutzklasse, der auf der Partition gespeicherten Daten, festgelegt.

Motivation: Es ist zu verhindern, dass Daten aus Kopien oder Sicherungen unberechtigt gelesen werden können.

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: 3.35-19/8.0

Req 19 Die System- bzw. Verwaltungspartition oder einzelne Daten einer virtuellen Maschine sowie deren Kopien, wie Snap Shots, Volumeschattenkopien, Wiederherstellungspunkte, etc., müssen verschlüsselt sein.

Eine virtuelle Maschine besteht aus einer Reihe von Dateien, einschließlich der VHD/VDMK-Dateien und VHD/VDMK-Konfigurations-Dateien. Zusätzlich werden beim Speichern der virtuellen Maschinen der Inhalt des virtuellen Arbeitsspeichers je nach angewandtem Szenario in den jeweiligen VHD/VDMK-Dateien gespeichert. Ggf. werden so schutzbedürftige Inhalte wie Passwörter oder Hashes, die normalerweise verschlüsselt auf der Festplatte vorliegen, unverschlüsselt in den Dateien für die Virtuelle Maschine gespeichert (disk as state information)

Motivation: Eine Kompromittierung von Dateien der virtuellen Maschinen kann einen potentiellen Angreifer in die Kenntnis von schutzbedürftigen Informationen bringen, indem er auf unverschlüsselte Daten aus dem virtuellen Arbeitsspeicher Zugriff hat oder schutzbedürftige Daten auf der virtuellen Festplatte extrahieren kann. Durch eine Verschlüsselung wird sichergestellt, dass Angreifer eine derartige Verschlüsselung nicht umgehen, indem sie das System von einem anderen Betriebssystem aus oder mittels spezieller Angriffswerkzeuge hochfahren.

Umsetzungsbeispiel: Aufteilung der virtuellen Maschine in eine System- bzw. Verwaltungspartition und Datenpartition. Verschlüsseln der System- bzw. Verwaltungspartition der virtuellen Maschine mittels verfügbarer Microsofttools oder Drittherstellerlösungen wie z. B. Trend Micro SecureCloud, Veeam Backup & Replication, Altaro Hyper-V Backup, etc.

Hinweis: Wichtig! Die Verwendung von Encrypting File System (EFS) um Ordner, in dem Dateien der virtuellen Maschine gespeichert sind, zu verschlüsseln ist nicht möglich. Hyper-V unterstützt die Nutzung von Speichermedien nicht, wenn EFS verwendet wurde um die VHD/VDMK-Datei zu verschlüsseln.

Hinweis: Die Verschlüsselung der Datenpartition wird durch die Klassifizierung gemäß der Konzernrichtlinie IT-/NT-Sicherheit bestimmt und muss gesondert umgesetzt werden. Das ist nicht Bestandteil dieser Sicherheitsanforderung.

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
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.49-19/8.0

Req 20	Der Zugriff auf virtuelle Maschinen und deren Dateien muss durch Access Control Lists (ACLs) reglementiert sein.
--------	--

Eine virtuelle Maschine besteht aus einem Satz von Dateien. Dazu gehören die virtuellen Disks, in denen die komplette Softwareumgebung – also das Gastbetriebssystem, die darauf installierten und laufenden Anwendungen sowie die zugehörigen Daten residieren. Zudem gibt es noch die Konfigurationsdateien, die festlegen, über welche grundlegenden Eigenschaften und Ressourcen eine virtuelle Maschine verfügt. Dazu gehören zum Beispiel die Anzahl der virtuellen Prozessoren, die Kapazität des Arbeitsspeichers sowie die zugehörigen Ein-Ausgabe-Möglichkeiten für die virtuelle Maschine. Zusätzlich werden beim Speichern der virtuellen Maschinen der Inhalt des virtuellen Arbeitsspeichers je nach Szenario in den VHD-Dateien gespeichert. Ggf. werden so schutzbedürftige Inhalte wie Passwörter oder Hashes, die normalerweise verschlüsselt auf der Festplatte vorliegen, unverschlüsselt in den Dateien für die Virtuelle Maschine gespeichert (disk as state information).

Motivation: Eine Kompromittierung von Dateien der virtuellen Maschinen kann einen potentiellen Angreifer in die Kenntnis von schutzbedürftigen Informationen bringen, indem er auf unverschlüsselte Daten aus dem virtuellen Arbeitsspeicher Zugriff hat oder schutzbedürftige Daten auf der virtuellen Festplatte extrahieren kann.

Umsetzungsbeispiel: Der Zugriff auf die jeweiligen Dateien der virtuellen Maschine kann durch Access Control Lists (ACLs) auf die zum Zugriff berechtigten Benutzer beschränkt werden.

Hinweis: Um eine sichere Separation zu erreichen, sollten die ACLs in den Software-Switch integriert sein. Ist dies nicht der Fall, kann es passieren, dass zwei virtuelle Maschinen, die auf dem gleichen physischen Server installiert sind, nicht vollständig voneinander abgeschottet sind. Hat jemand die Kontrolle über die virtuelle Maschine A, könnte er so auch auf eine virtuelle Maschine B zugreifen und womöglich Daten stehlen.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.49-20/8.0

Req 21	Die Virtualisierungssoftware muss verhindern, dass virtuelle Maschinen mit gefälschten Layer 2 Adresse (MAC) Daten senden können und dass virtuelle Maschinen Pakete empfangen, wenn sich ihre Layer 2 Adresse (MAC) ändert.
--------	--

Motivation: Hierdurch wird verhindert, dass eine virtuelle Maschine sich beispielsweise per DHCP eine IP Adresse erschleicht die Firewallfreischaltungen besitzt bzw. dass eine virtuelle Maschinen die MAC-Adresse eines anderen Rechners übernimmt und unberechtigt Netzwerkverkehr empfängt.

Umsetzungsbeispiel: Die Erfüllung dieses Requirements ist bei virtuellen Maschinen, die zum Zweck der Ausfallsicherheit als Cluster betrieben werden, nicht grundsätzlich erforderlich.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.35-21/8.0

Req 22	Das Hyper-V System muss verhindern, dass virtuelle Maschinen Pakete empfangen oder senden wenn sich ihre Layer 2 Adresse (MAC-Adresse) ändert.
--------	--

Um das unerwünschte Mitlesen von Paketen einer virtuellen Maschine zu verhindern, ist das Empfangen von Paketen

durch Veränderung der MAC-Adresse der virtuellen Maschine, zu verhindern. Dies gilt insbesondere bei Installationen mit mehreren zusammenhängenden Hyper-V Systemen. Ein einzelnes Hyper-V System hat Sicherheitsmaßnahmen implementiert um die doppelte MAC-Adressenvergabe oder die Übernahme durch eine andere virtuelle Maschine zu verhindern, diese Sicherheitsmaßnahme funktioniert allerdings nicht über mehrere Hyper-V Systeme hinweg.

Motivation: Hierdurch wird verhindert, dass eine virtuelle Maschine die MAC-Adresse einer anderen virtuellen Maschine übernimmt und unberechtigt Netzwerkverkehr versendet oder empfängt.

Umsetzungsbeispiel: Einsatz von System Center Virtual Machine Manager 2008 oder höher (SCVMM). SCVMM verwaltet einen eigenen globalen Pool von MAC-Adressen zur Verteilung an virtuelle Maschinen, unabhängig vom eingesetzten Host-System (Hyper-V, VMWare, etc.). Standardmäßig sind im Bereich von 00-1D-D8-B7-1C-00 bis 00-1D-D8-F4-1F-FF insgesamt 3.998.719 MAC-Adressen verfügbar. Web Application Firewalls wie das Microsoft Forefront Threat Management Gateway (<http://www.microsoft.com/germany/forefront/edgesecurity/tmg/default.mspx>) stellen eine sinnvolle weitere Sicherheitsinstanz dar. Deaktivierung im Hyper-V System der „Spoofing von MAC-Adressen“-Eigenschaft über die Netzwerkkarteneinstellungen im Hyper-V Manager oder Deaktivierung der „AllowMacSpoofing“-Eigenschaft über WMI. Zusätzlich Aktivierung der „ARP Spoofing Prevention“-Eigenschaft.

Hinweis: Bei kleineren Umgebungen kann die Vergabe von statisch vergebenen MAC-Adressen an die virtuellen Maschinen zum gewünschten Ergebnis führen.

Hinweis: Hyper-V Systeme gleichen sich selbstständig nicht untereinander ab. Das heißt auch, dass sie nicht aktiv ihre MAC-Adressbereiche abgleichen. Mit anderen Worten: Zwei Hyper-V Systeme können durchaus den gleichen Adressbereich verwenden. Wenn dann ein externes Netz angebunden wird, werden entsprechende Fehlermeldungen im Netz generiert. Es ist daher ratsam, die Adressbereiche nach der Installation von Hyper-V zu prüfen und ggf. zu korrigieren.

Hinweis: Im laufenden Betrieb ändert das Hyper-V System die MAC-Adresse der virtuellen Maschine nicht. Dies gilt auch für eine Live Migration. Bei einer dynamischen Vergabe der MAC-Adresse durch das Hyper-V System bekommt die virtuelle Maschine bei jedem Neustart eine andere MAC-Adresse zugewiesen und somit wird z. B. in einem Linux System per default bei jedem Neustart ein neues Netzwerkinterface angelegt.

Hinweis: In Einzelfällen, z. B. bei Einsatz eines NLB (Netzwerklastenausgleich) Cluster in Hyper-V R2 Umgebungen, kann es zu Problemen kommen, da NLB MAC Spoofing benutzt um die Last an den Cluster-Knoten zu verteilen. In dem Fall ist die „Spoofing von MAC-Adressen“-Eigenschaft wieder zu aktivieren und die Konfiguration der Hyper-V Systeme z. B. mittels des Microsoft Systems Operation Manager auf Abweichungen zu überwachen. Die Aktivierung von „Spoofing von MAC-Adresse sollte sehr sparsam angewendet werden, da dies Unicast-Paketen aus Flooding-Angriffen ermöglicht in die virtuelle Maschine einzutreten.

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: 3.49-22/8.0

Req 23	Die Virtualisierungssoftware muss verhindern, dass virtuelle Maschinen Pakete auf dem Netz abhören können (Promiscuous Mode).
--------	---

Um ein Abhören des Netzwerkverkehrs durch eine virtuelle Maschine zu unterbinden, ist die Aktivierung des Promiscuous Mode für alle virtuellen Maschinen zu verbieten. Diese Einstellung sollte zentral in der Virtualisierungssoftware des Hosts administriert werden, um eine Veränderung durch einen administrativen Benutzers der virtuellen Maschine zu verhindern.

Motivation: Hierdurch wird verhindert, dass eine virtuelle Maschine Netzwerkverkehr anderer Systeme abhören kann.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unbemerkt durchführbare Angriffe

- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.35-20/8.0

Req 24	Das Hyper-V System muss verhindern, dass virtuelle Maschinen Pakete auf dem Netz abhören können (Promiscuous Mode).
--------	---

Um ein Abhören des Netzwerkverkehrs durch eine virtuelle Maschine zu unterbinden, ist die Aktivierung des Promiscuous Mode für alle Virtuellen Maschinen zu verhindern.

Motivation: Hierdurch wird verhindert, dass eine virtuelle Maschine fremden Netzwerkverkehr abhört.

Umsetzungsbeispiel: Hyper-V unterstützt per default keinen Promiscuous Mode der virtuellen Netzwerkadapter. Trotz allem sollte jeder virtuelle Netzwerkadapter an ein dafür vorgesehenes Netz sowie virtuelles LAN (VLAN) gebunden werden, um den Netzwerkverkehr so weit wie möglich voneinander zu isolieren.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.49-24/8.0

Req 25	Eine wirksame Veränderung der VLAN-ID darf nicht durch die virtuelle Maschine erfolgen.
--------	---

Die Virtualisierungssoftware muss jeder virtuellen Maschine (-Gruppe) ihr dediziertes VLAN zuordnen. Die Konfiguration des VLAN muss von dem Virtualisierungsserver aus erfolgen.

Diese Anforderung entfällt, wenn jeder Netzschnittstelle einer virtuellen Maschine (-Gruppe) eine exklusive physische Netzschnittstelle zugeordnet wird.

Motivation: Virtuelle Maschinen könnten unberechtigten Zugriff auf Netze erhalten, die normalerweise nicht für sie erreichbar sind.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.35-22/8.0

Req 26	Das Hyper-V System muss VLAN Hopping von virtuellen Maschinen unterbinden.
--------	--

Das Hyper-V System muss jeder virtuellen Maschine ihr dediziertes VLAN zuordnen. Die Anforderung entfällt, wenn jeder virtuellen Netzschnittstelle einer virtuellen Maschine eine eigene physische Netzschnittstelle zugeordnet wird.

Motivation: Virtuelle Maschinen könnten unberechtigten Zugriff auf Netze erhalten, die normalerweise nicht für sie erreichbar sind.

Umsetzungsbeispiel: Die virtuellen Netzwerkadapter für jede virtuelle Maschine sollten an ein dafür vorgesehenes Netz sowie virtuelles LAN (VLAN) gebunden werden, um den Netzwerkverkehr so weit wie möglich voneinander zu isolieren.

Siehe auch <http://technet.microsoft.com/de-de/library/ee236499.aspx>.

Hinweis: Jede virtuelle Netzwerkkarte bietet integrierte Unterstützung für virtuelle Netze an (VLANs), ihr kann damit ein eindeutiger VLAN-Kanal zugewiesen werden.

Jede virtuelle Maschine kann mit 12 virtuellen Netzwerkkarten konfiguriert werden – 8 als synthetische Netzwerkadapter und 4 als emulierte Netzwerkadapter.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.49-26/8.0

Req 27	In Ausgaben und Meldungen dürfen keine Informationen über interne Strukturen des Systems preisgegeben werden.
--------	---

Informationen über die internen Strukturen eines Systems einschließlich der dort verwendeten Komponenten und entsprechende Implementationsdetails gelten grundsätzlich als schutzbedürftig.

Im Allgemeinen betrifft dies Informationen über

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

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

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

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

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

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

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

Umsetzungsbeispiel: [Beispiel 1]

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

[Beispiel 2]

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

Für diese Anforderung sind folgende Bedrohungen relevant:

- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.01-9/9.0

Req 28	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 29	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

Req 30	Virtuelle Maschinen, die sensible Daten enthalten, müssen bei Deaktivierung sicher gelöscht werden.
--------	---

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.35-33/8.0

6. Schutz der Verfügbarkeit und Integrität

Req 31 Das System muss vor Überlastsituationen geschützt werden.

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

Beispiele für mögliche Schutzmaßnahmen sind:

- Begrenzung des pro Anwendung verfügbaren Arbeitsspeichers (RAM)
- Begrenzung der maximalen Sessions einer Web-Anwendung
- Begrenzung der maximalen Größe eines Datensatzes
- Begrenzung von CPU-Ressourcen pro Prozess
- Priorisieren von Prozessen
- Begrenzung der Anzahl oder der Größe von Transaktionen eines Benutzers oder von einer IP-Adresse in einem bestimmten Zeitraum

Anmerkung:

vor Netzwerk-basierenden Angriffen mit extrem hohen Daten- oder Paketraten, den sogenannten "Distributed Denial of Service" (DDoS) Angriffen, kann ein System sich i. d. R. selbst nicht mehr schützen. Zur Abwehr von DDoS Angriffen wird eine vorgelagerte Lösung in der Netzwerk-Schicht benötigt.

Motivation: Angreifer können mit gezielten ressourcenlastigen oder großvolumigen Anfragen versuchen, die Ressourcen eines Systems aufzubrechen, so dass das System seine regulären Aufgaben bzw. vorgesehenen Aufgabenvolumen nicht mehr erfüllen kann und die Verfügbarkeit der angebotenen Dienste effektiv gestört ist. Die Begrenzung der Ressourcen, die je gestellter Anfrage an das System maximal in Anspruch genommen werden können, ist eine grundlegende Maßnahme, um die Auswirkungen solcher Denial-of-Service (DoS) Angriffe zu reduzieren.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit

ID: 3.01-12/9.0

Req 32 In Überlastsituationen muss sich das System berechenbar verhalten.

Selbst umfassende systemeigene Schutzmaßnahmen können in extremen Situationen möglicherweise nicht mehr verhindern, dass ein System in eine Überlastsituation gerät.

Es muss daher sichergestellt sein, dass das System in Überlastsituationen nicht in einen Zustand überwechselt, der sicherheitsrelevante Funktionen oder Eigenschaften des Systems außer Kraft setzt. Leistungseinbußen (bspw. die Verminderung des Durchsatzes von legitimen Netzwerk-Paketen oder der Anzahl beantworteter Server-Anfragen pro Zeitraum) sind in Überlastsituationen i. d. R. nicht vermeidbar, das reguläre funktionale Verhalten des Systems muss jedoch grundlegend erhalten bleiben.

Dies kann im Extremfall bedeuten, dass ein kontrolliertes Herunterfahren des Systems eher hinnehmbar ist, als ein Weiterbetrieb bei unkontrolliertem Versagen der Sicherheitsfunktionen und somit dem Verlust des Systemschutzes.

Motivation: Mittels eines Denial-of-Service-Angriffs kann ein Angreifer versuchen, ein System gezielt zu überlasten. Reagiert ein solches System dann unberechenbar oder versagt sein reguläres Verhalten, insbesondere hinsichtlich dessen Sicherheitsfunktionen, kann dies dem Angreifer eine erweiterte Angriffsfläche auf Funktionen und Daten des Systems eröffnen sowie potentiell weitere verknüpfte Systeme gefährden.

Umsetzungsbeispiel: Eine Firewall, die in Überlastsituationen ihr Filter-Regelwerk verwirft und sämtliche Pakete ohne Prüfung weiterleitet, würde die Anforderung nicht erfüllen. In diesem Fall wäre das Blockieren sämtlicher Pakete durch die Abschaltung der Firewall eher hinnehmbar als das Versagen ihrer regulär vorgesehenen Schutzaufgabe für nachgelagerte Systeme.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 3.01-13/9.0

Req 33	Das System muss robust gegenüber unerwarteten Eingaben implementiert werden.
--------	--

An das System übergebene Daten müssen vor der Weiterverarbeitung zunächst validiert werden, um sicherzustellen, dass die Daten dem erwarteten Daten-Typ und -Format entsprechen. Dies soll das Risiko einer Manipulation von Systemabläufen und -Zuständen durch entsprechend konstruierte Dateninhalte eliminieren. Eine Validierung ist für jegliche Daten durchzuführen, die an das System übergeben werden. Beispiele sind Benutzereingaben, Werte in Datenfeldern und Protokollinhalte.

Die folgenden typischen Implementierungsfehler müssen vermieden werden:

- Fehlende Validierung der Länge von übergebenen Daten
- Unzutreffende Annahmen über das Format von Daten
- Fehlende Validierung empfangener Daten auf Konformität mit der Spezifikation
- Unzureichende Behandlung von Protokollabweichungen in empfangenen Daten
- Unzureichende Begrenzung der Rekursion beim Parsing komplexer Datenformate
- Unzureichende Umsetzung von Whitelisting oder Escaping zum Schutz vor Eingaben außerhalb des validen Wertebereiches

Motivation: Ein Angreifer kann mittels gezielt konstruierter Dateninhalte versuchen, ein System, das empfangene Daten vor der internen Weiterverarbeitung nicht ausreichend validiert, in einen instabilen Zustand zu versetzen oder nicht autorisierte Aktionen innerhalb des Systems auszulösen. Das Schadenspotential entsprechender Angriffe ist individuell systemabhängig, besitzt jedoch eine theoretische Bandbreite von unkontrollierten Systemabstürzen bis hin zu einer kontrollierten Ausführung von eigens eingeschleustem Code und der daraus resultierenden vollständigen Kompromittierung eines Systems.

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: 3.01-11/9.0

Req 34	Falls für ein System ein SLA existiert, muss eine Verletzung des SLA durch Überbuchen von Ressourcen verhindert werden.
--------	---

Der Virtualisierungsserver muss verhindern, dass virtuelle Maschinen Ressourcen überbuchen können, so dass damit andere virtuelle Maschinen unter den Schwellenwert (der im SLA definiert wurde) fallen. Alle Ressourcen (CPU, RAM, Netzwerk, Festplatte) dürfen nur statisch bzw. limitiert den virtuellen Maschinen zugeordnet werden. Eine Veränderung der Buchungen sollte nur nach Prüfung durch einen Administrator erfolgen oder bis zu einem Schwellenwert der verhindert, dass andere Instanzen benachteiligt werden können.

Motivation: Eine Kompromittierung, Fehlfunktion oder Fehladministration einer virtuellen Maschine darf nicht dazu führen, dass andere virtuelle Maschinen ihre Funktion nicht erfüllen können.

Umsetzungsbeispiel: Eine Limitierung der maximal zu übertragenden Daten über eine definierte Schnittstelle kann

einen solchen gewünschten Effekt haben.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

ID: 3.35-17/8.0

Req 35	Ein Hyper-V System muss verhindern, dass virtuelle Maschinen Ressourcen überbuchen und damit das Hyper-V System selbst oder andere virtuelle Maschinen negativ beeinflusst.
--------	---

Alle Ressourcen (virtuelle Prozessoren, I/O-Zugriff, Arbeitsspeicher, Festplattengröße, Netzwerk, etc.) dürfen nur statisch bzw. limitiert den virtuellen Maschinen zugeordnet werden (Server Ressourcen Sizing). Eine Veränderung der Buchungen sollte nur nach Prüfung durch einen Administrator erfolgen oder bis zu einem Schwellwert, der verhindert dass andere Instanzen benachteiligt werden können. Bei unkritisch eingestuften Hyper-V Systemen sollte verhindert werden, dass Ressourcen überbucht werden können.

Motivation: Eine Kompromittierung oder Fehlfunktion darf nicht dazu führen, dass virtuelle Maschinen oder das Hyper-V System selbst ihre Funktion nicht erfüllen können oder nicht mehr ausreichend Ressourcen für eine einwandfreie Funktion zur Verfügung stehen.

Umsetzungsbeispiel: 2 virtuelle CPUs sollten als Minimum stets für die Parent Partition reserviert werden. Der Arbeitsspeicher kann ebenso wie virtuelle Festplatten (VHDs) den virtuellen Maschinen dynamisch (Dynamic Memory & Dynamic VHD's) bis zu einer festzusetzenden Obergrenze zugewiesen werden. Für die Parent Partition sollten je nach Anwendungsfall mindestens 2 bis 4 GB Arbeitsspeicher fest reserviert werden, die im Hyper-V System per Registryeintrag festgelegt werden muss.

- Am Hyper-V System regedit.exe starten und zu folgendem Key navigieren:
 - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Virtualization
- Einen neuen Key vom Typ DWORD erzeugen und als Name „MemoryReserve“ (bei Hyper-V Server 2008 R2 SP1) oder „RootMemoryReserve“ (bei Hyper-V Server 2008 R2 ohne Servicepack) angeben
- In diesen Schlüssel muss nun der zu reservierende Wert für das Parent Memory eingetragen werden, z. B. 2048 MB (2GB) RAM. “You can then set the value to the static amount of memory that you want to reserve for the parent.”
- Speichern und regedit schliessen
- Hyper-V Server neu starten

Hinweis: Einzelne Anwendungen werden nur mit einer 1:1-Zuordnung (1 kompletter physischer Prozessorkern) von ihren jeweiligen Herstellern supportet (kann z. B. für SAP gelten). Dies ist bei der Ressourcenverteilung zu berücksichtigen.

Hinweis: Die Reserve des Arbeitsspeichers muss insbesondere bei Cluster-Knoten berücksichtigt werden, damit dieser bei einem Failover nicht überlastet wird. So sind z. B. bei einem 2-Knoten-Cluster 50 Prozent Reserve vorzusehen, während sich die vorzuhaltende Reserve bei einem zusätzlichen Cluster-Knoten auf 33,33% verringert. Dies gilt analog auch für die CPU-Kerne.

Hinweis: Egal ob mit Dynamic Memory oder ohne – ein “Überbuchen” des Arbeitsspeichers ist bei einigen Versionen eines Hyper-V Systems nicht möglich! Wenn der physische Arbeitsspeicher des Hyper-V Systems ausgebucht ist und eine zusätzliche virtuelle Maschine versucht zu starten, so schlägt deren Startvorgang ohne eine aussagekräftige Meldung fehl. Dies muss insbesondere bei Live Migrations - Szenarien berücksichtigt werden, da sich hier signifikante Änderungen in der Ressourcenverteilung ergeben.

Hinweis: Auch in einem Storage Area Network (SAN) können bei Verwendung von Dynamic Disk die Kapazitätsgrenzen überschritten werden. Zusätzlich fragmentieren bei der Verwendung von Dynamic Disk die Daten schneller. Deshalb wird empfohlen ausschließlich Fixed Disk zu konfigurieren.

Hinweis: Die Auslagerungsdatei (pagefile) ist eines der wesentlichen Elemente der Windows-Speicherverwaltung. Für “allgemeine” Serversysteme gilt die Regel: Pagefile gleich anderthalb mal RAM. Bei Hyper-V Systemen die meist mit

sehr viel RAM ausgestattet sind, wovon das meiste ohnehin nie ausgelagert wird, da es an die virtuellen Maschinen zugewiesen ist, ist die Konfiguration nur zu Debuggingzwecken nötig. Da der Host üblicherweise nur zwischen 2 und 4 GB RAM selbst verwaltet, kann man diesen Wert als Grundlage für das Host-Pagefile nutzen, wenn der Plattenplatz knapp ist. Da viele Hyper-V Systeme aber mit lokalen Platten für das Host-Betriebssystem ausgestattet sind und die virtuellen Maschinen dann im SAN ablegen, kann man die Systemvorgabe übernehmen. Viele Administratoren verlegen die Auslagerungsdatei auch auf ein separates Laufwerk – dies muss dann aber eine dedizierte physische Platte sein, auf keinen Fall nur eine Partition oder gar ein Laufwerk, auf dem noch andere I/O-Last liegen.

Siehe hierzu: <http://www.server-talk.eu/2011/01/31/wie-viel-virtual-memory-braucht-ein-hyper-v-host/>

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

ID: 3.49-35/8.0

7. Authentifizierung und Autorisierung

Req 36 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 37 Benutzerkonten müssen die eindeutige Identifizierung des Benutzers sicherstellen.

Benutzer müssen eindeutig von einem System identifiziert werden können.

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

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

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

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

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

Weitere Lösungen sind im Einzelfall auf ihre Verwendbarkeit zu prüfen.

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

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.01-22/9.0

Req 38 Benutzerkonten müssen mit mindestens zwei Authentisierungsmerkmalen aus unterschiedlichen Faktoren geschützt werden.

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

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

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

Es müssen mindestens zwei Authentisierungsmerkmale miteinander kombiniert werden.

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

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

Beispiele für zulässige Authentisierungsmerkmale

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

*) Wichtiger Hinweis zum Einsatz von Passwörtern

Passwörter müssen als Authentisierungsmerkmal strikt vermieden werden.

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

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

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

Hinweis zu technischen Benutzerkonten

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

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

Umsetzungsbeispiel: Beispiele für MFA

MFA Kombination	Beschreibung	Anmerkung zur Anwendung
Telekom "myCard" plus PIN-Eingabe	1. Faktor: in Hardware implementiertes Zertifikat ("Besitz") 2. Faktor: PIN ("Wissen")	(keine)
FIDO2 Level 2 Security Key plus Fingerabdruck	1. Faktor: in Hardware gespeicherter Crypto-Schlüssel ("Besitz") 2. Faktor: Biometrisches Merkmal ("Inhärenz")	Die Biometrie-Funktion muss vorab konfiguriert werden, da der Biometrie-Sensor sonst nur als "Taste" funktioniert und somit der 2. Faktor ("Inhärenz") nicht gegeben wäre.
Device-bound Passkey in WH4B* auf Nucleus PC plus PIN	1. Faktor: in Hardware gespeicherter Crypto-Schlüssel ("Besitz") 2. Faktor: PIN ("Wissen")	(keine)
Device-bound Passkey in Secure Enclave auf iOS Device plus FaceID	1. Faktor: in Hardware gespeicherter Crypto-Schlüssel ("Besitz") 2. Faktor: Biometrisches Merkmal ("Inhärenz")	(keine)

Passwort plus freigegebene OTP App (z. B. MS Authenticator)	1. Faktor: Passwort ("Wissen") 2. Faktor: spezifisch generiertes One Time Password ("Besitz")	Passwörter sind nur dann zulässig, falls sicherere Alternativen nicht umgesetzt werden können. Die Synchronisation der Authenticator App über einen Clouddienst sowie das Teilen (z. B. über einen Passwortmanager) des OTP ist nicht zulässig.
--	--	--

*) WH4B: "Windows Hello for Business"

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.01-20/9.0

Req 39	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.

on, 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 40 Vordefinierte, nicht benötigte Benutzerkonten müssen gelöscht oder zumindest deaktiviert werden.

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

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

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

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

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.01-7/9.0

Req 41 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 42 Die Berechtigungen von Benutzern und Anwendungen müssen auf den zur Erfüllung ihrer Aufgaben benötigten Umfang beschränkt werden.

Die Berechtigungen auf einem System müssen so weit eingeschränkt werden, dass ein Benutzer nur auf Daten zugrei-

fen und Funktionen nutzen kann, die er im Rahmen seiner Arbeit benötigt. Entsprechende Berechtigungen sind auch für den Zugriff auf Dateien zu vergeben, die Bestandteil des Betriebssystems oder von Anwendungen sind oder von diesen erzeugt werden (z. B. Konfigurations- und Protokollierungsdateien).

Neben dem Zugriff auf Daten muss auch die Ausführung von Anwendungen und deren Bestandteilen mit möglichst niedrigen Berechtigungen erfolgen. Anwendungen sollten nicht mit Administrator- oder Systemberechtigungen ausgeführt werden.

Motivation: Werden einem Benutzer zu weitreichende Berechtigungen auf einem System gewährt, kann er in einem Umfang auf Daten und Anwendungen zugreifen, der zur Erfüllung der zugewiesenen Aufgaben nicht erforderlich ist. Dies erzeugt ein unnötig erhöhtes Risiko im Falle eines Missbrauchs, insbesondere auch, falls der Benutzer oder dessen Benutzerkonto durch einen Angreifer kompromittiert werden.

Anwendungen, die über zu weitreichende Berechtigungen verfügen, können von einem Angreifer missbraucht werden, um unbefugte Zugänge zu erhalten oder zu erweitern und damit einen Zugriff auf schutzbedürftige Daten und Systembereiche zu erlangen.

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: 3.01-23/9.0

Req 43	Die administrative Verwaltung des Hyper-V Systems und aller Komponenten muss durch unterschiedliche Benutzerrollen voneinander getrennt sein.
--------	---

Bei Produktivsystemen sind die Rollen Administrators für ein Hyper-V System strikt von den Rollen des Administrators für virtuelle Maschinen zu trennen. Administratoren von virtuellen Maschinen dürfen in keinem Fall der Funktionen des Administrators für Hyper-V Systeme beinhalten, ebenso wie umgekehrt (Least Privileges).

Motivation: Durch eine verfügbare, rollenbasierte Sicherheitseinstellungen in einer Hyper-V Systemumgebung, kann eine sichere Steuerung der erlaubten Vorgänge in der virtualisierten Umgebung ermöglicht werden. Damit wird eine Rechtentrennung, Separation of Duties (SOD), implementiert, da neben den Parametern zur näheren Spezifikation einer Rolle auch Bedingungen gesetzt werden können.

Umsetzungsbeispiel: Durch eine Benutzerrolle sind die Vorgänge (zusammengefasst in einem Profil) definiert, die für eine ausgewählte Gruppe von Objekten (definiert durch den Bereich der Benutzerrolle) zulässig sind. So können verschiedene Rollen der Kategorie „Delegierter Administrator“ erstellt werden, etwa für einen allgemeinen Administrator, welcher sämtliche Vorgänge an einem Standort verwaltet, einen spezialisierten Administrator zur Verwaltung der Bibliothekserver sowie einen fortgeschrittenen Benutzer, der komplexe virtuelle Umgebungen in einem Testlabor einrichten soll. Außerdem können Self-Service-Benutzerrollen von Benutzern dazu verwendet werden, eine festgelegte Reihe von Vorgängen für die eigenen virtuellen Maschinen auszuführen.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.49-43/8.0

Req 44	Der Betriebssystemadministrator eines Hyper-V Systems muss einer anderen der Rolle als der des Hyper-V Administrators zugeordnet sein.
--------	--

Ein Administrator des Betriebssystems eines Hyper-V Systems ist strikt von den Funktionen eines Administrators für die Rolle Hyper-V zu trennen (Least Privileges).

Motivation: Hyper-V stellt eine eigene Anwendung innerhalb der Serverrollen eines Windows Server Betriebssystems dar. Um eine sichere Rechtstrennung zu gewährleisten sind die administrativen Tätigkeiten für den Betrieb des Servers von den administrativen Tätigkeiten der zugewiesenen Serverrolle zu trennen. Zudem hat der Administrator des Hyper-V Systems je nach Konfiguration Administratorenrecht auf anderen Windows Server Betriebssystemen, die nicht die Rolle Hyper-V ausführen.

Umsetzungsbeispiel: Bei der Installation sind getrennte Administratoren-Gruppen für die Verwaltung des Betriebssystems und die Verwaltung der Rolle Hyper-V zu erstellen und entsprechende Nutzer zuzuordnen. Dies kann durch z. B. Richtlinien im Active Directory Service festgelegt werden oder durch Nutzung des Authorization Managers (AzMan), ein Snap-In für die Microsoft Management Console (MMC), das an ausgewählte Benutzer und Gruppen die der Hyper-V-Rolle angehören, zugewiesen wird.

Hinweis: Eine Auflistung der 33 verschiedenen Funktionen, die verschiedenen neben den 3 Standardoperationen noch weiteren Rollen zugeordnet werden können, können dem Dokument „Hyper-V Security Guide“, Kap. 2 Delegating Virtual Machine Management (<http://www.microsoft.com/download/en/details.aspx?id=16650>) entnommen 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
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 3.49-44/8.0

Req 45	Der Zugriff von Benutzern der Rolle ‚Hyper-V Administrator‘ auf virtuelle Maschinen und deren Dateien muss eingeschränkt sein.
--------	--

Es ist zwar nicht so leicht möglich, dass ein Benutzer mit zu geringen Zugriffsrechten auf eine virtuelle Disk zugreift und sie einfach kopieren kann. Doch jede virtuelle Maschine läuft bei Microsofts Hyper-V im Kontext eines speziellen Prozesses, dem Virtual Machine Worker Process (vmwp.exe). der wiederum wird über das Dienstkonto NETWORK gestartet und damit ist Nutzern der Rolle ‚Hyper V-Administrator‘ der Zugriff auf die Ressourcen im Dateisystem, die eine VM abbilden, machbar. Dies betrifft insbesondere das Szenario wenn verschiedene Administratoren, unterschiedliche virtuelle Maschinen auf einem physischen Hyper-V System betreuen.

Motivation: Jeder Benutzer, der in der Lage ist den Hyper-V Manager aufzurufen kann Snapshots einer virtuellen Maschine anlegen. Das ist auch dann der Fall, wenn der Benutzer regulär keinen Zugriff auf die entsprechend geschützten Objekte im Dateisystem hat. Wenn ein derartiger Benutzer dann einen Snapshot einer VM in einem Bereich ablegt, auf den er Zugriff hat, dann ist das System schnell kompromittiert.

Umsetzungsbeispiel: Der Zugriff auf die jeweiligen virtuellen Maschinen, Ordner und Ablageorte kann durch Access Control Lists (ACLs) auf die jeweiligen Benutzer beschränkt werden. Zusätzlich sollten die virtuellen Maschinen verschlüsselt werden.

Hinweis: Durch ein strukturiertes System von Unterverzeichnissen kann der Zugriff durch ACLs flexibler konfiguriert werden

Beispiel:

W:\Virtualization Resources\Project A\Virtual Machines
W:\Virtualization Resources\Project A\Virtual Hard Disks
W:\Virtualization Resources\Project A\Virtual Floppy Disks
W:\Virtualization Resources\Project A\ISO-Dateien
W:\Virtualization Resources\Project B\Virtual Machines
W:\Virtualization Resources\Project B\Virtual Hard Disks
W:\Virtualization Resources\Project B\Virtual Floppy Disks

W:\Virtualization Resources\Project B\ISO-Dateien
W:\Virtualization Resources\Project C\Virtual Machines
W:\Virtualization Resources\Project C\Virtual Hard Disks
W:\Virtualization Resources\Project C\Virtual Floppy Disks
W:\Virtualization Resources\Project C\ISO-Dateien

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
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.49-45/8.0

Req 46	Die Managementsoftware muss eine Trennung von Administration der virtuellen Maschinen und der Netzwerkadministration unterstützen.
--------	--

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
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.35-32/8.0

Req 47	Es muss der Microsoft System Center Virtual Machine Manager (SCVMM) in der aktuellen Version für administrative Aufgaben an der Hyper-V Systemumgebung verwendet werden.
--------	--

SCVMM ist für Hyper-V Systemumgebungen derzeit das „höchstwertige“ Verwaltungswerkzeug.

Motivation: Die vielfältigen Hyper-V Verwaltungswerkzeuge sind nicht alle sauber aufeinander abgestimmt, weshalb es bei einer Konfigurationsänderung zu Inkonsistenz des Gesamtsystems kommen kann falls ein anderes Verwaltungswerkzeug die durchgeführte Änderung nicht mitbekommen hat.

Umsetzungsbeispiel: Falls durch die Nutzung eines anderen Werkzeugs ein Hyper-V Verwaltungswerkzeug eine Änderung nicht mitbekommen hat, gibt es im SCVMM Abgleichsmöglichkeiten um eine Inkonsistenz zu verhindern.

Hinweis: „Virtual Machine Manager“ oder „System Center Virtual Machine Manager“ ist auf einem separaten physischen Server zu installieren und nicht in der Parent Partition eines Hyper-V Systems. Eine Installation von Anwendungen in der Parent Partition wird durch Microsoft nicht supportet. Weiterführende Informationen unter <http://technet.microsoft.com/en-us/library/jj136794.aspx>

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

ID: 3.49-47/8.0

Req 48 Ein Hyper-V System muss einer eigenen Active Directory Domäne angehören.

Da ein Windows-Cluster zwingend voraussetzt, dass die Clusterknoten Mitglieder einer Active Directory Domäne sind, nimmt man die Hyper-V-Server meist direkt in die Produktionsdomäne auf. Es ist allerdings empfehlenswert die Hyper-V-Systeme von der Produktionsumgebung zu trennen.

Motivation: Der Zugang zu dieser Domäne lässt sich gut kontrollieren, da man nur sehr wenige Anmeldekonto für die Administration der Hyper-V Systeme braucht.

Umsetzungsbeispiel: Für die Hyper-V Systeme erzeugt man eine eigene Active Directory Domäne, die aus physischen Domain Controllern und den Host-Clustervern besteht. Das Produktions Active Directory kann auf einer virtuellen Maschine betrieben werden.

Hinweis: Beim Einsatz des System Center Virtual Machine Manager (SCVMM) muss darauf geachtet werden, dass er bei diesem Szenario in der Hyper-V-Domäne installiert wird, denn ein Hyper-V-Cluster kann der SCVMM nur in seiner eigenen oder einer vertrauten Domäne verwalten.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.49-48/8.0

8. Schutz von Sitzungen

Req 49	Das System muss es Benutzern ermöglichen, sich von ihrer laufenden Sitzung abzumelden.
--------	--

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

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

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.01-17/9.0

Req 50	Sitzungen müssen nach einer dem Verwendungszweck angepassten Zeit der Inaktivität automatisch beendet werden.
--------	---

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

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

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

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.01-18/9.0

9. Authentisierungsmerkmal Passwort

Req 51	Falls Passwörter als Authentisierungsmerkmal genutzt werden, muss deren Speicherung unter Einsatz eines für diesen Zweck als ausreichend sicher anerkannten "Password Hashing"-Verfahrens erfolgen, um Offline-Angriffe wie Wörterbuch- und Brute-Force-Attacken stark zu erschweren.
--------	---

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

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

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

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

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

In expliziter Deutlichkeit ist als NICHT ZULÄSSIG hervorzuheben:

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

Hinweis:

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

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

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

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

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

Für diese Anforderung sind folgende Bedrohungen relevant:

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

- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.01-24/9.0

Req 52	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 53	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 54	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 55	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

Req 56	Falls Passwörter als Authentisierungsmerkmal genutzt werden, muss eine Änderung des eigenen Passwortes jederzeit durch den Benutzer möglich sein.
--------	---

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

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

Motivation: Nur durch die Möglichkeit, dass ein Benutzer sein Authentisierungsmerkmal jederzeit selbstständig ändern kann, ist ein zeitnahe Änderung möglich, wenn der Benutzer den Verdacht hat, dass dieses in den Besitz Dritter gelangt sein könnte.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.01-29/9.0

Req 57	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 58	Falls Passwörter als Authentisierungsmerkmal genutzt werden, darf deren Darstellung während der Eingabe nicht im Klartext erfolgen.
--------	---

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

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

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

Ausnahmeregelungen:

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

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

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

Für diese Anforderung sind folgende Bedrohungen relevant:

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

- Abstreiten von durchgeführten Aktionen
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.01-31/9.0

10. Protokollierung

Req 59	Sicherheitsrelevante Ereignisse müssen mit einem exakten Zeitstempel und einer eindeutigen Systembezeichnung protokolliert werden.
--------	--

Sicherheitsrelevant sind jegliche Ereignisse, die Auswirkungen auf die Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) eines Systems haben können oder dessen mißbräuchliche Verwendung anzeigen. Systeme müssen das Auftreten von sicherheitsrelevanten Ereignissen protokollieren.

Um eine Zuordnung und Auswertung dieser Ereignisse zu ermöglichen, müssen diese zusammen mit einer eindeutigen Systembezeichnung (z. B. Hostname, IP- oder MAC-Adresse) und dem genauen Zeitpunkt des Auftretens ("Zeitstempel") protokolliert werden. Der Zeitstempel eines protokollierten Ereignisses muss mindestens folgende Informationen beinhalten:

- Datum des Ereignisses (Jahr, Monat, Tag)
- Uhrzeit des Ereignisses (Stunden, Minuten, Sekunden)
- Zeitzone, auf die sich diese Zeitangaben beziehen

Die Sicherheitsrelevanz konkreter Ereignisse ergibt sich individuell aus Art und Funktion des Systems sowie den darin verarbeiteten Daten. Daher kann keine einheitliche Liste aus Ereignissen, die Sicherheitsrelevanz besitzen, vorgegeben werden. Relevante Ereignisse müssen passend zum System identifiziert werden. Die folgende Auflistung enthält typische sicherheitsrelevante Ereignisse und ist entsprechend als eine grundlegende Orientierungshilfe bei der Identifikation der sicherheitsrelevanten Ereignisse für ein bestimmtes System zu verstehen.

Sicherheitsrelevantes Ereignis	Informationen, die zum Ereignis zu protokollieren sind
Fehlerhafte Anmeldeversuche	• betroffenes Benutzerkonto, • Anzahl der Fehlversuche • Quelle des Zugriffs (IP-Adresse, Client-ID/Client-Name, lokale Konsole, ...)
Systemzugriffe über Benutzerkonten (einschliesslich System-Konten bzw. technischer Benutzerkonten)	• betroffenes Benutzerkonto • Startzeit/Endzeit des Zugriffs (Anmeldung/Abmeldung) • Quelle des Zugriffs (IP-Adresse, Client-ID/Client-Name, lokale Konsole, ...)
Änderungen an Benutzerkonten (einschliesslich System-Konten bzw. technischer Benutzerkonten)	• Benutzerkonto, mit dem die Änderung vorgenommen wurde • Benutzerkonto, an dem die Änderung vorgenommen wurde • Art der vorgenommenen Änderung (Neueinrichtung, Aktivierung, Deaktivierung, Löschung, Passwort-Rücksetzung, ...)
Änderungen der Rollenzuweisungen/Berechtigungen von Benutzerkonten (einschliesslich System-Konten bzw. technischer Benutzerkonten)	• Benutzerkonto, mit dem die Änderung vorgenommen wurde • Benutzerkonto, an dem die Änderung vorgenommen wurde • Bezeichnung der betroffenen Rolle / Typ der betroffenen Berechtigung • Art der vorgenommenen Änderung (Rolle/Berechtigung hinzugefügt, Rolle/Berechtigung entfernt, ...)

Nutzung/Initiierung von kritischen Systemfunktionen	• Benutzerkonto, mit dem die Nutzung vorgenommen wurde • Bezeichnung/Typ der genutzten Systemfunktion
Zugriff auf sensible Daten ("Sensitive Data"), die im System verarbeitet werden	• Benutzerkonto, mit dem der Zugriff vorgenommen wurde • Bezeichnung des betroffenen Datenfelds (der Inhalt des Datenfelds sollte dabei nicht mit protokolliert werden, um einen Datenabfluss über Log-Dateien zu verhindern) • Art des Zugriffs (Lesen, Ändern, Löschen, ...)
Abnormaler Anstieg in der Auslastung von Systemressourcen, wie etwa Arbeitsspeicher, CPU, Netzwerk oder Festplattenzugriffen über einen längeren Zeitraum	• Schwellwert der betroffenen Systemressource • Dauer der Überschreitung des Schwellwerts • Höhe der Überschreitung des Schwellwerts Es müssen abhängig vom individuellen System sinnvolle Schwellwerte definiert werden.
Sonstige Ereignisse, die für versuchte oder erfolgreiche Angriffe gegen das System Hinweise liefern können *)	• individuell abhängig von der Art des Ereignisses

*) Dies erfordert eine Identifizierung der wichtigsten, für das System typischerweise zu erwartenden Angriffsformen und die Sicherstellung, dass zu deren Erkennung relevante Ereignisse durch das System tatsächlich protokolliert werden. In der Regel kann das nur durch den Entwickler/Hersteller des Systems gewährleistet werden.

Bei der Protokollierung müssen die jeweils geltenden gesetzlichen und betrieblichen Bestimmungen beachtet werden. Letztere umfassen insbesondere auch Vereinbarungen, die mit den betrieblichen Sozialpartnern getroffen wurden. Diese Bestimmungen besagen unter anderem, dass die Protokollierung von Ereignissen nur zweckgebunden erfolgen darf. Die Protokollierung von Ereignissen zum Zweck der Arbeitskontrolle von Mitarbeitern ist nicht zulässig.

Zudem muss - wie für jegliche Daten, die von einem System verarbeitet werden - auch für Protokollierungsdaten ein angemessener Schutzbedarf berücksichtigt und umgesetzt werden; dies gilt für die Speicherung, die Übertragung sowie den Zugriff. Insbesondere falls Wirkdaten in den Protokollierungsdaten enthalten sind, muss derselbe Schutzbedarf berücksichtigt werden, der auch für die reguläre Verarbeitung dieser Wirkdaten innerhalb des Quell-Systems Anwendung findet.

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: 3.01-33/9.0

Req 60 Die für den Betrieb notwendigen, sicherheitsrelevanten und veränderbaren Konfigurationsparameter müssen regelmäßig kontrolliert werden.

Um eine unrechtmäßig veränderte Konfiguration von virtuellen Maschinen und Virtualisierungs-Host frühzeitig zu entdecken, müssen die Konfigurationseinstellungen (von Netzwerk, Geräten, usw.) geprüft werden. Hiermit ist z. B. eine Veränderungen der Netzwerkeinstellungen einer VM oder das unberechtigte Verändern eines vom Virtualisierungs-Hosts verwendeten Dienste wie NTP gemeint.

Motivation: Bei einer regelmäßigen Überwachung der Konfiguration, lassen sich Fehlkonfigurationen und Manipulation aufdecken.

Umsetzungsbeispiel: Eine solche Überwachung ist mit Hilfe von entsprechenden Management-Tools wie z. B. 'Veeam Reporter' durchführbar.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Modifikation von Daten
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.35-34/8.0

Req 61	Die Zugriffsaktionen auf die virtuellen Maschinen bzw. Daten der virtuellen Maschine muss protokolliert werden.
--------	---

Ein weiterer Aspekt, der zu mehr Sicherheit bei den virtuellen Maschinen führt, ist das Überwachen der Aktionen, die die Benutzer ausführen. Dazu bietet Hyper-V die Option, dass man die erfolgreichen sowie die fehlgeschlagenen Versuche von Zugriffen auf Objekte mitprotokolliert.

Motivation: Mit einer Zugriffsprotokollierung lässt sich verfolgen, von welchen Konto aus der – ggf. unerlaubte – Zugriff auf eine virtuelle Festplatte bzw. virtuelle Maschine ausgeführt wurde. Durch Monitoringsoftware lässt sich automatisiert Maßnahmen zum Schutz der virtuellen Festplatten bzw. virtuellen Maschinen einleiten.

Umsetzungsbeispiel: Verwendung des Tools Auditpol.exe verwenden, um die Überwachungsrichtlinien des Dateisystems auf Erfolg und Misserfolg bei öffnen, kopieren, ändern oder löschen zu konfigurieren. Des Weiteren sollte man zusätzlich ein Monitoring-Produkt wie System Center Operations Manager (<http://www.microsoft.com/germany/systemcenter/opsmgr/default.aspx>) einsetzen um bei definierten Aktionen Warnungen zu generieren

Für diese Anforderung sind folgende Bedrohungen relevant:

- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.49-61/8.0

Req 62	Die virtuelle Maschine muss mit einem zuverlässigen Zeitserver synchronisiert werden.
--------	---

Für den Betrieb eines Hyper-V Systems und der virtuellen Maschinen ist eine exakte Zeitsynchronisation im Gesamtsystem notwendig. Eine Synchronisation der virtuellen Maschine mit dem Hyper-V System kann bei großer Last auf dem Hyper-V System zu einem „out of sync“ führen, was dazu führt das sich die Systemzeit der virtuellen Maschine von der des Hyper-V Systems signifikant unterscheiden kann.

Motivation: Durch eine Manipulation aufgrund von unterschiedlichen Zeitstempeln lassen sich Dienste wie die Kerberos-Authentifizierung, die Zeitstempel bei Logfiles, Zeitstempel bei der Zertifikatsvalidierung sowie bei digitalen Signaturen und virtuelle Maschinen selbst negativ beeinflussen.

Umsetzungsbeispiel: Zeitsynchronisation über das Active Directory, übergeordneten Domäne bzw. dem Forrest Master über das NTP-Protokoll.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.49-62/8.0

Req 63	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 Zeitzonen-Konfiguration bei der Ausgabe von Zeitinformationen in die Ortszeit transformiert werden, sofern die so stattfindende Zeitzonenanpassung eindeutig erkennbar und nachvollziehbar ist.

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

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

Umsetzungsbeispiel: Einige zulässige Zeitgeber-Quellen:

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

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.01-32/9.0

Req 64	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 65	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 66	Für sicherheitsrelevante Protokollierungsdaten, die an den Log Server weitergeleitet werden, muss die Einhaltung geltender Aufbewahrungszeiträume und Löschfristen sichergestellt werden.
--------	---

Folgende Grundregelung ist zu berücksichtigen:

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

Abweichungen

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

Log Server in Verantwortung eines Dritten

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

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

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

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

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.01-36/9.0

Req 67	Sicherheitsrelevante Protokollierungsdaten müssen echtzeitnah an eine Erkennungs- und Reaktionslösung für Sicherheitsvorfälle bereitgestellt werden.
--------	--

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

- Es erfolgt eine kontinuierliche Analyse bzw. Korrelation der aus angebundenen IT/NT-Systemen bereitgestellten Protokollierungsdaten.

- Die Identifizierung bedrohlicher Aktivitäten und laufender Angriffe findet auf Basis einer fortlaufend aktuell gehaltenen Erkennungsmuster-Datenbank statt.
- Integrierte Alarmierungsprozesse lösen im Fall eines Fundes die Einleitung von Gegenmaßnahmen aus.
- Sicherheitsexperten sind aktiv involviert in den Betrieb der Lösung sowie die Auswertung von Alarmen.

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

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

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

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

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

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

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

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

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

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unbemerkt durchführbare Angriffe

ID: 3.01-37/9.0