

Sicherheitsanforderung

Architektur Rechenzentrums- und Cloud-Infrastrukturen

Deutsche Telekom Gruppe

Version	3.0
Datum	01.07.2025
Status	Freigegeben

Impressum

Herausgeber
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Deutschland

Dateiname	Dokumentennummer 3.58	Dokumententyp Sicherheitsanforderung
Version 3.0	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

Sicherheitsanforderungen für die Architektur von Cloud- und Rechenzentrumsinfrastrukturen. Der Schwerpunkt liegt auf Netzen und System-Trennungen, insbesondere im Bereich Systemmanagement. Dies gilt sowohl für physische als auch für virtuelle Rechenzentren ("Cloud") und betrifft alle Arten von Infrastrukturkomponenten (Netze, Storage, Computing, Monitoring usw.).

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.	Infrastruktur	5
3.	Virtualisierung	8
4.	Netze	10
5.	Firewalls	12
6.	System Management	14

1. Einleitung

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

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

2. Infrastruktur

Req 1	Eine Rechenzentrumsinfrastruktur oder Cloud-Plattform muss eine Trennung der darin betriebenen Systeme und gespeicherten Daten gemäß deren Schutzbedürfnissen ermöglichen.
-------	--

Insbesondere Systeme mit einem hohen Schutzbedarf müssen immer von anderen Systemen getrennt sein, d. h. auch von anderen solchen Systemen. Ebenso sind Systeme auf denen personenbezogene Daten verarbeitet werden vor unerwünschten Zugriffen oder Datenströmen sowohl aus dem eigenen wie auch aus anderen Netzen zu schützen.

Motivation: Eine Kompromittierung eines wenig geschützten Systems ist eher wahrscheinlich. Dies darf nicht dazu führen, dass andere Systeme mit einem hohen Schutzbedarf von diesem kompromittierten System aus angegriffen werden können.

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: 3.58-1/3.0

Req 2	Falls Systeme von extern (Nicht-DTAG, z. B. aus dem Internet) erreichbar sind, müssen diese auf einer physisch von internen Systemen getrennten Infrastruktur abgebildet werden.
-------	--

Zur Unterstützung der geforderten Trennung im Schichtenmodell müssen alle extern erreichbaren Maschinen sowie die dabei genutzten Infrastrukturkomponenten wie Hypervisor und Netzkomponenten (Switches, Router, Firewalls und Loadbalancer) physisch von anderen, internen Systemen getrennt sein.

Motivation: Diese Anforderung stellt sicher, dass es von aus dem Internet erreichbaren Systemen nur einen Weg zu den dahinter liegenden Anwendungs- und Datenbanksystemen gibt. Die Firewall oder Filterelemente können nicht über gemeinsam aus Internet und internen Netzen erreichbare Komponenten umgangen werden. Zudem hat diese Trennung den Vorteil, dass Störungen in der Infrastruktur nur Teilbereiche tangieren, während andere Teile weiterhin verfügbar bleiben.

Umsetzungsbeispiel: Für die Anbindung der Komponenten einer Präsentationsschicht an das Internet werden andere Switches und Router verwendet als im internen Netz.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 3.58-2/3.0

Req 3	Falls Infrastrukturelemente Dienste oder Funktionen für interne und zugleich für von extern erreichbaren Maschinen erbringen, müssen diese Funktionen nach internen und externen Gesichtspunkten getrennt sein.
-------	---

Mit Infrastrukturelementen sind sowohl Netzelemente wie Router und Switches gemeint, gemeinsam genutzte (Basis-)Dienste wie DNS und NTP, Management- und Monitoringsysteme als auch zentrale Speichersysteme. Bei diesen muss sichergestellt werden, dass ein Zugriff auf einen internen Bereich nicht von extern möglich ist.

Motivation: Interne Daten und Systeme dürfen nicht von extern kompromittiert werden können. Umsetzung der Prinzipien Need-to-know und Need-to-see.

Umsetzungsbeispiel: Eine Umsetzung besteht bspw. in der getrennten Nutzung von Speichermedien, getrennten SAN Fabrics oder einer Virtualisierung der Funktionen (Storage-Virtualisierung) wie vFiler.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Störung der Verfügbarkeit

ID: 3.58-3/3.0

Req 4 Zentral genutzte Dienste in der Infrastruktur müssen besonders abgesichert und verfügbar sein.

Der Ausfall zentraler Dienste und Sicherheitseinrichtungen kann den Schutz von Systemen beeinträchtigen. Somit müssen diese entsprechend abgesichert und verfügbar gestaltet werden und keine Single-Point-of-Failures aufweisen. Dazu gehören:

- DNS-Server zur Namens- und Adressauflösung
- NTP-Server zur Zeitsynchronisation
- Ausgehende (Web-)Proxies für kontrollierten Zugriff auf das Internet
- Mail-Gateways zum Versenden von (System-) E-Mails
- Jump hosts für Zugriff auf die Systeme von intern und Fremdfirmenzugänge
- Systemmanagement und -monitoring
- Installations-Server, Patch- und Update-Server, Software Repositories
- Logserver für zentrales Logging
- Backup- und Restore Systeme zur Wiederherstellung von Maschinen
- Identity und Access Management (IAM) als zentrale ID-Instanz
- Privileged Access Management (PAM) zur Erlangung höherer Rechte

Entsprechende Redundanzen ermöglichen auch die Wartbarkeit zentraler Systeme im laufenden Betrieb. Erstreckt sich die Infrastruktur über mehrere Standorte so ist es empfehlenswert, auch diese zentralen Funktionen standortübergreifend zur Verfügung zu stellen.

Motivation: Infrastrukturdienste haben einen erhöhten Schutzbedarf und müssen daher besonders abgesichert und verfügbar sein.

Umsetzungsbeispiel: Jump hosts sollten redundant vorhanden sein, damit jederzeit die Administrierbarkeit aller Systeme, auch durch Fremdkräfte, gewährleistet ist. Ausgehende (Web-) Proxies sollten jederzeit in der Lage sein, den daran angeschlossenen Systemen notwendige Sicherheitsupdates zu liefern.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit

ID: 3.58-4/3.0

Req 5 IP-Adressen von Infrastrukturkomponenten müssen statisch konfiguriert werden.

Motivation: Verhindern, dass Infrastrukturelemente ungewollt neue IP-Adressen erhalten.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

ID: 3.58-5/3.0

Req 6	Angriffe auf die Infrastruktur (-plattform) müssen erkannt werden, so dass rechtzeitig Gegenmaßnahmen eingeleitet werden können.
-------	--

Um Angriffe auf die Plattform frühestmöglich zu erkennen und mögliche Auswirkungen zu minimieren, ist es notwendig, angemessene Maßnahmen zur Überwachung und Erkennung (zum Beispiel ein Monitoring mit Korrelation verschiedener Meldungen) einzusetzen.

Motivation: Insbesondere virtuelle Umgebungen bieten durch die Virtualisierungsschicht eine zusätzliche Angriffsfläche. Diese muss durch entsprechende Sicherheitsfunktionen, wie sie bereits in anderen Bereichen eingesetzt werden, überwacht und geschützt werden. Nur durch eine aktive Überwachung, der anschließenden Erkennung und daraus resultierenden Aktionen ist ein durchgängiger Schutz der betriebenen Maschinen möglich.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 3.58-6/3.0

3. Virtualisierung

Req 7	Daten und Funktionen von virtuellen Maschinen müssen durch die Virtualisierungsumgebung zuverlässig voneinander getrennt werden.
-------	--

Es gilt virtuelle Maschinen, inklusive ihrer Daten und den genutzten Diensten und Funktionen im Netz, voneinander zu schützen. Hierzu sind durchgängig Sicherheitseigenschaften der Virtualisierungsumgebung auf allen Ebenen (physisch, logisch, im Netz, in der Verwaltung usw.) zu nutzen.

So ist insbesondere darauf zu achten, dass bei Kompromittierung einer virtuellen Instanz der Zugriff auf eine andere virtuelle Instanz oder auf den Hypervisor nicht möglich sein darf. Das heißt, die virtuellen Maschinen müssen voneinander abgeschottet sein und es darf keine direkte Verbindung zwischen ihnen möglich sein. Die Grundeinstellung der Virtualisierungsumgebung muss sein, dass eine virtuelle Maschine zunächst keinerlei Zugriffe auf gemeinsame Ressourcen hat.

Virtuelle Maschinen und deren Daten müssen so gruppiert werden, dass nach Überwindung der Schutzfunktionen der Virtualisierungsumgebung das potentielle Schadensausmaß auf ein akzeptables Minimum (Restrisiko) begrenzt ist. Hierzu ist eine Betrachtung des möglichen Schadensausmaßes genauso notwendig wie eine Bewertung des Schutzbedarfs, der Kritikalität, des Bedrohungspotenzials der einzelnen Systeme sowie der jeweils zu verarbeitenden Daten. Diese benannten Indikatoren sind bei der Planung und Umsetzung zu bewerten und zu berücksichtigen.

Motivation: Die konsequente Abschottung der virtuellen Instanzen limitiert die Gefahr der Kompromittierung aller virtuellen Instanzen. Um mögliche Auswirkungen eines Angriffs, zum Beispiel in Form einer übernommenen virtuellen Maschine, auf weitere virtuelle Maschinen inklusive der darauf befindlichen Daten, so gering wie möglich zu halten, ist eine entsprechende Segmentierung umzusetzen.

Umsetzungsbeispiel: Eine entsprechende Gruppierung kann sich am N-Tier Architektur-Modell orientieren. Durch die Umsetzung hätten kompromittierte virtuelle Maschinen, welche sich in der Präsentationsschicht befinden, über eine Schwachstelle in der Virtualisierungsumgebung keinen Zugriff über den Hypervisor auf die Anwendungs- und Datenbankschichten, die sich auf physisch getrennten Maschinen befinden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 3.58-7/3.0

Req 8	Durch den Einsatz einer Virtualisierung dürfen Sicherheitsschnittstellen, -funktionen sowie Intrusion Detection/Prevention Systeme nicht umgangen werden.
-------	---

Durch den Einsatz der Virtualisierung ist es teilweise möglich, bestimmte vorgegebene Sicherheitsmechanismen z. B. die auf einem Host oder dem dahinterliegenden Netz eingerichteten Berechtigungen, Regeln oder Routen zu umgehen. Durch eine Umgehung dieser Sicherheitsfunktionen wird ggf. die Sicherheit anderer Systeme gefährdet.

Motivation: Wenn Schnittstellen direkt über die Virtualisierungssoftware miteinander verbunden werden (z. B. interner vSwitch), können Angriffe nicht erkannt werden bzw. sind Netzdienste ungeschützt zugreifbar.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.58-8/3.0

Req 9	Die Netze, die für den Betrieb der Virtualisierungsumgebung notwendig sind (Hypervisor-Management, LiveMigration, Heartbeat, ...), müssen vollständig von den Netzen der virtuellen Maschinen inkl. deren Management getrennt werden.
-------	---

Die Verkehrsdaten der virtuellen Maschinen müssen von der Administration der Virtualisierungsumgebung getrennt werden. Eine physische Trennung wird empfohlen.

Motivation: Die (Hardware-basierte) Plattform und deren Management muss immer unter Kontrolle des Betreibers bleiben. Es soll verhindert werden, dass von einer virtuellen Maschine aus die Virtualisierungsumgebung beeinflusst wird bzw. ein Zugriff darauf erfolgt.

Umsetzungsbeispiel: Nutzung einer oder mehrerer physischer Schnittstellen für die Verwaltung des Hypervisors, ggf. VLANs, und eine oder mehrere weitere Schnittstellen für die Netze der VMs.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Störung der Verfügbarkeit
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.58-9/3.0

4. Netze

Req 10	Produktionsnetze (extern sowie intern), Managementnetze, Bürokommunikationsnetze, Test- & Entwicklungsnetze, Transportnetze und weitere Netzbereiche müssen voneinander getrennt werden.
--------	--

Eine physische Trennung dieser Netzbereiche wird empfohlen.

Wenn auf einer Virtualisierungsumgebung nicht genügend physische Adapter zur Verfügung stehen, um den Management- und Produktionsdatenverkehr der virtuellen Maschinen voneinander zu trennen, so können diese Verkehre über einen gemeinsamen physischen Adapter geführt werden, sofern dieser eine logische Trennung dieser beiden Verkehrstypen ermöglicht. Damit sind die virtuellen Maschinen letztendlich nur an das eine physische Layer-2-Netz verbunden, das nicht mit dem Management-Netz der Hardware-Infrastruktur identisch ist.

Statt gerouteter Übergänge zwischen Netzbereichen (über eine Firewall reglementiert) wird empfohlen, Application Layer Gateways einzusetzen, bspw. Jumphosts.

Weiterhin wird empfohlen, für diese unterschiedlichen Netzbereiche eindeutig unterscheidbare IP-Adressbereiche zu verwenden.

Motivation: So sind Systeme gemäß ihrem Einsatzzweck voneinander getrennt.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.58-10/3.0

Req 11	Eine kunden-/produktionsseitig durchgeführte Netztrennung von Systemen muss im Managementnetz und weiteren angeschlossenen Netzen, auch im Speichernetz, in analoger Weise erfolgen.
--------	--

Es muss eine netzbasierte Trennung von Systemen, bspw. durch VLANs, private VLANs oder andere Layer-2 Techniken, auf allen angeschlossenen Netzbereichen (z. B. Produktionsnetz, Management-Netz, Storage-/Backup-Netz) sinngleich erfolgen. Dasselbe gilt für andere Techniken, z. B. Fibre Channel (FC).

Besondere Aufmerksamkeit benötigen Systemmanagement- und Backup-Systeme: Häufig werden viele Systeme über eine einzelne Instanz verwaltet. Dabei ist darauf zu achten, dass keine Kommunikation / Kompromittierung von einem System zum anderen über das Managementnetz erfolgen darf. So dürfen extern erreichbare Systeme nicht zusammen mit rein internen Maschinen im gleichen Management-Netzsegment angeschlossen sein.

Motivation: Eine Trennung, um zu vermeiden, dass nach einer Kompromittierung weitere Systeme angegriffen werden können, bringt nur dann einen echten Mehrwert, wenn sie auf allen Schnittstellen in gleicher Weise erfolgt.

Umsetzungsbeispiel: Präsentationsschicht und Datenbankschicht sind netzseitig aus „Kundensicht“ getrennt. Die administrativen Management-Schnittstellen wären jedoch in ein und demselben Netz angeschlossen und könnten darüber miteinander kommunizieren. Dann könnte bei Kompromittierung der Präsentationsschicht ein Angreifer direkt auf Layer-2 die Systeme der Datenbankschicht erreichen unter Umgehung einer möglichen Firewall, die die Kommunikation ins Daten-/Produktionsnetz reglementiert.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 3.58-11/3.0

Req 12	„Standort-zu-Standort“-Verbindungen, z. B. generische IPSec-Tunnel zur Verbindung interner Netze zwischen Rechenzentren, müssen so terminiert werden, dass die darüber laufende Kommunikation an der Firewall / dem Paketfilter des Zielnetzes geprüft werden kann.
--------	---

Dies gilt insbesondere für generisch eingerichtete Tunnel / VPNs zwischen Rechenzentren, die von mehreren Systemen genutzt werden. Beispielsweise werden damit nicht vertrauenswürdige Netzabschnitte überbrückt.

Motivation: Verschlüsselte Verbindungen auf IP-Ebene müssen so terminiert werden, dass weiterhin die Kommunikationsmatrix geprüft werden kann.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.58-12/3.0

Req 13	An der Netzgrenze der Cloud, dem Rechenzentrum oder anderer zusammenhängender Infrastruktur müssen IP-Pakete mit logisch ungültigen Adressen sowohl eingehend als auch ausgehend verworfen werden.
--------	--

Wenn Absenderadressen offensichtlich gespoofed oder Pakete anderweitig ungültig sind, müssen diese ausgefiltert werden. Dies gilt für das ganze RZ- oder Cloud-Netz und ist unabhängig vom Schutz einzelner Systeme durch systemspezifische Filterelemente.

Motivation: Schutz der eigenen Systeme vor unsinnigen Anfragen und maliziösen Paketen. Schutz fremder Systeme vor falsch versandten Paketen aus dem eigenen Netz, z. B. zur Vermeidung von Denial-of-Service Angriffen mit gefälschten Absender-IP-Adressen.

Umsetzungsbeispiel: Herausfiltern privater Adressen (als Absender oder Ziel) am Übergang zum öffentlichen Internet; eingehendes Filtern von Absender-Adressen, die lokal im RZ-Netz verwendet werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

ID: 3.58-13/3.0

5. Firewalls

Req 14	Filterelemente wie Firewalls und Loadbalancer müssen unabhängig von den zu schützenden Systemen sein.
--------	---

Filterelemente können neben klassischen Firewalls (physisch oder virtuell) auch Loadbalancer, Session Border Controller, Access Listen auf Routern oder in einer Virtualisierungsumgebung implementierte Mechanismen sein, die einen Schutz für die Systeme bieten. Diese Schutzfunktion darf nicht vom zu schützenden System aus auf direktem Weg verändert werden können.

Für virtualisierte Umgebungen wird empfohlen, diese Firewalls auf anderen Hostsystemen laufen zu lassen und nicht auf den Hosts für die zu schützenden Systeme. Im Falle einer in die Virtualisierung direkt implementierten Filterfunktion, z. B. Mikrosegmentierung, läuft die Filterung direkt im Hypervisor der jeweiligen virtuellen Maschine.

Loadbalancer nehmen häufig eine Doppelrolle ein, wenn sie neben dem Loadbalancing auch Verkehr auf IP-Ebene filtern und so eine Schutzfunktion mit übernehmen.

Motivation: Die Abtrennung der Sicherheitselemente

- sorgt für eine klare Abgrenzung zwischen Sicherheitsfunktionen und Diensten,
- unterstützt die Trennung administrativer Tätigkeiten und Verantwortungen und
- verhindert, dass ein Angreifer auf einem kompromittierten System die (netzbasierten) Filter deaktivieren kann.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.58-14/3.0

Req 15	Filternde Netzelemente (meist Firewalls) dürfen keine Dienste oder Funktionen enthalten, die einen negativen Einfluss auf die Zuverlässigkeit der Firewall-Funktionalität haben.
--------	--

Netzfunktionen, die sich gegenseitig beeinträchtigen können, müssen auf verschiedene Systeme aufgeteilt werden:

- Router mit dynamischen Routingprotokollen,
- Firewalls, wenn häufig Änderungen am Regelwerk vorgenommen werden oder tiefgehende Paketanalysen durchgeführt werden.

Hingegen können statische IPSec-Tunnel auf einer Firewall terminiert werden, sofern sichergestellt ist, dass dadurch keine Filterfunktionen des Firewall-Systems umgangen werden.

Motivation: Je mehr Funktionen auf einem Gerät vereint sind, desto höher ist die Gefahr einer Kompromittierung bzw. einer Störung der hauptsächlichen Funktion.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

ID: 3.58-15/3.0

Req 16	Die Basiskonfiguration eines Filterelements (Firewall) muss "deny any any" sein; d. h. jede erforderliche Kommunikation ist explizit freizugeben.
--------	---

Es muss mit sogenannten „Whitelists“ gearbeitet werden. Bei einer sequentiellen Abarbeitung des Regelwerks muss am Ende ein generelles Kommunikationsverbot (default deny) stehen. Es ist „eingehender“ und „ausgehender“ Verkehr zu filtern. Vereinfachungen davon sind je nach Einzelfall zu entscheiden. Logisch falsche IP-Pakete, z. B. mit offensichtlich gefälschten Absenderadressen („Spoofing“), müssen verworfen werden. Die eingetragenen Regeln müssen einer dokumentierten Kommunikationsmatrix entsprechen.

Um Freischaltungen für größere TCP-/UDP-Port-Ranges zu vermeiden, sollten benötigte Dienste/Protokolle mit dynamischer Portzuweisung auf Alternativen untersucht werden, sofern die dynamischen Ports nicht durch eine Firewall mit entsprechendem Protokollsupport gezielt frei geschaltet werden können. Über die frei geschalteten Ports könnten sonst Dienste erreichbar sein, die hätten geschützt sein sollen.

Es muss nicht jede Source-IP-Adresse einzeln freigegeben werden, wenn es um den Schutz erreichbarer Dienste des Zielsystems geht. In Abhängigkeit von der Kritikalität der zu schützenden Systeme können auch Netze statt einzelner IPs freigeschaltet werden, wenn dadurch der Verwaltungsaufwand sowie die Anzahl möglicher Fehler signifikant verringert werden und von keinem erhöhten Risiko für die Zielsysteme auszugehen ist.

Motivation: Die Verwendung von Blacklists kann trotz aller Sorgfalt zu einer unbeabsichtigten Freigabe von Kommunikationsverbindungen führen. Diese Maßnahme dient sowohl dem direkten Schutz der Systeme als auch dem Schutz und der Stabilität des gesamten Netzes.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.58-16/3.0

Req 17	Filterelemente (Firewalls) dürfen an interne Systeme nur Pakete aus zulässigen internen Netzen weiterleiten.
--------	--

IP-Pakete mit anderen Adressen (Absender oder Ziel) als im internen Netz verwendete Adressen sind zu verwerfen.

Motivation: Schutz der Systeme vor maliziösen Paketen, die die Verfügbarkeit und Integrität des Zielsystems beeinträchtigen könnten.

Umsetzungsbeispiel: Keine Default-Route auf internen Netzelementen. So ist sichergestellt, dass nur Pakete, die zu explizit vorhandenen Routingeinträgen passen, zugestellt werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

ID: 3.58-17/3.0

Req 18	Falls IPv6 im Einsatz ist, müssen Filterregeln für IPv4 und IPv6 gleichermaßen konfiguriert werden.
--------	---

Paketfilter, Firewall Regeln etc. müssen so gesetzt werden, dass dieselben Schutzmaßnahmen für IPv4 und IPv6 gelten. Dienste, die per IPv4 aus nicht erreichbar sind, dürfen auch nicht per IPv6 erreichbar sein.

Motivation: Durch den Einsatz von IPv6 dürfen keine Schutzmaßnahmen umgangen werden, die für IPv4 getroffen wurden.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.58-18/3.0

6. System Management

Req 19	Das Management der Rechenzentrums- bzw. Cloud-Infrastruktur muss über ein von anderen Netzen strikt getrenntes Managementnetz erfolgen.
--------	---

Die Zugänge zur Administration sind so zu gestalten, dass Zugriffe nur den Administratoren möglich sind. Der Zugang muss so konfiguriert sein, dass dieser nur über speziell für diese Umgebung aufgebaute Jumphosts möglich ist.

Es wird empfohlen, dass alle verwaltbaren ("aktive") physischen Komponenten stets über deren Management-Netz erreichbar sind. Server via ILO, Netzwerkkomponenten wie Router und Switches über deren dedizierte Management-Ports. Um sicherzustellen, dass der Zugriff auf die Komponenten über das Managementnetz immer möglich ist, muss dieses auf einer separaten Netz-Infrastruktur abgebildet sein, da es sonst durch Datenverkehr von Kunden bzw. Anwendern beeinträchtigt werden kann. Es sollte zudem für jeden Typ von Infrastrukturkomponenten ein eigenes Managementnetz (z. B. abgeschottetes VLAN) angelegt sein, das Zugriff nur den für diese Technik bestimmten Managementsystemen erlaubt.

Das Systemmanagement von Infrastrukturkomponenten, die sowohl interne als auch externe Leistungen erbringen, muss über ein eigenes oder das Managementnetz für interne Systeme erfolgen.

Motivation: Die Beschränkung der Zugangsmöglichkeiten auf einen eindeutig definierten Weg und damit eine feste Anzahl von Möglichkeiten erlaubt eine klare Kontrolle der Zugriffe. Implementierte Schutzmechanismen der Systeme können so nicht umgangen werden. Der Betreiber darf die Kontrolle über die Hardware nicht verlieren.

Umsetzungsbeispiel: Ein VLAN für das Management aller internen Netzkomponenten und ein zweites für externe Netzkomponenten. Ein weiteres VLAN für den Anschluss der ILO-Ports interner Server und eines für die Speichersysteme. Eine Kommunikation zwischen diesen VLANs darf nicht möglich sein; alle diese Systeme können nur mit den dazugehörigen Managementsystemen kommunizieren, ggf. auch mit Jumphosts, wenn erforderlich.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unbemerkt durchführbare Angriffe

ID: 3.58-19/3.0

Req 20	Systemmanagement-Systeme müssen kontrolliert eingesetzt werden.
--------	---

Management-, Backup- und auch Monitoring-Systeme sind sorgfältig zu planen, aufzubauen und zu betreiben. Sie verfügen meist standardmäßig über privilegierte Zugriffe auf viele Systeme. Wenn auf diesen privilegierten Zugriff, z. B. mit Administrator-Rechten, nicht verzichtet werden kann, müssen Maßnahmen implementiert sein, um die damit verbundenen Risiken für die zu managenden Systeme zu minimieren (zu „kontrollieren“). Es gilt:

- Die Kommunikation zwischen Managementsystem und verwalteten Systemen muss unidirektional über möglichst nur einem TCP/IP-Port erfolgen.
- Die Richtung des Kommunikationsaufbaus von/zu verwendeten Agenten hängt von der Vertrauensstellung daran beteiligter Systeme und den zu übermittelnden Daten ab.
- Die zentralen Systeme sollten – wenn möglich – gänzlich ohne privilegierten Zugriff auf die zu managenden Systeme auskommen.
- Eine ausreichende Authentifizierung der Agenten gegenüber dem Management-Server und andersherum ist erforderlich.
- Keine zentrale Komponente sollte privilegierten Zugriff auf eine kritische Menge von Systemen haben.
- Automatische Installations- und Konfigurationsmechanismen sollten so abgesichert sein, dass sie nicht für ungewollte Änderungen an Systemen missbraucht werden können; z. B. können diese nach Installation und initialer Konfiguration deaktiviert werden. Oder es werden Signaturmechanismen eingesetzt, die sicherstellen, dass nur autorisierte Änderungen automatisch durchgeführt werden.
- Backup-Daten dürfen nur von berechtigten Systemen aus abgerufen werden können.

Motivation: Im Falle der Kompromittierung eines zentralen Systems muss die Möglichkeit eingeschränkt sein, weitere Systeme unmittelbar mit privilegierten Rechten kompromittieren zu können.

Umsetzungsbeispiel: Zur Konfiguration eines Systems oder beim Abruf von Konfigurationsparametern wird eine Form gewählt, bei der jeweils das Zielsystem die Kommunikation aufbaut. Ein Zugriff in nahezu Echtzeit kann durch regelmäßiges Triggern erreicht werden. Als Transferprotokoll empfiehlt sich HTTPS, das nur einen Port benötigt, Verschlüsselung und eine Authentisierung bietet.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.58-20/3.0

Req 21	Eine Management-Software zur Verwaltung verschiedener Typen von Infrastrukturkomponenten oder (Anwendungs-) Systemen muss eine an den unterschiedlichen Zuständigkeiten ausgerichtete, rollenbasierte Trennung der Verwaltungsaufgaben unterstützen.
--------	--

Neben einer Trennung der Verwaltung verschiedener physischen Geräte wie z. B. Speichersysteme und Server sollte die Managementsoftware auch in virtuellen Umgebungen eine Rollentrennung von Maschinen- und Netzadministration ermöglichen.

Motivation: Eine Trennung von Netz- und Systemadministration unterstützt das Prinzip „separation of duties“.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Modifikation von Daten

ID: 3.58-21/3.0

Req 22	Alle Infrastrukturkomponenten müssen über ein lokales Notfall-Konto verfügen.
--------	---

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

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

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

Motivation: Sicherstellen des Zugriffs auf die Infrastruktur bei Störungen der zentralen Authentifizierungs- und Autorisierungsinstanz. Dazu gehören Major Incidents wie Ransomware Angriffe, Ausfälle des Netzes oder zentraler Identity Systeme. Kleinere Störungen, wie Verlust einer Netz-basierten Multi-Faktor-Authentifizierung, gesperrte Konten oder falsch konfigurierte Richtlinien können ebenso abgemildert werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

ID: 3.58-22/3.0

