

Sicherheitsanforderung

Architektur von Systemen

Deutsche Telekom Gruppe

Version	3.2
Datum	01.07.2023
Status	Freigegeben

Impressum

Herausgeber
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Deutschland

Dateiname	Dokumentennummer 3.14	Dokumententyp Sicherheitsanforderung
Version 3.2	Stand 01.07.2023	Status Freigegeben
Fachlicher Ansprechpartner Telekom Security psa.telekom.de	Gültigkeitsdauer 01.07.2023 - 30.06.2028	Freigegeben von Stefan Pütz, Leiter SEC-T-TST

Zusammenfassung
Sicherheitsanforderungen für die Architektur von IT- und NT-Systemen.

Copyright © 2023 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.	Systemtrennungen	5
3.	Kommunikation	7
4.	Schichtenmodell	10
5.	Verfügbarkeit	13
6.	Administration	17
7.	Einhaltung von Industriestandards	19

1. Einleitung

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

Die Sicherheitsanforderung dient u. a. als Grundlage zur Freigabe im PSA-Prozess. Sie dient darüber hinaus als Umsetzungsempfehlung in 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.

Der Begriff "DTAG" bezieht sich in diesem Dokument in der Regel auf "Deutsche Telekom Gruppe".

2. Systemtrennungen

Beim Zusammenspiel von Systemen gilt es, sich nicht auf einzelne, lokale Sicherheitsmaßnahmen zu verlassen. Eine Basissicherheit wird durch grundsätzliche Trennungen insbesondere im Kommunikationsnetz erreicht.

Req 1 Systeme müssen ihrem Schutzbedarf entsprechend voneinander getrennt werden.

Der Schutzbedarf eines Systems leitet sich von den verarbeiteten Daten, der Exponiertheit, den darauf laufenden Anwendungen und weiteren anderen Faktoren ab. So sind Systeme auf denen personenbezogene Daten verarbeitet werden durch dem aktuellen Stand der Technik entsprechende Maßnahmen (z. B. Firewalls) vor unerwünschten Zugriffen oder Datenströmen sowohl aus dem eigenen wie auch aus anderen Netzen zu schützen. Ist ein System in Schichten aufgebaut, so sind diese Schichten entsprechend voneinander zu trennen. Systeme mit einem hohem Schutzbedarf bzgl. Vertraulichkeit, Verfügbarkeit, Integrität oder Datenschutz, sogenannte "Kritische Systeme", müssen von anderen Systemen getrennt sein, auch von anderen kritischen Systemen. Diese Trennung ist zumindest logisch durchzuführen. Anforderungen an eine physische Trennung (z. B. bei besonders hohem Schutzbedarf) sind zu prüfen und entsprechend umzusetzen.

Beispiele für Trennungen sind: VLAN, VxLAN, private VLAN oder andere, sicher konfigurierte Netztrennungen.

Motivation: Eine Kompromittierung eines Systems mit geringem Schutzbedarf ist eher wahrscheinlich. Dies darf nicht dazu führen, dass weitere Systeme direkt durch gemeinsam genutzte Netze oder andere Ressourcen angegriffen werden können. Eine Aufteilung des Netzes ermöglicht es, ein höheres Sicherheitsniveau für die besonders zu schützenden Systeme zu etablieren, ohne dass pauschal alle Systeme kostenintensiv zu schützen sind.

Umsetzungsbeispiel: Ein kritisches Verwaltungssystem für Kundendaten wird netztechnisch durch VLANs getrennt von anderen Systemen, z. B. Webserver die Werbebanner ausliefern, aufgebaut. Innerhalb des Verwaltungssystems befindet sich zudem ein großer Datenbankcluster; dieser wird wiederum in ein eigenes Netzsegment ausgelagert, um eine Trennung von Log- und Statistikservern des Systems herzustellen.

In einer Cloud stehen virtuelle Netzumgebungen zur Trennung von Systemen zur Verfügung, z. B. VPC (Virtual Private Cloud) auf Amazon AWS.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.14-1/3.2

Req 2 Produktionssysteme müssen von Test- und Entwicklungssystemen vollständig getrennt sein.

Neben Servern sind auch Infrastrukturelemente wie Netz- und Speichersysteme zu trennen. Eine in Teilen lediglich logische Trennung ist nur dann zulässig, wenn gewährleistet ist, dass diese logische Trennung nicht umgangen werden kann, und dass eine sicherheitsrelevante Beeinträchtigung der Produktion durch Aktivitäten auf den Test- und Entwicklungssystemen ausgeschlossen ist. Um dies zu erreichen wird eine physische Trennung empfohlen. Für Referenzanlagen muss entschieden werden, ob diese einen eher produktiven Charakter haben oder eher einer Testumgebung zuzuordnen sind.

Eine direkte Kommunikation ist nur dann zulässig, wenn sie absolut unumgänglich ist und über Firewalls geführt wird. Ansonsten sind Übergänge zwischen diesen Netzbereichen über Sicherheitssysteme wie Jumphosts herzustellen.

Testaktivitäten mit Sicherheitsbezug wie Penetrationstests und die Durchführung von Netzwerk-Scans müssen jederzeit ohne schädliche Auswirkungen auf die Produktion durchgeführt werden können.

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

den.

Motivation: Bei Test- und Entwicklungssystemen kann nicht von einem hinreichend sicheren Systemzustand ausgegangen werden, insbesondere da diese naturgemäß permanenten Veränderungen ausgesetzt sind. Bei einer Verknüpfung der Systemarten untereinander oder der Nutzung gleicher Plattformen bestehen die Risiken, dass Unberechtigte aus der Test-/Entwicklungsumgebung heraus auf Produktionssysteme und Wirkdaten zugreifen können oder die Stabilität der Produktionssysteme und damit die Verfügbarkeit der zugehörigen Dienste gefährdet wird. Eine von der Produktion vollkommen unabhängige Test- und Entwicklungs-Infrastruktur ermöglicht auch während einer „Frozen Zone“ Änderungen für Test- und Entwicklungssysteme durchzuführen. So können Sicherheitsupdates schneller getestet und für die Produktion bereitgestellt werden.

Umsetzungsbeispiel: Für Abnahmetests, in denen auch Sicherheits-Scans und Penetrationstests durchgeführt werden, wird eine von der Produktion unabhängige Umgebung verwendet, um jedwede Beeinträchtigung zu vermeiden. Ein weiteres Beispiel ist eine Umgebung für Performancetests, die physisch getrennt von der Produktion aufgebaut ist. Bei Nutzung gemeinsamer Komponenten, z. B. gleiches Speichersystem oder gemeinsames Netz, könnten ansonsten Beeinträchtigungen produktiver Systeme nicht ausgeschlossen werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Verfügbarkeit

ID: 3.14-2/3.2

Req 3 Systemtrennungen dürfen nicht umgangen werden.

Eine Trennung von Systemen oder Systemkomponenten muss an allen Stellen, über die eine Kommunikation möglich ist, mit der gleichen Trennungslogik erfolgen. So muss eine netzbasierte Trennung von Systemen, bspw. durch VLANs, private VLANs oder andere Ebene-2 Techniken, auf allen angeschlossenen Netzbereichen (z. B. Produktionsnetz, Administrationsnetz, Storage-/Backup-Netz) erfolgen. Dasselbe gilt für andere Netztechniken, z. B. Fibre Channel (FC), und auch Hardware-Management, z. B. per ILO. Es ist darauf zu achten, dass keine Kommunikation / Kompromittierung von einem System zum anderen über das Managementnetz erfolgen darf.

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

Umsetzungsbeispiel: Zwei Systeme 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 eines Systems ein Angreifer direkt auf Ebene-2 das andere Systeme unter Umgehung einer möglichen Firewall erreichen.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.14-3/3.2

3. Kommunikation

Die Klassifikation von Daten und der Schutzbedarf bei deren Übertragung sind der Datenschutz- und Sicherheitsempfehlung "Klassifikation von Informationen" der Deutschen Telekom Gruppe entnommen.

Vertraulichkeit und Integrität sind zweierlei Zielstellungen (eine Verschlüsselung verhindert unberechtigtes Mitlesen, ein Schutz der Integrität stellt Veränderungen an den Daten fest). Moderne Kommunikationsprotokolle bieten i. d. R. beides. Zudem ist eine Authentifizierung der Kommunikationspartner erforderlich.

Folgende Tabelle gibt einen Überblick über die Mindestanforderungen nach Verschlüsselung:

	Lokale Übertragung innerhalb DTAG-eigenem RZ über eigene Systeme, Netze und Leitungen	DTAG-internes Netz	Anderes, z. B. öffentliches Netz
Vertraulich	verschlüsselt oder unverschlüsselt*	verschlüsselt	verschlüsselt
Intern	unverschlüsselt	unverschlüsselt	verschlüsselt
Offen	unverschlüsselt	unverschlüsselt	unverschlüsselt

*) unverschlüsselt nur dann, wenn der Schutz durch weitere Maßnahmen sichergestellt ist, siehe unten

Req 4	Es müssen Filterelemente aufgebaut sein, die sicherstellen, dass nur die notwendigen Dienste eines Systems und seiner Komponenten erreichbar sind.
-------	--

Dienste, die nicht erreichbar sind, können auch nicht angegriffen werden. Jedes System muss durch einen unabhängigen Schutzmechanismus, z. B. einen Paketfilter im Netz auf Ebene-3 oder höher, abgesichert sein. Dieser Filter kann im Falle einer Virtualisierungsplattform auch als virtuelle Komponente oder direkt in den Hypervisoren implementiert sein. Entscheidend ist, dass dieser Schutz unabhängig von den zu schützenden Maschinen ist.

Auf einem System könnten Dienste gestartet sein (bspw. durch einen Angreifer oder auch durch ein Systemupdate), die im regulären Betrieb nicht erforderlich sind und die keinesfalls erreichbar sein dürfen. Es ist darauf zu achten, dass ein solcher Schutzmechanismus alle verwendeten Internet Protokoll Versionen (IPv4, IPv6) gleichermaßen unterstützt.

Motivation: Ein unabhängiger netzbasierter Schutzmechanismus verringert die Wahrscheinlichkeit, dass es zu einer Kompromittierung des Systems kommt.

Umsetzungsbeispiel: Innerhalb eines (Sub-)Netzes kommunizieren Server miteinander. Eingehende Verbindungen von außerhalb dieses Netzes sind für diese Dienste nicht erforderlich. Der Router, die Firewall, ein Loadbalancer oder ein entsprechend virtualisiertes Netzelement müssen solche Kommunikationsversuche unterbinden.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.14-4/3.2

Req 5	Die möglichen Kommunikationswege zwischen Systemen müssen durch Filterelemente auf das zur Zweckerfüllung notwendige Minimum reduziert sein.
-------	--

Die Default-Policy muss lauten: deny any any. Bei Freischaltungen muss eine sinnvolle Abwägung zwischen exakten Regeln für einzelne IP-Adressen und der Verwendung vordefinierter IP-Ranges getroffen werden. Die Verwendung von sinnvollen IP-Ranges vermeidet häufiges Ändern des Regelwerks, was zu einer höheren Stabilität führen kann.

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

Motivation: Kommunikationswege ermöglichen Zugriff auf andere Systeme. Je weniger davon existieren, desto besser ist das System geschützt.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.14-5/3.2

Req 6	Der Aufbau einer Maschine-zu-Maschine Kommunikationsverbindung muss beiderseits mit den minimal dafür erforderlichen Rechten erfolgen.
-------	--

Die Initiierung einer Maschine-zu-Maschine-Kommunikation soll wenn möglich mit einem nicht-privilegierten Benutzerkonto erfolgen und nicht als Administrator; der Login auf der Gegenseite muss als Benutzer ohne privilegierte Rechte erfolgen.

Motivation: Potentiellen Schaden minimieren durch Umsetzung des Prinzips der "minimalen Rechte".

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.14-6/3.2

Req 7	Falls schutzbedürftige Daten übertragen werden, müssen die beteiligten Kommunikationspartner ausreichend authentifiziert werden.
-------	--

Schutzbedürftige Daten sind hier „Intern“ oder höher klassifizierte Informationen bzgl. des Schutzziels Vertraulichkeit oder Informationen mit einem erhöhten Bedarf nach Integrität. Für "Vertraulich" klassifizierte Daten ist eine Authentifizierung allein anhand von IP-Adressen in der Regel nicht ausreichend. Empfohlen wird der Einsatz von Zertifikaten.

Motivation: Schutzbedürftige Daten dürfen nicht in falsche Hände gelangen oder von gefälschten Absendern angenommen 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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.14-7/3.2

Req 8 „Vertraulich“ klassifizierte Informationen müssen verschlüsselt übertragen werden.

Grundsätzlich sind vertrauliche Daten verschlüsselt zu übermitteln, z. B. per TLS, IPSec oder SSH. Eine "Ende-zu-Ende"-Verschlüsselung in der Anwendung (z. B. per XML Encryption oder PGP), mit Authentifizierung der Kommunikationspartner, ist gegenüber systemseitiger Verschlüsselung zu bevorzugen.

Eine Ausnahme von der Forderung nach Verschlüsselung liegt nur dann vor, wenn die Übertragung ausschließlich lokal innerhalb eines DTAG-eigenen Rechenzentrums über DTAG-interne Systeme, Netze und Leitungen geführt wird. Ein Beispiel hierfür ist ein Layer-2 Switch, an den alle beteiligten Systeme lokal angeschlossen sind. Es ist sicherzustellen, dass nur Berechtigte Zugang zu diesem Netz haben.

Erfolgt eine Kommunikation über ein Zusammenspiel eines solchen vertrauenswürdigen Netzes mit anderen Netzen, so können – anstatt jede Verbindung einzeln zu schützen – auch Tunnelmechanismen mit Verschlüsselung (z. B. IPSec) zur Überbrückung nicht vertrauenswürdiger Netze eingesetzt werden.

Virtuelle Netz-Konstrukte wie VPNs oder MPLS-Netze, die ohne Verschlüsselung arbeiten, und nur den Verkehr voneinander trennen, sind in der Regel nicht ausreichend zur Übertragung vertraulich klassifizierter Daten. Hier können zusätzliche Geräte eingesetzt werden, die eine Verschlüsselung auf Leitungsebene unabhängig von darüber transportierten Protokollen durchführen.

Motivation: Eine Verschlüsselung stellt sicher, dass Daten auf dem Weg vom Sender zum Empfänger nicht manipuliert werden oder gelesen werden können. Ausschließlich Berechtigte dürfen auf diese Daten zugreifen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.14-8/3.2

Req 9 „Intern“ sowie nicht klassifizierte Inhalte müssen bei der Übertragung über unsichere oder öffentliche Netze (z. B. Internet oder Drahtlosnetze) verschlüsselt werden.

In durch Dritte einsehbaren Netzen kann die Vertraulichkeit interner Informationen nicht sichergestellt werden. Dies gilt auch für Netze innerhalb von "Clouds", die nicht von DTAG-Einheiten betrieben werden.

Motivation: Interne Daten der DTAG müssen vor fremder Einsichtnahme geschützt sein.

Umsetzungsbeispiel: Verwendung von SSH, IPSec; Einsatz von TLS zur Absicherung nicht gesicherter Protokolle wie z. B. IMAP.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.14-9/3.2

4. Schichtenmodell

Req 10 Systeme, die schutzbedürftige Informationen bereitstellen, müssen in mindestens zwei netztechnisch voneinander getrennten Schichten aufgebaut werden.

Schutzbedürftige Informationen sind als „Intern“ oder höher klassifizierte Daten bzgl. des Schutzziels Vertraulichkeit oder Daten mit einem hohen Bedarf an Integrität oder Verfügbarkeit. Ein Schichtenmodell besteht meist aus einer Präsentationsschicht mit direktem Zugriff durch die Anwender, einer Schicht mit Anwendungsservern und als Drittes einer Schicht mit den Datenbanken. Bei einer Vereinfachung auf 2 Schichten laufen die Anwendungsserver mit den Datenbanksystemen zusammen in einer Schicht, so dass die Präsentationsschicht für die Anwender immer separiert ist. In einzelnen Fällen kann ein Loadbalancer als Präsentationsschicht angesehen werden, wenn dieser die (Benutzer-)Anfragen inhaltlich prüfen und ggf. bereinigen kann, bevor die Anfrage weitergeleitet wird.

Die Schichten entsprechen i. d. R. einzelnen Netzen, meist VLANs, die über Filterelemente wie eine Firewall miteinander verbunden sind. In virtualisierten Umgebungen können die voneinander getrennten Schichten auch durch Sicherheitsfunktionen innerhalb der Virtualisierungsinfrastruktur, z. B. sogenannte "Mikrosegmentierung", realisiert werden.

Wird Zugriff auf Datenquellen mehrerer Systeme benötigt, so muss dieser aus einer Anwendungsschicht heraus erfolgen.

Motivation: Ein Schichtenmodell stellt sicher, dass der Nutzer nie einen direkten Zugriff auf Schichten mit schutzbedürftigen Daten erhält. Es gilt nur so wenige Systemkomponenten wie möglich für den Anwender sichtbar zu machen – interne Strukturen dürfen von außen nicht sichtbar sein.

Angriffe auf TCP/IP sowie TLS terminieren auf einem System der Präsentationsschicht. Dadurch ist das Schadenspotential deutlich geringer, als wenn diese Angriffe bis in die Applikationsschicht liefen.

Umsetzungsbeispiel: Datenbanken werden üblicherweise nicht von Nutzern direkt angesprochen sondern über vorgelegte Anwendungsserver. Somit können die Datenbanken so aufgebaut werden, dass sie nicht direkt vom Nutzer erreicht werden können.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.14-10/3.2

Req 11 Die möglichen Kommunikationswege zwischen den Schichten (Netzen) eines Systems müssen durch ein filterndes Element auf das notwendige Minimum begrenzt sein.

Diese Kommunikationseinschränkung muss durch ein von den zu schützenden Systemkomponenten unabhängiges Filterelement erfolgen. Geeignet können je nach Situation neben Firewalls auch Router oder Loadbalancer mit installierten Paketfiltern sein. In virtuellen Umgebungen können dabei in der Virtualisierungsinfrastruktur implementierte Mechanismen wie die sogenannte "Mikrosegmentierung" genutzt werden.

Motivation: Die Verwendung aktiver Filterelemente zwischen den Netzen bietet einen zusätzlichen netzbasierten Schutz für die Systeme. Angriffe auf TCP/IP sowie TLS terminieren auf einem System der Präsentationsschicht. Dadurch ist das Schadenspotential deutlich geringer, als wenn diese Angriffe bis in die Applikationsschicht liefen.

Umsetzungsbeispiel: Ist ein System in Präsentationsschicht (z. B. Webserver) und eine weitere Schicht (z. B. Datenbanken) aufgeteilt, die netztechnisch getrennt sind, so darf die Kommunikation vom Webserver zur Datenbank nur über eine von diesen Systemen unabhängige Firewall möglich sein. Diese ist so konfiguriert, dass sie nur zulässige, notwendige Verbindungen ermöglicht.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System

- Unberechtigte Nutzung von Diensten oder Ressourcen

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.14-11/3.2

Req 12	Schutzbedürftige Informationen dürfen nicht dauerhaft in der Präsentationsschicht gespeichert werden.
--------	---

Die Präsentationsschicht ist direkt (intern oder extern) erreichbar und somit das erste Ziel von Angriffen. Daher dürfen in dieser Schicht keine schutzbedürftigen Informationen (d. h. der Schutzbedarf bzgl. des Schutzziels Vertraulichkeit ist „Intern“ oder höher) länger als absolut notwendig zwischengespeichert werden.

Motivation: Die Speicherung in nachgelagerten Schichten verringert das Angriffsrisiko auf diese Daten.

Umsetzungsbeispiel: Bei der Registrierung von Kunden an einem Webportal dürfen die zu schützenden Kundendaten nicht auf dem Webserver vorgehalten werden. Sie müssen zur Speicherung und weiteren Verarbeitung an die nächste Schicht, einen Anwendungsserver, weitergegeben werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.14-12/3.2

Req 13	Falls Systeme, oder einzelne Systemkomponenten, aus externen Netzen (Nicht-DTAG, z. B. Internet) erreichbar sind, müssen diese physisch von internen Systemen getrennt sein.
--------	--

Alle extern erreichbaren Komponenten sind physisch von internen Systemen zu trennen; dies wird in der Regel durch dafür getrennte Infrastrukturen gewährleistet.

Nicht-DTAG-Netze sind auch Netze von IT-Kunden, die auf Dienste in DTAG-Rechenzentren zugreifen – hier gilt diese Anforderung nicht, wenn die Systeme ausschließlich für und im Auftrag des Kunden, d. h. entsprechend seiner Anforderungen, betrieben werden.

Motivation: Aus z. B. öffentlichen Netzen erreichbare IT-/NT-Systeme sind einem erheblich höheren Angriffspotenzial ausgesetzt als interne Systeme. Alle Anfragen und Daten, die an nachgelagerte Systeme wie Anwendungsserver und Datenbanken weitergereicht werden, müssen zunächst validiert werden. Auf Basis dieser Anforderung kann das Risiko einer nachgelagerten Kompromittierung eines Systems deutlich minimiert werden.

Umsetzungsbeispiel: Ein physisch getrennter Reverse Proxy terminiert HTTPS-Verbindungen. Die dort inhaltlich überprüften Datenpakete werden (ggf. unter Zuhilfenahme einer erneuten Verschlüsselung) an die Zielsysteme weitergereicht.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unbemerkt durchführbare Angriffe

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.14-13/3.2

Req 14	Verbindungen von/zu externen Systemen (Nicht-DTAG) müssen über eine für diese Anwendung geeignete Präsentationsschicht, z. B. einen Webserver oder ausgehenden Proxy, geführt werden.
--------	---

Von extern eingehende und von intern ausgehende Verbindungen werden in der Präsentationsschicht terminiert – auch TLS.

Bei ausgehenden Verbindungen ist festzulegen, wie in Abhängigkeit des Schutzbedarfs der zu übertragenden Daten diese geschützt werden müssen. Ggf. sind entsprechende Vereinbarungen mit dem Empfänger abzuschließen.

Motivation: Zum einen bleibt die interne Netzstruktur verborgen, zum anderen kann der Proxy den Verkehr filtern und insbesondere eingehende Daten prüfen.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.14-14/3.2

5. Verfügbarkeit

Req 15	Auf einer Betriebssysteminstanz dürfen Dienste und Anwendungen nur dann zusammen betrieben werden, wenn sie einer gemeinsamen Administration unterliegen, gleiche Daten-Eigentümer sowie einen vergleichbaren, niedrigen Schutzbedarf haben.
--------	--

Systeme (Dienste/Anwendungen) mit unterschiedlichem oder einem hohem Schutzbedarf sind grundsätzlich voneinander zu trennen. Somit dürfen auf einer Betriebssysteminstanz nur Dienste und Anwendungen laufen,

- die einen gleichen, niedrigen Schutzbedarf haben und
- die administrativ vom gleichen Personenkreis betrieben werden und
- deren Daten einer gemeinsamen Verantwortung unterliegen.

Motivation: Eine Vermischung unterschiedlicher Schutzbedarfe gefährdet einerseits unnötig Anwendungen mit hohem Schutzbedarf, während andererseits geringe Schutzbedarfe auf dafür viel zu aufwändigen Systemen realisiert werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.14-15/3.2

Req 16	Falls ein System/eine Systemkomponente aus externen Netzen (Nicht-DTAG, z. B. Internet) erreichbar ist, darf nur genau ein (Anwendungs-) Dienst auf der entsprechenden Betriebssysteminstanz laufen.
--------	--

Zulässig sind bspw. ein Webserver oder ein Mailserver, aber nicht beide zugleich auf der gleichen Betriebssysteminstanz. Mehrere gleiche Dienste (z. B. Webserver) sind zulässig, solange sie einen gemeinsamen, niedrigen Schutzbedarf aufweisen. Dazu können Sandboxing-Verfahren/Container eingesetzt werden. Spezielle Loadbalancer können für mehrere Anwendungstypen eingesetzt werden, wenn die im Loadbalancer integrierten Schutzfunktionen als ausreichend angesehen werden.

Eine Vermischung interner und externer Dienste muss generell vermieden werden.

Motivation: Wird die Anwendung/das System kompromittiert, dürfen keine weiteren Dienste in Mitleidenschaft gezogen werden.

Umsetzungsbeispiel: Kapseln der Anwendung in einer eigenen, möglichst kleinen, virtuellen Maschine. Diese kann wiederum mit anderen, ähnlichen virtuellen Maschinen gemeinsam auf einem physischen Host platziert werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Störung der Verfügbarkeit

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.14-16/3.2

Req 17	Systeme und Komponenten, auf die nur intern zugegriffen wird, müssen IP-Adressen verwenden, die aus externen Netzen (Nicht-DTAG, z. B. Internet) nicht erreichbar sind.
--------	---

Eine Umsetzung kann auf verschiedene Weisen erfolgen:

- Verwendung spezieller „privater“ bzw. „Unique Local“ IP-Adressen, die im Internet nicht geroutet werden
- Einsatz entsprechender Routing- und Firewall-Regeln bei Verwendung anderer IP-Adressen

Motivation: Diese Maßnahme stellt bereits bei der Adressierung auf Netzebene sicher, dass nur die absolut notwendigen Systeme bzw. Komponenten von extern erreichbar und damit angreifbar sind.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.14-17/3.2

Req 18	Falls das System UDP-basierte Dienste anbietet, müssen Maßnahmen zum Ausgleich der fehlenden Sicherheitsmechanismen des zustandslosen Transportprotokolls getroffen werden.
--------	---

Es müssen Schutzmaßnahmen getroffen werden

- gegen die Verarbeitung von Paketen mit gefälschten Absenderadressen sowie
- gegen die Ausnutzung als Verstärker als Teil eines UDP-basierten Angriffs.

Motivation: DoS-Angriffe gegen das eigene System abwehren und Amplification Attacks verhindern, die auf der Zustandslosigkeit von UDP basieren.

Umsetzungsbeispiel:

- Einsatz eines Monitoring-Systems, um Anomalien in den Anfragen frühzeitig zu erkennen und Abwehrmaßnahmen einzuleiten.
- Eine in der Anwendung implementierte Logik, die bei Erkennung von Angriffsmustern das Antwortverhalten anpasst.
- Keine Bearbeitung von Paketen mit gefälschten Absenderadressen durch frühzeitiges Verwerfen solcher Pakete im Netz.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.14-18/3.2

Req 19	Das System und seine Daten müssen nach einem Ausfall wiederhergestellt werden können.
--------	---

Gemäß Vereinbarungen zur Verfügbarkeit sind Mechanismen zu wählen, die die Nutzbarkeit des Systems gewährleisten und nach einer Fehlersituation wiederherstellen können. Falls ein automatischer Wiederanlauf vorgesehen ist, darf das System keine Abhängigkeiten zu sich selber enthalten, die einen solchen Wiederanlauf verhindern.

Das Einspielen eines Software-Updates ist auch mit dem Risiko eines Ausfalls verbunden. Hier kann ein stufenweiser Mechanismus gewählt werden, der darauf ausgelegt ist, nicht das ganze System in einem Rutsch zu aktualisieren, sondern zunächst nur Teile davon (sogenanntes "Canary Testing"). Nach erfolgreichem Probelauf wird dann der Rest des Systems aktualisiert.

Motivation: Das System muss innerhalb seiner Spezifikation verfügbar sein (inkl. der darin abgelegten und verarbeiteten Daten).

Umsetzungsbeispiel: Klassisches Backup und Recovery, Snapshots von Dateisystemen oder ganzer virtueller Maschinen, Auslagerung der Daten auf zentralen Storage mit eigenem Backup, Wiederherstellung einer Maschine nach Template und in der Konfigurationsdatenbank hinterlegten Informationen, Wiederherstellung mit Automatisierung, z. B. puppet/chef.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.14-19/3.2

Req 20	Ein für das System angewandtes Backup & Restore Design muss sicherstellen, dass abgelegte Datensicherungen im Fall einer Systemkompromittierung oder Systemfehlfunktion nicht beeinträchtigt werden können.
--------	---

Ein System darf keinen permanenten Zugriff auf bereits gesicherte und somit im Sinne des Backup & Restore Konzepts aktuell in der Sicherheitsverwahrung befindliche Datensicherungen erhalten. Ein Zugriff darf nur zum Zweck und für die Dauer eines Datensicherungsvorgangs respektive Datenwiederherstellungsvorgangs gezielt geöffnet werden und muss nach Beendigung des Vorgangs unmittelbar wieder geschlossen werden. Zudem sollte der Zugriff im Rahmen eines Datenwiederherstellungsvorgangs nach Möglichkeit nur lesend geöffnet werden.

Motivation: Permanent im Zugriff stehende Datensicherungen sind bei einer Kompromittierung des Systems potentiell auch für den Angreifer erreichbar, der somit die archivierten Datensicherungen verändern oder beschädigen kann. Im schlimmsten Fall ist dadurch ein kompromittiertes System nicht wiederherstellbar, da keine Datensicherungen mehr zur Verfügung stehen oder deren Integrität nicht mehr gewährleistet ist.

Eine spezifische Bedrohungslage geht hierbei auch von Malware aus, insbesondere sogenannten Crypto-Trojanern, die verstärkt dazu übergehen, nicht nur lokale Dateisysteme eines infizierten Systems, sondern sämtliche erreichbaren Dateisysteme - beispielsweise auch Netzlaufwerke - zu verschlüsseln und enthaltene Daten unzugänglich zu machen. Ein äquivalentes Risiko besteht im Rahmen von Fehlfunktionen in einem System, die ggf. erreichbare Dateisysteme bzw. abgelegte Datensicherungen beschädigen.

Umsetzungsbeispiel: Implementation eines technischen Verfahrens, im Rahmen eines Datensicherungslaufs ein (Archiv-)Netzwerk-Laufwerk nur temporär zu öffnen und nach Abschluss des Kopiervorgangs der zu sichernden Daten wieder zu schließen.

Dieser Ansatz ist jedoch nicht vollständig optimal, da für den Zeitraum des Datensicherungslaufs das Archiv-Netzwerk-Laufwerk auch einem Angreifer wie einem Crypto-Trojaner zugänglich sein kann und somit zumindest temporär wieder ein Risiko für alle dort archivierten Datensicherungen entsteht. Ein unter diesem Gesichtspunkt bessere Lösung wäre, die Daten so auf ein Datensicherungslaufwerk zu schreiben, dass sie anschließend vom schreibenden System nicht mehr verändert werden können.

Eine andere Methode wäre ein Mechanismus auf dem Backup-Ziel-Server, Datensicherungen nach dem Empfang in einen schreibgeschützten Bereich zu verschieben und archivierte Sicherungen so vor Veränderungen durch ein kompromittiertes Quell-System zu schützen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Integrität

Req 21	Falls das System auf einer Cloud-Plattform betrieben wird, muss verhindert werden, dass das System (bzw. der komplette Mandant/Tenant mit all seinen Diensten und Daten) versehentlich oder durch Unbefugte vollständig gelöscht werden kann.
--------	---

Mit einer Administrations-Rolle, die die nötigen Rechte zum Löschen von Ressourcen und ganzen Mandanten/Tenants auf einer Cloud besitzt, ist es möglich, eine komplette Systemumgebung absichtlich oder aus Versehen schnell und vollständig zu löschen. Dabei werden i. d. R. auch Sicherungslaufwerke und Backups dieses Mandanten gelöscht.

Mögliche Maßnahmen um einen Totalausfall zu verhindern können sein: Nutzung eines getrennten Mandanten für einen zweiten Hochverfügbarkeits-Standort, eine Policy, die das Löschen durch einen einzelnen Account/Rolle verhindert oder zumindest eine besondere Absicherung einer solchen Rolle, wenn Ressourcen gelöscht werden sollen.

Alternativ kann auch ein Backup der Daten außerhalb der Cloud eine Lösung sein (lediglich die Daten extra zu sichern sollte ausreichend sein unter der Annahme, dass die Umgebung selber und die darin enthaltene Software automatisiert aus Software-Quellen außerhalb der Cloud-Umgebung vollständig installiert und konfiguriert werden kann).

Motivation: Im Gegensatz zu klassischen Maschinen und Rechenzentren besteht in einer Cloud die Gefahr, dass mit ein paar Mausklicks in der GUI oder einem falschen Kommando über die API vollständige (virtuelle) Umgebungen deprovisioniert werden können. Das System ist somit gegen unbeabsichtigtes Löschen sowie bewusste Angriffe auf dieses Szenario zu schützen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

6. Administration

Hier ist das Login über das Netz gemeint, im Gegensatz zu einem Konsolenzugriff am physischen Server.

Req 22	Der Zugang für System- und Anwendungsadministratoren muss von der Schnittstelle des Anwendungsdatenverkehrs getrennt sein.
--------	--

Administrativer Zugang darf nur auf der Schnittstelle zum Managementnetz angeboten werden. Eigenständige physische Schnittstellen müssen für dieses Netz verwendet werden, wenn sie in den Geräten vorhanden sind oder eingebaut werden können, da diese auch bei einer Überlast oder Störung anderer Schnittstellen noch erreichbar sein können. In Einzelfällen können virtuelle oder logische Schnittstellen ausreichend sein. Für virtuelle Systeme können natürlich nur virtuelle Schnittstellen bereitgestellt werden.

Der Dienst, der zum Login auf das System verwendet wird, z. B. SSH oder RDP, muss allein an die für administrative Tätigkeiten vorgesehene Schnittstelle gebunden sein. Für Systeme, bei denen die Administration über mehrere Schnittstellen erfolgt, ist der Zugriff auf die kleinstmögliche Anzahl zu beschränken.

Motivation: Administrative Zugriffe auf Systeme erfolgen in der Regel mit höheren Privilegien. Diese Trennung ist erforderlich, um verschiedene Arten von Zugriffen und Datenströmen voneinander zu separieren.

Umsetzungsbeispiel: Ein Webserver hat eine Schnittstelle zum Kunden und eine weitere für die Kommunikation mit nachgelagerten Anwendungsservern. Für die Administration dieses Systems ist eine eigene Schnittstelle vorzusehen, auf der die administrativen Zugänge angeboten werden (und nur dort).

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.14-22/3.2

Req 23	Die Sicherheit der zur (interaktiven) Administration verwendeten Arbeitsplätze von Produktionssystemen muss dem Schutzbedarf dieser Systeme genügen.
--------	--

Abhängig vom Schutzbedarf der zu administrierenden Systeme, deren (Geschäfts-)Kritikalität und möglichen Bedrohungen müssen passende Maßnahmen zur Sicherung der Arbeitsplätze getroffen werden. Ziel ist es, eine Kompromittierung der Produktionssysteme durch Zugriffe über unsichere Arbeitsplätze zu vermeiden. Dazu sind geeignete und angemessene Maßnahmen zu wählen. Möglichkeiten sind:

- Nutzung gesonderter, getrennter Admin-Arbeitsplätze gänzlich ohne Bürofunktionalität ("privilegierte Arbeitsstation")
- Nur eingeschränkter, besonders abgesicherter Zugang zum Internet, dem WWW und E-Mail
- Nutzung von Jumphosts für Zugriffsreglementierung (ggf. mit Protokollierung bei besonderer Anforderung und entsprechender Vereinbarung)
- Nutzung geeigneter (grafischer) Terminal-Lösungen
- Dateiübertragung vom/zum System nur über Zwischensysteme mit Malware-Scannern
- Arbeitsplatz unterliegt einem Sicherheitsmanagement, z. B. für das Einspielen notwendiger Sicherheits-Aktualisierungen

Falls ein System nur extern (z. B. über das Internet) erreichbar ist, muss der administrative Zugriff auf das Betriebssystem und die Anwendungen auf fest definierte Quell-IP-Adressen eingeschränkt sein.

Motivation: Eine Kompromittierung durch eingeschleuste Malware oder nicht-autorisierte Benutzer verhindern.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.14-23/3.2

Req 24	Falls das System einen hohen Schutzbedarf hat, muss der interaktive, administrative Zugang über einen oder mehrere fest definierte Jumphosts erfolgen.
--------	--

Ein Jumphost dient der Kanalisierung der administrativen Zugänge. Ein Jumphost ist einer stark begrenzten Anzahl Systemen eines Herstellers und einer Technik zugeordnet. Für Systeme im gleichen Anwendungskontext, deren Betrieb vom gleichen Personenkreis durchgeführt wird, kann ein gemeinsamer Jumphost zugeordnet werden.

Wird der Zugang nur von sehr wenigen Arbeitsplätzen (<5) benötigt, und sind diese als sicher und vertrauenswürdig anzusehen, so sollte der Mehrwert des Jumphosts geprüft werden gegen den Aufwand diesen zu implementieren und zu pflegen. Ist eine ausreichende Absicherung des Zugangs nur für diese wenigen sicheren Arbeitsplätze sichergestellt, z. B. durch Firewall-Regeln, kann im Einzelfall auf den Jumphost verzichtet werden.

Ein Jumphost muss nur dann eine Verbindung terminieren und zum Zielsystem neu aufbauen, wenn dem Arbeitsplatzsystem der zugreifenden Person nicht vollständig vertraut wird, oder ein Logging aller Aktivitäten notwendig ist.

Je nach Kritikalität eines Systems können Jumphosts auch für Benutzerzugänge notwendig sein.

Motivation: Technisch sicherstellen, dass nur ein möglichst kleiner Kreis Berechtigter Zugang zum System erhält.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unbemerkt durchführbare Angriffe

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.14-24/3.2

Req 25	Falls ein manipulationsresistentes Logging von Zugängen und Aktivitäten erforderlich ist, muss dies mit Hilfe eines speziell dafür ausgelegten Jumphost erfolgen.
--------	---

Wird ein manipulationsresistentes Logging der System-Administrationstätigkeiten benötigt, so muss zunächst durch technische Restriktionen zwangsweise ein Jumphost (Hopping, Terminalserver o. ä.) zum Login auf das Zielsystem verwendet werden. Nutzer des Jumphosts dürfen auf diesem über keine administrativen Rechte verfügen. Auf dem Jumphost ist ein geeignetes Logging einzurichten.

Motivation: Nur so kann ein Audit-Trail sichergestellt werden.

Umsetzungsbeispiel: Der Zugriff mit administrativen Rechten von Mitarbeitern externer Firmen auf interne Systeme der DTAG unterliegt im Regelfall diesen Restriktionen. Eine Umsetzung für einen solchen Jumphost ist in der Sicherheitsanforderung "Fremdfirmenzugänge" beschrieben.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Abstreiten von durchgeführten Aktionen

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.14-25/3.2

7. Einhaltung von Industriestandards

Req 26 Falls das System Zahlungsverkehrsdaten für Kreditkarten verarbeitet oder speichert, müssen Vorgaben und Regeln von PCI DSS eingehalten werden.

Die Vorgaben und Regeln von PCI DSS (Payment Card Industry Data Security Standards) sowie ggf. weiterer Sicherheitsstandards der Zahlungsmittelindustrie sind in jedem Fall für Systeme einzuhalten, die Zahlungsverkehrsdaten von Kreditkarten verarbeiten, durchleiten oder speichern. Dies gilt auch für interne und externe Dienstleister, die für die Deutsche Telekom Gruppe entsprechende Systeme betreiben und dabei Zahlungsverkehrsdaten verarbeiten, durchleiten oder speichern. Solche Dienstleister müssen die PCI DSS Compliance nachweisen.

Motivation: Die Umsetzung dieser Anforderung ist für den Nachweis der PCI DSS Compliance der Deutschen Telekom Gruppe und der Systeme, die für die Verarbeitung von Zahlungsverkehrsdaten genutzt werden, notwendig. Andernfalls ist eine solche Verarbeitung nicht zulässig.

ID: 3.14-26/3.2