

Sicherheitsanforderung

Verwendung von Public Clouds

Deutsche Telekom Gruppe

Version	5.0
Datum	01.07.2025
Status	Freigegeben

Impressum

Herausgeber
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Deutschland

Dateiname	Dokumentennummer 3.66	Dokumententyp Sicherheitsanforderung
Version 5.0	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

Dieses Dokument behandelt die sichere Nutzung von „Public Cloud“-Diensten. Die Anforderungen in diesem Dokument sind meist grob umrissen, sodass sie die meisten Cloudanbietern und Anwendungsfälle abdecken können. Dieses Dokument enthält keine technischen Implementierungsdetails für bestimmte Cloudanbieter.

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.	Einführung in Cloud Computing	5
3.	Voraussetzungen für die Nutzung der Public Cloud	7
4.	Governance und Management	13
4.1.	Schutz von Sitzungen	24
5.	Authentifizierung und Autorisierung	26
6.	Authentisierungsmerkmal "Passwort"	38
7.	Schutz von Daten und Informationen	45
8.	Schutz von Verfügbarkeit und Integrität	50
9.	Architektur und Vernetzung	54
9.1.	Anbindung der Cloud	56
9.2.	Anbindung der Cloud - Externe Anbindung	57
9.3.	Anbindung der Cloud - Interne Anbindung	60
10.	Protokollierung und Überwachung	62
11.	Querverweise und Quellenangaben	71
12.	Glossar	72

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.

Sollte die Einhaltung der beschriebenen Anforderungen in individuellen Fällen nicht oder nur eingeschränkt umsetzbar sein, sind gemeinsam mit einem Sicherheits- und/oder Datenschutzexperten (entsprechend der betroffenen Anforderungen) Risikobewertungen vorzunehmen und mögliche alternative Schutzmaßnahmen abzustimmen.

2. Einführung in Cloud Computing

Einführung

Laut NIST (National Institute of Standards and Technology) ist Cloud Computing ein Modell, das bei Bedarf – meist über das Internet und geräteunabhängig – zeitnah und mit wenig Aufwand geteilte Computerressourcen als Dienstleistung, etwa in Form von Servern, Datenspeicher oder Applikationen, bereitstellt und nach Nutzung abrechnet. Angebot und Nutzung dieser Computerressourcen ist definiert und erfolgt in der Regel über eine Programmierschnittstelle (API) bzw. für Anwender über eine Website oder App. Dieses Cloud-Modell setzt sich aus fünf wesentlichen Merkmalen, drei Servicemodellen und vier Bereitstellungsmodellen zusammen.

Umfang

Dieses Dokument deckt die folgenden Themen ab:

- Sicherheitsanforderungen für die Nutzung der Public Cloud APIs, IaaS und andere angebotene Services
- Sicherheitsanforderungen für das Management der Cloud
- Sicherheitsanforderungen für Cloud-Nutzer und darauf laufende Anwendungen

Es werden folgende Cloudtypen behandelt:

- Public Cloud

Diese Cloudtypen werden in diesem Dokument nicht betrachtet:

- Private Cloud
- Community Cloud

Hybride Clouds werden nicht direkt behandelt. Falls eine Applikation Public und Private Cloud nutzt, gelten diese Anforderungen für alle Anwendungsbestandteile, welche in der Public Cloud laufen.

Was wird behandelt:

- Public Cloud API – Verwendung, Konfiguration und Limits
- Public Cloud Dienste

Was nicht behandelt wird:

- Anforderungen an Betriebssysteme und Applikationen
- Container und Orchestrierungstechniken (z. B. Docker oder Kubernetes)

Shared Responsibility Model (Modell der geteilten Verantwortung)

Die Sicherheit der Cloud und der auf der Cloud bereitgestellten Dienste ist Aufgabe sowohl des Cloud-Service-Anbieters als auch des Cloud-Konsumenten. Die Sicherheit der Cloud-Plattform und der angebotenen Dienste liegt in der Verantwortung des Cloud-Service-Providers, während ihre Nutzung, entweder direkt oder als Bausteine für einen endgültigen Dienst, in der Verantwortung des Cloud-Konsumenten liegt (Sicherheit in der Cloud genannt). Die Grenze hängt vom verwendeten Servicemodell ab, z. B. muss der Cloud-Anbieter bei der Verwendung von IaaS den Hypervisor sichern und das Netz sowie den Speicher zwischen den Mandanten trennen, während der Cloud-Kunde (Mandant) die virtuellen Maschinen und die darin laufende Software ordnungsgemäß sichern muss.

Dieser Ansatz wird als Shared Responsibility Model bezeichnet und kann hier visuell eingesehen werden: <https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>.

An dieser Stelle sollte erwähnt werden, dass der Cloud-Kunde weiterhin für die Sicherheit der Daten verantwortlich ist, unabhängig vom Shared Responsibility Model.

Hintergrund

Informationssicherheit wird nach ISO/IEC 27000:2014 wie folgt definiert: „Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen. Hinweis: Darüber hinaus können auch andere Eigenschaften, wie z. B. Authentizität, Nachvollziehbarkeit, Nichtabstreitbarkeit und Zuverlässigkeit betroffen sein.“

Bedrohungen, die entweder absichtlich oder aus der Umgebung, durch Unfälle oder Fahrlässigkeit entstehen, werden typischerweise in die folgenden Typen klassifiziert:

- Physischer Schaden

- Naturereignisse
- Verlust grundlegender Services
- Kompromittierung von Informationen und Daten
- Technische Ausfälle
- Kompromittierung von Funktionen

Schutzmechanismen gegen Bedrohungen können Schutzmechanismen des Cloud-Service-Providers sein (die vom Kunden noch entsprechend konfiguriert werden müssen) und solche, die der Kunde zusätzlich zu anderen Diensten des Cloud-Anbieters oder natürlich eine Kombination aus beidem.

In einer Cloud-Umgebung ist es, wie in jeder anderen Datenverarbeitungsumgebung auch, notwendig, die Daten zu klassifizieren. Dabei muss nicht nur die Datenverfügbarkeit, sondern auch der Lebenszyklus der Daten berücksichtigt werden (z. B. wann die Daten archiviert, gelöscht usw. werden können) bzw. ist es nötig, die Daten während des gesamten Lebenszyklus zu schützen.

3. Voraussetzungen für die Nutzung der Public Cloud

Cloudanbieter (CSP - Cloud Service Provider) bieten ihren Kunden Rechenleistung (z. B. Speicher, Netzkomponenten, Anwendungen, etc.), welche abhängig von der Nutzung durch diese konsumiert werden kann. Die Ressourcen können durch APIs oder sogenannte Cloud-Konsolen (Weboberfläche zur Administration der Ressourcen bei einem CSP) verwaltet, provisioniert und allokiert werden. Der CSP ist sowohl für den sicheren Betrieb der Cloudinfrastruktur als auch der angebotenen Services und APIs verantwortlich, während der Kunde für alle Komponenten, welche auf den konsumierten Ressourcen aufbauen, verantwortlich ist.

Req 1	Bevor eine Applikation in der Cloud betrieben werden darf, muss die relevante Dokumentation der jeweiligen Cloudservices verstanden werden.
-------	---

Alle Nutzer, einschließlich der Betreiber einer Landing Zone und insbesondere des Applikationsbetriebs, müssen sich ausführlich mit den Funktionen und Verhaltensweisen der konsumierten Cloudservices beschäftigen und diese verstehen. Den Betreibern einer Landing Zone wird empfohlen, relevante Informationen für die Nutzer vorzubereiten, sodass der Onboardingprozess einfacher und schneller gestaltet wird. Hierbei kann es sich zum Beispiel um Bedingungen zur Cloudnutzung oder der Nutzung bestimmter Services handeln.

Motivation: Die Sicherheit der Services eines CSP (Cloud Service Provider) ist in der Regel gegeben, da die Services öffentlich verfügbar sind und damit fortlaufend von verschiedenen Seiten auf Sicherheitsprobleme untersucht werden. Daraus ergibt sich, dass die meisten Sicherheitsprobleme, die bei einem konsumierten Service auftreten, vor allem durch fehlerhafte Konfigurationen durch die Nutzer hervorgerufen werden. Beispiele sind:

- *Sogenannte Buckets sind (versehentlich) vom Internet und somit öffentlich erreichbar.*
- *Erstellung und Verwendung sogenannter „Allow-All“ Security Groups (ein- und ausgehend), wodurch z. B. Datenbanken im Internet erreichbar werden.*
- *(versehentliches) Offenlegen von Anmeldeinformationen von Cloud-Diensten (Debug-Ausgabe aktiviert, Schlüssel im Klartext in CI/CD-Kette)*

Umsetzungsbeispiel: Zur relevanten Dokumentation gehört unter anderem:

- Freigabe des CSP und des verwendeten Services innerhalb der DTAG und wie Daten dort verarbeitet werden können und dürfen (oder eben nicht).
- Dokumentation des konsumierten Cloudservices, sowie den Sicherheitsempfehlungen durch den CSP oder der DTAG (wenn verfügbar).
- Weitere PSA-Anforderungskataloge, da diese weiterhin gültig sind; auch bei der Nutzung von Cloudumgebungen.

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: 3.66-1/5.0

Req 2	Der CSP und bestimmte Servicemodelle dürfen nicht verwendet werden, solange keine BoM (Board of Management) Entscheidung durch die DTAG vorliegt. Einschränkungen bezüglich der freigegebenen Datenschutzzklassen und Informationsschutzklassen müssen eingehalten werden. In Ergänzung zur BoM können weitere offizielle Verfahren und Prozesse, wie der Simplified Cloud Approval Process (SCAP) für die Cloud-Service-Freigabe, zur Anwendung kommen.
-------	--

Der CSP ist für die Sicherheit der Infrastruktur, der Services und der APIs verantwortlich. Dies bildet die Basis für die gesamtheitliche Sicherheit. Des Weiteren ist der CSP für die Einhaltung rechtlicher Verpflichtungen und der SLA zuständig. Da es unmöglich ist, durch alle Kunden eines CSPs Audits für diesen durchzuführen, wird dies typischerweise von unabhängigen Auditoren durchgeführt, die diese durchführen und Auditberichte erstellen.

Der wichtigste Bericht aus dem Audit ist der SOC-2 Typ 2, der von der Telekom Security ausgewertet wird, bevor Verträge mit dem CSP unterzeichnet werden. Wenn ein BSI-C5-Auditbericht vorhanden ist, muss dieser ebenfalls ausgewertet werden.

Neben der technischen Sicherheitsbewertung des CSP auf Basis von Auditberichten werden auch rechtliche und vertragliche Aspekte kombiniert und eine Empfehlung an den DTAG-Vorstand gegeben, der letztlich entscheidet, ob die Nutzung des bestimmten CSP erlaubt ist. Hierfür wird eine jeweilige Liste spezifischer Servicemodelle und Dienste veröffentlicht, welche verwendet werden dürfen.

Der „Trusted Cloud Provider Approach“ sollte hierfür beachtet werden und ist separiert im YAM zu finden, da er sich wesentlich öfter ändert, als diese Anforderungen: <https://yam-uni ted.telekom.com/pages/cloud-infrastructure-security/apps/blog/view/ac4dd58b-6f85-477d-b3f1-e98829bb354f>. Weitere Informationen gibt es auch hier bei DT Cloud Taskforce: <https://yam-uni ted.telekom.com/pages/dt-cloud-taskforce/apps/wiki/wiki/list>, wo auch Kontakte zu Verantwortlichen zu finden sind. Der Link zur aktuellen Version des Simplified Cloud Approval Process (SCAP), besonders nützlich für SaaS-Cloud-Dienste, ist hier zu finden: <https://yam-uni ted.telekom.com/pages/psa/apps/content/materials>. Man kann über die gleichen Links entsprechende Kontakte finden, um Informationen über bereits genehmigte Cloud-Dienste zu erhalten.

Motivation: Jedes Servicemodell und jeder einzelne Dienst jedes CSP kann eine andere Freigabe für unterschiedliche Datenklassen haben. Zum Beispiel bedeutet die Freigabe für die Verarbeitung und Speicherung personenbezogener Daten in einem IaaS eines CSP nicht automatisch, dass die Verarbeitung und Speicherung von personenbezogenen Daten für das IaaS eines anderen CSP erlaubt ist, auch wenn in beiden Fällen das IaaS als Servicemodell zugelassen ist.

Aufgrund der steigenden Anzahl von Public-Cloud-Anbietern und deren Diensten können bestimmte PaaS- und SaaS-Anbieter oder Dienste, die in der ursprünglichen DTAG BoM-Genehmigung nicht enthalten waren, von anderen Managementeinheiten zugelassen werden. Allerdings müssen diese Managementeinheiten entsprechende DTAG-Sicherheitsverantwortliche einbeziehen.

Umsetzungsbeispiel: Beispiel für eine Freigabe: Basierend auf der Evaluierung hat das BoM der DTAG entschieden, dass der Cloud-Anbieter X von der DTAG genutzt werden darf. Es sind alle Arten von IaaS-Workloads mit beliebigen Daten, inklusive den Key-Value-Datenbanken aus dem PaaS-Portfolio für alle nicht personenbezogenen Daten zugelassen. Allerdings sind alle SaaS-Dienste verboten.

Kann die DTAG VMs, virtuelle Router, Firewalls und andere Dienste nutzen, die eng mit VM-Compute-Services verbunden sind?

- Ja

Kann die DTAG Daten innerhalb einer Key-Value-Datenbank speichern?

- Allgemein, ja. Allerdings sollte hierfür die Freigabe berücksichtigt werden, welche die freigegebenen Datenklassen spezifiziert.

Kann die DTAG IoT SaaS-Lösungen eines CSP für die Verwaltung von IoT-Geräten verwenden?

- Nein, solche Services sind nicht freigegeben.

Kann die DTAG PCI-DSS Daten in der Cloud verarbeiten?

- Im Allgemeinen nicht, obwohl viele Cloud-Anbieter PCI-DSS-konform sind, muss geprüft werden, ob die Zertifizierung für alle Dienste vom CSP gilt, die die DTAG nutzen möchte. Für die Verwendung von PCI-DSS gibt es eine zusätzliche Anforderung in diesem Kapitel.

Kann die DTAG personenbezogene Daten auf IaaS-Level verarbeiten und speichern?

- Ja

Kann die DTAG personenbezogene Daten in einer Key-Value-Datenbank speichern?

- Nein

Kann die DTAG Software eines Anbieters X verwenden, welcher die Lösung auf Azure – Giant Swarm aufbaut?

- Anbieter X wird hier als Drittanbieter, welcher Giant Swarm verwendet, betrachtet. Hierbei handelt es sich um eine SaaS-Lösung, die durch Microsoft Azure angeboten wird. Wenn Azure als CSP freigegeben ist und eine Freigabe für SaaS, inklusive Giant Swarm, vorliegt, ist die Antwort ja. Dennoch muss eine Sicherheitsbetrachtung des Drittanbieters durchgeführt werden. Insbesondere Datenklassifizierungen und -einschränkungen sollten untersucht werden. Falls es keine Freigabe für Giant Swarm geben sollte, ist eine separate DTAG BoM (oder equivalent) Entscheidung notwendig, welche die Verwendung der Software des Drittanbieters bewertet.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.66-2/5.0

Req 3	Alle geltenden Gesetze, Vorschriften und Unternehmensrichtlinien müssen berücksichtigt und befolgt werden, bevor die Cloud für ein System oder Daten verwendet werden darf.
-------	---

Unabhängig davon, ob Bestandssysteme (bzw. Teile davon), Daten oder neu entwickelte Systeme in die Cloud migriert werden sollen, müssen alle gesetzlichen Regularien und Konzernvorgaben eingehalten werden. Dazu zählen unter anderem:

- Rechtmäßiges Abhören
- Vorratsdatenspeicherung
- Einschränkungen hinsichtlich geografischer Grenzen, sowohl für Daten at Rest (z. B. welche Regionen, Rechenzentren oder Verfügbarkeitszonen genutzt werden dürfen), als auch für Data in Use / Transit (z. B. ist es erlaubt, Daten über das Internet oder über geografische Grenzen hinweg zu übertragen).
- Telekommunikation/Kommunikationsgesetz
- Datenbeschaffung

Es muss überprüft werden, ob der Cloud-Anbieter ausreichende Kontrollen zur Erfüllung der Anforderungen bietet und ob diese Anforderungen als Richtlinien für das System oder die Daten, die in der öffentlichen Cloud gehostet werden, implementiert sind.

Motivation: Die Nichtbeachtung von Gesetzen und Vorschriften kann zu finanziellen Schäden oder Rufschädigungen der DTAG, sowie zu rechtlichen Konsequenzen der Mitarbeiter führen.

Umsetzungsbeispiel: In Bezug auf die Implementierung bieten Cloud-Anbieter eine Vielzahl von konfigurierbaren Richtlinien, die es dem Cloud-Kunden ermöglichen Einschränkungen zu konfigurieren, die durch Gesetze, regulatori-

sche Anforderungen und Unternehmensrichtlinien in der gesamten Landing Zone, d. h. für alle Verbraucher der Cloud einer bestimmten Organisation. Für alle Einschränkungen, die nicht durch die Richtlinien des CSP durchgesetzt werden können, müssen entsprechende administrative und/oder organisatorische Kontrollen vorhanden sein. Personen, die die Cloud-Dienste nutzen, müssen über die Einschränkungen informiert werden und diese befolgen.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.66-3/5.0

Req 4	Der CSP und seine Dienste dürfen nicht für schutzbedürftige Daten, insbesondere PCI-DSS-Daten, genutzt werden, es sei denn, der CSP bietet entsprechende Garantien, beispielsweise eine PCI-DSS-Zertifizierung. Des Weiteren muss diese Art der Nutzung von der DTAG-Geschäftsführung genehmigt werden.
-------	---

Obwohl viele Cloud-Anbieter PCI-DSS-konform sind, ist zu prüfen, ob die Zertifizierung für alle Dienste des CSP gilt, die die DTAG nutzen möchte. Zusätzlich zur Zertifizierung ist es erforderlich, dass der Vorstand der DTAG den CSP und die spezifischen Dienste für die Nutzung mit PCI-DSS-Daten freigegeben hat.

Motivation: Die Nichteinhaltung der PCI-DSS-Anforderungen für den Umgang mit Kreditkartendaten kann zu Geldstrafen für die DTAG führen.

Umsetzungsbeispiel: Dieses Verfahren (Prüfung des spezifischen Diensts des CSP) gilt generell für schutzbedürftige Daten, nicht nur für PCI-DSS-Daten, obwohl PCI-DSS ein sehr prominentes Beispiel für solche Anwendungsfälle ist.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.66-4/5.0

Req 5	Vor dem Onboarding eines Projekts oder eines Systems auf einer Public Cloud muss eine klare Exit-Strategie existieren.
-------	--

In der traditionellen Welt wurde dieses Problem durch eine Dual- (oder Multi-) Vendor-Strategie gelöst, um Vendor-Lock-ins zu vermeiden. Der Übergang von einem Anbieter zum Anderen war möglich, weil die Geräte von der DTAG gekauft wurden und ihr gehörten. Dies ist nicht der Fall bei der Nutzung von Public Cloud-Anbietern. Zwei oder mehr CSPs zur Verfügung zu haben, ist nicht ausreichend für eine Dual- (oder Multi-) Vendor Strategie. Es ist auch notwendig, die betroffenen Systeme und Daten zu verlagern, entweder vom CSP zu einem anderen CSP oder vom CSP in die eigenen Räumlichkeiten.

Verträge und Gerichtsverfahren können nicht als brauchbarer Ersatz für eine Ausstiegsstrategie angesehen werden.

Beispiele für Probleme:

- Der CSP erhöht die Preise, was die Lösung unwirtschaftlich macht.
 - Ein anderer CSP hat weiterhin günstigere Preise -> eine Migration macht Sinn. Ein Konzept muss von Beginn an existieren, um Vendor Lock-In zu vermeiden.
- Der CSP meldet Bankrott, Hardware wird beschlagnahmt und der Betrieb eingestellt.
- Der CSP bietet schlechten Service (SLA wird nicht erfüllt) und kann technische Probleme über mehrere Stunden / Tage / Monate nicht lösen.
- Der CSP kündigt an, einen Service abzusetzen, welcher von der DTAG konsumiert wird.
- Der CSP kann aufgrund von gesetzlichen Regularien nicht mehr eingesetzt werden.
- Die Entwicklung einer Applikation, welche von der API eines CSP abhängig ist (z. B. AWS BeanStalk), führt da-

zu, dass die Applikation bei einer Migration vollständig neu entwickelt werden muss.

Motivation: Trotz guter Absichten und Verträge ist es möglich, dass der CSP nicht in der Lage sein wird, die Bedürfnisse der DTAG und der jeweiligen Systeme auch in Zukunft zu erfüllen. Um mögliche rechtliche, finanzielle oder technische Probleme zu berücksichtigen ist es notwendig einen Plan zu haben, um Dienste und Daten von einem bestimmten Cloud-Anbieter und zu einem bestimmten Zeitpunkt runter migrieren zu können.

Umsetzungsbeispiel: Wenn möglich, sollten Cloud-Konsumenten in Erwägung ziehen, mehr generische Cloud-Dienste zu nutzen, so dass der Übergang in die Public Cloud von einem anderen CSP (oder in die eigenen Räumlichkeiten) mit minimalen Modifikationen (oder im besten Fall ohne Modifikationen) erfolgen kann.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen

ID: 3.66-5/5.0

Req 6 Die Cloud-Dienste des CSP dürfen nur über die freigegebene Landingzone genutzt werden.

CSP und DTAG unterzeichnen in der Regel einen einzigen Vertrag und die DTAG erhält ein einziges großes Konto innerhalb von CSP. Innerhalb dieses Kontos kann die erforderliche Hierarchie erstellt werden, z. B. durch Nachahmung der Organisationsstruktur. Grundlegende Regeln (z. B. minimale Passwortlänge) würden für alle DTAG-Benutzer dieses CSP gelten, während einige system- bzw. anwendungsspezifische Regeln (z. B. ob eine VM auf das Internet zugreifen kann oder nicht) von den Eigentümern einer bestimmten Organisation oder eines Projekts festgelegt würden.

Jede Ausnahme von dieser Regel erfordert eine separate BoM (Board of Management)-Entscheidung, entsprechend der aktuellen Situation zum Zeitpunkt des Schreibens.

Eine Landing Zone für SaaS-Cloud-Dienste wird von SaaS-Cloud-Anbietern manchmal einfach als "Verwaltungsportal/Adminportal" bezeichnet. Dies darf nicht mit einer bestehenden Landing Zone der DTAG für andere Clouds verwechselt werden, wie z. B. der DTIT Landing Zone für AWS, Azure und GCP.

Eine Landing Zone von einem SaaS-Anbieter hat in der Regel einen geringeren Funktionsumfang im Vergleich zu den Varianten der großen Cloudanbieter (Hyperscalern), bietet aber dennoch Aspekte wie die Verwaltung von Benutzern (Hinzufügen und Entfernen), Berechtigungen (Einrichten von Administratoren, Zuweisen von Benutzern zu Gruppen), Einschränkungen bei der Datenaufbewahrung (Chat-Verlauf, maximale Lebensdauer von Dokumenten), Protokollverwaltung (Anzeigen und Exportieren von Audit-Protokollen), Verwaltung von Abrechnung und Zahlung, Einrichten von Kontingenten (Begrenzung der Anzahl der Benutzer oder der Datenmenge), Anzeigen von Nutzungsinformationen und Einrichten von Benachrichtigungen für bestimmte Ereignisse.

Die Freigabe des SaaS-Cloud-Dienstes durch den Sicherheitsberater umfasst auch die Freigabe der Landing Zone des SaaS-Cloud-Dienstes, da es sich um den Ort für die Verwaltung dieses SaaS-Cloud-Dienstes handelt.

Motivation: Eine Umgehung der Landing Zone (z. B. durch Anlegen eines anderen Root-Kontos) würde die Umgehung aller Richtlinien ermöglichen und ist verboten.

Umsetzungsbeispiel: Die Nutzung einer freigegebenen Landing Zone. Es darf keine separate Landing Zone ohne BoM Freigabe erstellt werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.66-6/5.0

Req 7 Nicht benötigte Dienste müssen deaktiviert werden.

Nach der Installation von Systemen und Softwareprodukten sind häufig herstellenseitig 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.

Im Kontext der Cloud bedeutet das: Alle Cloud-Dienste, die nicht benötigt werden oder außerhalb des Geltungsbereichs einer Landing Zone oder eines Projekts liegen, müssen deaktiviert werden, sofern der Cloud-Dienstanbieter dies unterstützt (bspw. service control policies)

Im Zusammenhang mit SaaS-Cloud-Diensten bedeutet dies effektiv, unerwünschte und unnötige Funktionen und (Unter-)Dienste zu deaktivieren.

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.

Umsetzungsbeispiel: Für Azure oder AWS können Azure-Policies oder AWS Service Control Policies verwendet werden, um den Zugriff auf die Dienste zu verhindern, die nicht benötigt werden.

Beispiele für SaaS-Dienste sind die Deaktivierung der Dateifreigabe, wenn sie nicht verwendet wird, Protokolle und Schnittstellen, die nicht benötigt werden, oder Analysen für Übersetzungsdienste, insbesondere wenn die Daten zur Verbesserung des Übersetzungsdienstes verwendet werden, um Datenlecks zu verhindern.

ID: 3.66-7/5.0

4. Governance und Management

Req 8	Prozess für den Umgang mit Missbrauchs- und Vorfallsmeldungen vom und zum CSP muss etabliert werden.
-------	--

CSP benachrichtigen Kunden in der Regel bei festgestelltem Missbrauch und Vorfällen, manchmal auch bei festgestellten Unregelmäßigkeiten (z. B. ein sprunghafter Anstieg des Ressourcenverbrauchs). Die Landing-Zone-Betreiber müssen in Zusammenarbeit mit dem zuständigen SOC einen Prozess etablieren, der die Bearbeitung solcher Meldungen rund um die Uhr ermöglicht.

Ebenso muss es für einen Cloud-Nutzer oder Landing-Zone-Betreiber möglich sein, Vorfälle und Missbrauch an den CSP zu melden, was durch die Landing-Zone-Betreiber in Absprache mit dem zuständigen SOC organisiert werden kann.

Motivation: CSP können Missbräuche und Vorfälle erkennen, auch wenn der Kunde diese nicht bemerkt. In solchen Fällen wird der Kunde benachrichtigt.

Umsetzungsbeispiel: Ein E-Mail-Postfach, das rund um die Uhr überwacht wird, oder eine Telefonnummer mit permanent diensthabendem Personal dahinter.

Für diese Anforderung sind folgende Bedrohungen relevant:

- 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: 3.66-8/5.0

Req 9	Für alle Assets in der Cloud muss ein zentrales Asset-Inventar geführt werden und ein Prozess zur Verwaltung der Assets muss etabliert werden.
-------	--

Jedes System in der Cloud ist dafür verantwortlich, den Überblick über seine Assets zu behalten. Assets sollten, wenn möglich, mit Tags versehen oder auf andere Weise markiert werden, so dass es möglich ist, den Systembesitzer und die Personen, die im Falle eines Sicherheitsvorfalls benachrichtigt werden müssen, leicht zu identifizieren. Zusätzlich muss die Kritikalität, die Priorität im Falle einer Wiederherstellung, und die geschäftlichen Relevanz des jeweiligen Assets bestimmt werden. Die Details hängen von der Landing Zone und der Art und Weise, wie die Behandlung von Sicherheitsvorfällen zwischen Landing Zone-Betreibern, Systemverantwortlichen und dem verantwortlichen SOC organisiert wurde, ab.

Motivation: Alle Cloud-Assets (virtuelle Maschinen, IP-Adressen, Storage-Buckets, URLs von Serverless-Funktionen, etc.) haben in der Regel einen (monatlichen) Preis. Daher ist es extrem wichtig, den Überblick über alle Assets zu behalten. Die zusätzlichen Kosten sind nicht das einzige Problem in der Cloud. Übrig gebliebene Assets können auch als leichtere Angriffspunkte genutzt werden.

Umsetzungsbeispiel: Falls verfügbar, sollte das zentrale Asset-Management-System auch die Asset-Informationen aus der Cloud enthalten, vorzugsweise durch die Landing Zone.

Der beste Weg für ein verantwortliches SOC, auf den Anlagenbestand in der Cloud zuzugreifen, ist über eine API, da die Informationen dann aktuell sind. In einigen Fällen können jedoch regelmäßige periodische Exporte und Snapshots den Zweck erfüllen, wenn der API-Zugriff nicht möglich oder bequem ist.

Bei SaaS-Cloud-Diensten gibt es selten detaillierte Asset-Berichte. In manchen Fällen kann aber eine Abrechnungsübersicht oder eine ähnliche, regelmäßig erstellte Zusammenfassung ausreichen. Andererseits könnte man für die Befüllung eines Asset-Inventars für Backup-as-a-Service einen größeren Aufwand erwarten.

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: 3.66-9/5.0

Req 10 Sicherheitsrelevante Aufgaben müssen automatisiert werden, um menschliche Fehler zu vermeiden.

Typische Aufgaben, die nach Möglichkeit automatisiert werden müssen, sind im Abschnitt „Umsetzungsbeispiel“ aufgeführt.

Motivation: In modernen voll automatisierten Umgebungen wie Public Clouds (und CI/CD-Chains, die von DevOps/DevSecOps-Organisationen verwendet werden) behindern manuelle Prozesse nur den erwarteten schnellen Ablauf und können auch häufiger zu menschlichen/operativen Fehlern führen.

Umsetzungsbeispiel: Es ist notwendig, entscheidende Prozesse zu automatisieren:

- IAM-bezogene Aufgaben wie Konto-, Benutzer, Gruppen- und Richtlinienverwaltung.
- Sicherheitshärtung von Systemen (Security as Code)
- Sicherheitsscans und -tests in CI/CD-Chains
- Einhaltung- und Sicherheitsprüfungen von Cloud-Diensten und Systemen (einschließlich Überprüfung von Software/Paketen), die in der Cloud betrieben werden
- Schwachstellenerkennung (sowohl in der CI/CD-Chain als auch in Live-Umgebungen)
- Korrelation von Log-Daten und Erkennung von Angriffen
- Schlüssel-, Secrets- und Zertifikatsmanagement
- Erkennung und Alarmierung von Fehlkonfigurationen, die nicht durch Richtlinien erzwungen werden können
- Erstellung von Sicherheitsdokumenten für den PSA-Prozess

SaaS-Cloud-Dienste erfordern in der Regel weniger Konfiguration, d. h. sie haben weniger Konfigurationsoptionen. Obwohl bei einigen SaaS-Cloud-Diensten die Konfiguration nur über eine Webschnittstelle verfügbar ist, bei der überhaupt keine Automatisierung implementiert werden kann, bieten viele Anbieter von SaaS-Cloud-Diensten CLI- und/oder API-Zugriffe für die Konfiguration einiger Optionen an, z. B. die Verwaltung von Benutzern, Rollen und Berechtigungen, das Exportieren von Protokollen, das Verwalten von Kontingenten oder das Generieren (Erstellen) von Nutzungsberichten usw. Ein solcher CLI- und API-Zugriff kann für die Automatisierung der Sicherheitsaufgaben verwendet 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
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.66-10/5.0

Req 11 Es dürfen nur freigegebene Images verwendet werden.

Um mögliche Sicherheitsvorfälle zu vermeiden, wird empfohlen, die Landing Zone soweit zu beschränken, sodass nur die Verwendung von vorab abgenommenen Images (einschließlich, aber nicht beschränkt auf VM-Images und Container-Images) zugelassen ist. Je nach ausgewähltem Cloud-Anbieter können diese Images die Standard-Images des Anbieters sein, soweit diese die DTAG-Sicherheitsanforderungen für das jeweilige Betriebssystem und die Software erfüllen.

Falls die Einschränkung, nur abgenommen Images zu verwenden, in der Landing Zone nicht praktikabel oder in manchen Fällen nicht möglich ist, muss eine Überwachung der von den Benutzern hochgeladenen Images eingerichtet werden. Die Überwachung soll sicherstellen, dass nur geeignete und beabsichtigte Images verwendet werden.

Images, welche direkt vom Lieferanten geliefert werden, müssen generell wie üblich behandelt werden: Signaturen müssen überprüft und das Image muss auf bekannte Sicherheitslücken und -probleme überprüft werden.

Motivation: Dies verhindert, dass ein Angreifer, der sich Zugang zu den Cloud-Accounts (persönliche oder technische) verschafft hat, seine eigenen Images verwenden kann. Die Möglichkeiten eines Angriffs werden hierbei mehr eingeschränkt, sodass ein Missbrauch von Cloud-Ressourcen und weitere Angriffe auf andere Systeme, die in der Public Cloud gehostet werden, oder auf interne Systeme der DTAG im Allgemeinen schwerer durchzuführen sind.

Umsetzungsbeispiel: Die Magenta Trusted Registry (MTR) kann verwendet werden, um Containerimages nach Schwachstellen zu scannen: <https://yam-united.telekom.com/pages/digital-hub-ci-cd/apps/content/magenta-trusted-registry-mtr>.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.66-11/5.0

Req 12	Auf dem System darf ausschließlich nur benötigte Software eingesetzt werden.
--------	--

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

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

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

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

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.01-3/9.0

Req 13	Nicht benötigte Funktionen in der eingesetzten Software, einschließlich Anwendungsprogrammierschnittstellen (APIs) und Befehlszeilenschnittstellen (CLI), und Hardware müssen deaktiviert werden.
--------	---

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

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

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

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

Umsetzungsbeispiel: [Beispiel 1]

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

[Beispiel 2]

Deaktivierung von ungenutzten Netzwerk-Schnittstellen eines Servers.

ID: 3.66-13/5.0

Req 14	Virtuelle Maschinen und Container, die unveränderlich (immutable) sind (d. h. während ihrer Lebensdauer nicht verändert werden), dürfen für menschliche Benutzer nicht zugänglich sein, außer zur Fehlersuche.
--------	--

Das Konzept der Verwendung unveränderlicher virtueller Maschinen und Container wird als unveränderliche Infrastruktur bezeichnet. Jede virtuelle Maschine oder Container bleibt während ihrer Lebensdauer unverändert. Anstatt ein Live-System zu patchen oder neu zu konfigurieren, beruht der Ansatz auf der Erstellung neuer virtueller Maschinen oder Container und das Löschen der älteren Versionen.

Alle Produktionssysteme, die unveränderliche virtuelle Maschinen und Container verwenden, dürfen für menschliche Benutzer nicht zu Verwaltungszwecken zugänglich sein, es sei denn, dies ist zur Fehlersuche erforderlich und daher nur für einen bestimmten Zeitraum erlaubt (bedingter Zugriff).

Dieses Konzept ist typischerweise nicht vollständig auf Entwicklungs- und in einigen Fällen auf Testsysteme anwendbar.

Das Patchen von unveränderlichen Systemen muss durch erneute Bereitstellung erfolgen.

Motivation: Diese Praxis wird sehr häufig in Kombination mit CI/CD-Chains benutzt. In den Ketten werden automatisierte Tests und Deployments verwendet, um neue Funktionen zu testen, Images zu patchen und diese dann in Betrieb zu nehmen. Der Ansatz bringt zudem weitere folgende Vorteile mit sich:

- *Es ist kein Remote-Managementzugang mehr nötig*
- *Keine Notwendigkeit für komplexe und zeitaufwändige Patching-Verfahren*
- *Sowohl Funktions- als auch Sicherheitstests sind von Anfang an integriert*

Umsetzungsbeispiel: Erstellen eines neuen Images, einschließlich der erforderlichen Änderungen, und ersetzen der alten virtuellen Maschine/Container. Die alte virtuelle Maschine/Container muss gelöscht werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.66-14/5.0

Req 15	Software und Hardware des Systems müssen von einem Sicherheitsschwachstellen-Support seitens des Herstellers abgedeckt werden.
--------	--

In einem System dürfen nur Software- und Hardware-Produkte eingesetzt werden, für die ein Sicherheitsschwachstellen-Support vorhanden ist.

len-Support durch den Hersteller besteht.

Ein solcher Support muss umfassen, dass der Hersteller

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

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

Support-Phasen mit eingeschränktem Leistungsumfang

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

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

Open Source Software und Hardware

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

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

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.01-1/9.0

Req 16	Eingesetzte Software muss aus vertrauenswürdigen Quellen bezogen und auf Integrität geprüft werden.
--------	---

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

Diese Anforderung bezieht sich auf sämtliche Arten von Software:

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

sowie weitere Software, die ggf. zum Einsatz kommt.

Vertrauenswürdige Quellen

Als vertrauenswürdige Bezugsquellen gelten allgemein:

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

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

(2) Sichert der Bereitstellungs-Server die Transport-Schicht mittels kryptografischer Protokolle (z. B. HTTPS, sftp), müssen die zugehörig präsentierten Server-Zertifikate oder Server-Keys/Fingerprints bei jedem Download validiert werden, um die Identität des Bereitstellungs-Servers zu bestätigen; schlägt die Validierung fehl, ist der Download abubrechen und der Bereitstellungs-Server als nicht vertrauenswürdige Quelle zu bewerten.

Integritätsprüfung

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

Valide Mechanismen sind:

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

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

Erweiterte Integritätsprüfung bei Bezug von Software aus öffentlichen Registries

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

Beispiele für solche Registries sind:

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

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

Methoden für eine erweiterte Integritätsprüfung können beispielsweise sein:

- strikte Validierung der Projekt-/Paket-Namen (Vermeidung der Verwechslung mit maliziösen, gezielt nachgeahmten Software-Projekten)
- dynamische Code Analyse / strukturierte Funktionsprüfung in einer Test-Umgebung
- statische Code Analyse mittels eines Linters (z. B. Splint, JSLint, Pylint)
- Untersuchung mittels eines Sicherheitsschwachstellen-Scanners (z. B. Qualys, Nessus)

- Untersuchung mittels eines Container Security Scanners (z. B. JFrog Xray, Harbor, Clair, Docker Scan)
- Untersuchung mittels eines SCA (Software Composition Analysis) Tools bzw. Dependency-Scanners (z. B. OWASP Dependency Check, Snyk)

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

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

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

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

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.01-2/9.0

Req 17 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 unabhängi-

ger 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 18 Systeme müssen in das Compliance-/Sicherheits-Tool des Unternehmens aufgenommen werden.

Das System (als Gesamtsystem - nicht nur virtuelle Maschinen und Container, sondern auch Images, Storage-Buckets, serverless Funktionen usw.) muss in die Compliance-/Sicherheits-Tools des Unternehmens mit aufgenommen werden. Hierbei ist es unabhängig davon, ob sie als unveränderliche Systeme oder auf eine traditionellere Weise eingesetzt werden.

Für ein System, das nicht direkt in das/die Compliance-/Sicherheitstool(s) des Unternehmens integriert werden kann, muss ein geeigneter Prozess vorhanden sein, der die tägliche Überprüfung des Patch-Levels und den Vergleich mit bekannten Schwachstellen ermöglicht.

Ein regelmäßiges Monitoring der Meldungen des Telekom Security CERTs ist notwendig, falls das firmeneigene Compliance/Security-Tool keine zutreffenden Informationen für das jeweilige System liefern kann.

Im Falle eines Systems, für das das Anforderungsdokument 3.63 „Betrieb in der DT IT“ gilt, sind die Anforderungen 10 und 11 aus 3.63 als spezifische Anforderungen zu beachten.

Motivation: Ein System, das in das Compliance-Tool integriert ist, ermöglicht eine schnellere Erkennung von Schwachstellen und erleichtert die rechtzeitige Behebung von Schwachstellen.

Umsetzungsbeispiel: Von der Telekom Security wird hierbei das Tool TASTE-OS (OS = Offline-Scanner) bereitgestellt. Bei TASTE-OS müssen entsprechende Skripte in CI/CD-Build-Chain und in den Produktionssystemen eingebunden werden. Es ist unabhängig davon, ob diese als unveränderliche Systeme oder auf herkömmliche Weise deployt werden. Eine Liste aller TOS-Instanzen sind unter folgendem Link zu finden: <https://yam-united.telekom.com/pages/taste-os-anwender/apps/wiki/dokumentation/list/view/8a2d0018-3bfb-4933-9289-61a022ceb5d3>.

Wenn der Cloud-Anbieter Überprüfungen der Datenschutz- und Sicherheitslage für die eigenen Dienste anbietet, sollten diese zusätzlich zu bestehenden Compliance-Tools der DTAG genutzt und die Empfehlungen befolgt werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.66-18/5.0

Req 19	Sofern der CSP dies zulässt müssen Intrusion-Detection- und Intrusion-Protection-Systeme für alle in der Public Cloud gehosteten Workloads und Daten, die hinreichend sensibel sind und einen solchen Schutz erfordern, auf virtuellen Maschinen in der Cloud installiert werden.
--------	---

Intrusion-Detection-Systeme (IDS) und Intrusion-Prevention-Systeme (IPS) können die Sicherheit von virtuellen Maschinen in der Public Cloud verbessern, obwohl ihr Einsatz im Allgemeinen nicht zwingend erforderlich ist. Abhängig von der Systemklassifizierung, der Sensibilität der Daten und den potenziellen Bedrohungen kann es jedoch erforderlich sein, zusätzliche IDS oder IPS für bestimmte Workloads zu verwenden. Die meisten Anbieter von öffentlichen Cloud-Diensten erlauben in der Regel den Betrieb solcher Systeme. Es ist aber notwendig, dies für jeden einzelnen Anwendungsfall zu überprüfen.

Obligatorische Zugriffskontrollen (wie AppArmor oder SELinux, welche als grundlegende IDS/IPS betrachtet werden können) müssen in der üblichen Weise verwendet werden, die durch andere gültige Sicherheitsanforderungen für Betriebssysteme und Anwendungen definiert ist.

Motivation: IDS/IPS-Systeme können ungewöhnliches Systemverhalten erkennen und können auch bei Zero-Day-Angriffen sehr nützlich sein.

Umsetzungsbeispiel: Mindestens AppArmor oder SELinux sollten verwendet werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.66-19/5.0

Req 20	Ein Konfigurations-Repository muss als Single Source of Truth für alle Konfigurationsdateien und Infrastructure-as-Code-Skripte (IaC) verwendet werden, die die Cloud-Ressourcen definieren, und ein solches Konfigurations-Repository darf nicht in derselben Cloud gehostet werden.
--------	---

Die Einrichtung eines Konfigurations-Repositorys als Single Source of Truth für alle Konfigurationsdateien und Infrastructure-as-Code-Skripte (IaC) ist unerlässlich, um eine effiziente, organisierte und zuverlässige Verwaltung von Cloud-Ressourcen zu gewährleisten. Durch ein dediziertes Repository mit Versionskontrolle können Teams Änderungen einfach nachverfolgen, die Konsistenz aufrechterhalten, die Zusammenarbeit verbessern und die Notfallwiederherstellung unterstützen, was zu einem optimierten und transparenten Verwaltungsprozess der Cloud-Infrastruktur beiträgt.

Das Repository muss mit geeigneten Zugriffskontrollen geschützt werden, um das "Need-to-know"- und Least-Privilege-Prinzip durchzusetzen, das nur autorisiertem Personal den Zugriff auf bestimmte Konfigurationen und die Bereitstellung in der Cloud ermöglicht.

Während einige SaaS-Cloud-Dienstanbieter die Konfiguration nur über eine Webschnittstelle verfügbar haben, bei der überhaupt keine Automatisierung implementiert werden kann, bieten viele SaaS-Cloud-Dienstanbieter CLI- und/oder API-Zugriffe für die Konfiguration an. Ein solcher CLI- und API-Zugriff kann für die Konfiguration verwendet werden.

Das Konfigurations-Repository, das zur Steuerung der Konfiguration der Cloud verwendet wird, muss außerhalb der Cloud platziert werden, die gesteuert wird, damit es möglich ist, die Cloud-Umgebung mithilfe eines solchen Konfigurations-Repositorys wiederherzustellen.

Motivation: Ein dediziertes Konfigurations-Repository zu haben, hilft bei der Reduzierung von Konfigurationsfehlern, der Optimierung von Konfigurationsmanagementprozessen, der Verbesserung der Sicherheit durch die Durchsetzung standardisierter Konfigurationen und der Vereinfachung von Fehlerbehebungs- und Überwachungsaktivitäten.

Das Hosten eines Konfigurations-Repositorys der Cloud-Umgebung in derselben Cloud-Umgebung kann zu einer Situation führen, in der eine Cloud-Umgebung nicht repariert werden kann, da das Konfigurations-Repository nicht verfügbar oder nicht erreichbar ist, und das Konfigurations-Repository nur verfügbar gemacht werden kann, wenn die Cloud-Umgebung repariert wird.

Umsetzungsbeispiel: Die Infrastruktur als Code-Repository der AWS-Landingzone kann weder in der AWS-

Landingzone noch in einem CI/CD-System gespeichert werden, das in derselben AWS-Landingzone gehostet wird. Ein solches Repository sollte vielmehr in den Räumlichkeiten der DTAG gehostet werden. Oder in einigen speziellen Fällen muss ein solches Repository einen voll funktionsfähigen Mirror außerhalb der Umgebung haben, die es definiert.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.66-20/5.0

Req 21	Tags mit geeigneten und aussagekräftigen Metadaten müssen auf alle Cloud-Ressourcen (virtuelle Maschinen, Storage Buckets, Datenbanken, Netzwerkkomponenten usw.), die Tags unterstützen, angewendet werden.
--------	--

Tagging ist eine wesentliche Funktion, die in Cloud-Umgebungen implementiert werden muss, um Ressourcen innerhalb einer Organisation zu organisieren und Komplexität und Verwaltungsaufwand zu reduzieren. Durch die Durchsetzung einer Tagging-Richtlinie kann die Konsistenz, Genauigkeit und Standardisierung aller Ressourcen in einer Cloud-Umgebung sichergestellt werden, was eine bessere Ressourcenverfolgung und -verwaltung ermöglicht.

Einige SaaS-Cloud-Dienste bieten Tagging an, insbesondere solche, die verschiedene Arten von Daten wie Cloud-Speicher oder Cloud-Backup verarbeiten. Tags können hier verwendet werden, um die Datenklassifizierung und das Eigentum darzustellen.

Motivation: "Tags" ermöglichen die Kategorisierung von Ressourcen mit eigenen Metadaten. Dies kann nützlich sein, um z. B. Sicherheitskonfigurationen auf automatisierte Weise zu implementieren und Daten zu klassifizieren.

Umsetzungsbeispiel: Die Vorgaben, welche Tags zu verwenden sind, wird durch die Landing Zone definiert. Zusätzliche Tags können durch Anwendungen selbst definiert 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
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.66-21/5.0

Req 22	Berechtigungen und Kontrollen, die als Landezone implementiert sind, müssen vor der Verwendung und nach wesentlichen Änderungen geprüft werden.
--------	---

Die Überprüfung der Korrektheit der als Landing Zone implementierten Controls ist vor dem Einsatz und bei jeder wesentlichen Änderung der Landing Zone (z. B. komplette Neudefinition von Rollen) zwingend erforderlich. Dies gilt mindestens für die Haupt-Landing Zone und für die Teile der Landing Zone, die abweichende (übergeordnete) Richtlinien im Vergleich zur Haupt-Landing Zone haben. Die Sicherheitsberatung muss kontaktiert und die Anwendung der Änderungen mit ihr abgestimmt werden.

Der Einsatz von automatisierten Tools für Penetrationstests und CIS-Benchmarks kann schnell sehr teuer werden. Daher ist es sehr wichtig, den Umfang der Tests und Scans entsprechend den Anforderungen festzulegen.

Motivation: Jede Änderung der Konfiguration und der Kontrollen (insbesondere Richtlinien in Bezug auf die Cloud-Landing Zone) kann zu neuen Sicherheitslücken führen.

Umsetzungsbeispiel: Die folgenden Tools und Methoden können zur Durchführung der Überprüfung verwendet werden:

- automatisierte Penetrationstest-Tools (häufigstes Beispiel sind Privilegieneskalationen)
- benutzerdefinierte (manuelle) Penetrationstests - erfordern in der Regel einen kreativen Ansatz
- CIS-Benchmarks (<https://www.cisecurity.org/>) und ähnliche automatisierte Überprüfungs-/Berichtstools

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: 3.66-22/5.0

Req 23 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

4.1. Schutz von Sitzungen

Der Sitzungsschutz ist unerlässlich, um unbefugten Zugriff und Session-Hijacking zu verhindern und die Vertraulichkeit von Daten für Benutzerinteraktionen mit Webdiensten zu wahren. Im Cloud-Umfeld ist vor allem das Webportal der Cloud der Ort, um den Sitzungsschutz zu überprüfen.

Req 24 Sitzungen müssen gegen eine unautorisierte Übernahme ("Session Hijacking") geschützt werden.

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

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

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

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

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.01-16/9.0

Req 25 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 26	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 legitimierter 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

5. Authentifizierung und Autorisierung

Um zugelassene CSP durch einen ordnungsgemäßen Vertrag nutzen zu können, ist es notwendig, eine "Landing Zone" für jeden CSP zu erstellen. Landing Zone ist ein Konzept, das eine zentrale Verwaltung von Identitäten und Projekten innerhalb des CSP für die gesamte DTAG-Gruppe.

Die Landing Zone beginnt mit einem "Root-Konto" für die gesamte DTAG, das von einem Team verwaltet wird, welches für die Verwaltung der CSP-Nutzung zuständig ist (Cloud-Management-Team im weiteren Verlauf des Kapitels). Der Begriff "Root-Konto" ist in bestimmten SaaS-Cloud-Diensten auch einfach als Administrator bekannt. Das Cloud-Management-Team verwaltet eine Reihe von grundlegenden (Sicherheits-) Richtlinien, Benutzern und Projekten. Jedes Projekt/System/Abteilung/Organisation würde über die Landing Zone Zugang zum CSP erhalten und kann Cloud-Dienste mit vordefinierten Kontingentgrenzen und innerhalb grundlegender Sicherheitsrichtlinien nutzen. Jede Organisation hat die Freiheit, ihren Anteil unter den gegebenen anfänglichen Beschränkungen anzupassen. Jedes Projekt unter jeder Organisation kann weitere Anpassungen vornehmen.

Die Landing Zone ist die Voraussetzung für eine vollständige und umfassende Sicherheitsüberwachung und Abrechnung.

Req 27	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 28	Benutzerkonten müssen mit mindestens zwei Authentisierungsmerkmalen aus unterschiedlichen Faktoren geschützt werden.
--------	--

Sämtliche Benutzerkonten des Systems müssen vor einer unberechtigten Nutzung geschützt werden.

Dies ist durch Verwendung von Authentisierungsmerkmalen umzusetzen, die eine eindeutige Identifizierung des legitimen Benutzers ermöglichen.

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

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

Es müssen mindestens zwei Authentisierungsmerkmale miteinander kombiniert werden.

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

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

Beispiele für zulässige Authentisierungsmerkmale

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

*) Wichtiger Hinweis zum Einsatz von Passwörtern

Passwörter müssen als Authentisierungsmerkmal strikt vermieden werden.

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

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

Dazu gehören:

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

Hinweis zu technischen Benutzerkonten

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

Personen sollen den nicht-interaktiven Zugang nicht direkt nutzen (wie den API-Zugang), sondern technische Benutzer(unter)konten, die ihnen gehören. Technische Benutzerkonten werden später in diesem Dokument behandelt.

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"

ID: 3.66-28/5.0

Req 29 Privilegierte Benutzerkonten müssen mit mindestens zwei Authentisierungsmerkmalen geschützt werden, die aus unterschiedlichen Faktoren stammen und erhöhte Resilienz gegen Phishing-Angriffe bieten.

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

Beispiele für privilegierte Benutzerkonten:

- Konten für Administrations-, Wartungs- oder Entstörungsaufgaben
- Konten für Benutzer-Verwaltungsaufgaben (z. B. Anlegen/Löschen von Benutzern; Zuweisen von Berechtigungen; Passwort-Rücksetzungen)
- Konten, die zur Freigabe, Auslösung oder Unterbindung von geschäftskritischen Vorgängen berechtigt sind
- Konten mit Zugriff auf Daten, die im Interesse des DTAG-Konzerns, dessen Kunden oder der Öffentlichkeit als SCD (Sensitive Customer Data) eingestuft sind
- Konten, die in hohem Umfang auf lt. EU-DSGVO als „personenbezogen“ definierte Daten zugreifen können (z.

B. Massenabruf von größeren Teilen oder des vollständigen Datenbestands)

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

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

Eine Kombination von Authentisierungsmerkmalen desselben Faktors ist nicht zulässig.

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

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

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

Als nicht anfällig gegenüber Phishing-Angriffen gelten

- FIDO2 Level 2 Security Keys
- in Hardware implementierte Zertifikate

Wichtiger Hinweis zum Einsatz von Passwörtern

Passwörter müssen als Authentisierungsmerkmal strikt vermieden werden.

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

Hinweis zu technischen Benutzerkonten

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

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

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

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

FIDO2 Level 2 Security Key plus PIN-Eingabe	1. Faktor: in Hardware gespeicherter Crypto-Schlüssel ("Besitz") 2. Faktor: PIN ("Wissen")	(keine)
--	--	---------

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.01-21/9.0

Req 30 Standard-(Root-)Konto(s) müssen als privilegierte Benutzerkonten behandelt werden, und wenn möglich, muss das Vier-Augen-Prinzip befolgt werden.

Das Root-Konto für die gesamte DTAG innerhalb des CSP wird mit allen verfügbaren Berechtigungen erstellt. Ein solches Konto ist ein Sicherheitsrisiko und darf nicht für den täglichen Betrieb verwendet werden. Für den täglichen Betrieb müssen andere Konten mit extrem eingeschränkten Rechten verwendet werden. In einigen seltenen Fällen ist es jedoch notwendig, Aufgaben mit dem Root-Konto auszuführen, und Daher muss dieses Konto wie ein privilegiertes Benutzerkonto behandelt und entsprechend behandelt werden (z. B. MFA, erhöhte Widerstandsfähigkeit gegen Phishing-Angriffe usw.).

Es ist eine sehr gute Praxis, zu überwachen, ob die E-Mail-Adresse (im Allgemeinen die Kontokennung) für den Fall von Sicherheitsverletzungen beim CSP verwendet wird.

Alle oben genannten Anmeldeinformationen und Geräte für solche Root-Konten müssen an einem sicheren Ort, z. B. in einem physischen Safe, aufbewahrt werden. Es wird empfohlen sie an 2 Orten aufzubewahren (z. B. Passwort + Token an einem Ort, Wiederherstellungsgeheimnisse an einem anderen Ort) zur Redundanz, da Erdbeben, Brände und Überschwemmungen immer noch vorkommen.

Jede Aktion des Standard-/Rootkontos/der Standard-/Rootkonten ("Superadmins") muss zu Revisionszwecken vollständig protokolliert werden. Es ist ratsam, auch eine Benachrichtigung aller Personen einzurichten, die an der Top-Level-Cloud-Administration beteiligt sind (z. B. per E-Mail), wenn ein Login oder eine Änderung an einem solchen Konto vorgenommen werden.

Diese Anforderung steht im Einklang mit Anforderung 16 aus 3.63 ("Betrieb in DT IT") für die Systeme, für die 3.63 gilt. Es ist jedoch zu beachten, dass die Passwortlänge/-komplexität aus dieser Anforderung die Anforderung 16 aus 3.63 überschreibt.

Motivation: Reduzierung der Angriffsfläche.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System

ID: 3.66-30/5.0

Req 31 Technische Benutzerkonten müssen geeignete Authentifizierungs Mechanismen (kurzlebige Token oder Zugriffsschlüssel anstelle von MFA) verwenden.

Technische Benutzerkonten sind für die Automatisierung notwendig und können keine typischen MFA verwenden, die für Personen obligatorisch sind. Glücklicherweise gibt es andere Optionen, die für automatisierte M2M-Kommunikationsszenarien verwendet werden können. Eine dieser Optionen ist die Verwendung von Token, Zugriffsschlüsseln und Zertifikaten (im Folgenden wird nur der Begriff Token verwendet), die einen sehr begrenzten Umfang, Berechtigungen und Lebensdauer haben. Je nach gewähltem CSP können die Optionen variieren, aber die folgenden Einschränkungen müssen, wann immer möglich, angewendet werden:

- Technische Benutzerkonten oder deren Zugriffsschlüssel/Token dürfen nicht von Personen verwendet werden

den

- Token für technische Benutzerkonten müssen eine begrenzte Lebensdauer haben und periodisch ausgetauscht werden.
 - Wenn es keine Möglichkeit gibt, die anfängliche Lebensdauer eines Tokens festzulegen, muss es einen etablierten Prozess für die Rotation von älteren Token geben.
 - Der Prozess für die Rotation von Token muss einen reibungslosen Übergang vom alten zum neuen Token berücksichtigen.
 - Die Lebensdauer von Token muss angemessen überwacht werden, um Ausfallzeiten durch abgelaufene Token zu vermeiden.
 - Gestohlene oder veröffentlichte Token müssen sofort widerrufen/gelöscht werden.

Motivation: Kurzlebige Anmeldeinformationen tragen dazu bei, die Auswirkungen potenzieller Sicherheitsverletzungen zu minimieren, die Offenlegung schutzbedürftige Informationen zu begrenzen und eine proaktive Sicherheitslage aufrechtzuerhalten.

Umsetzungsbeispiel: Verwenden Sie OpenID Connect mit GitLab, um temporäre Anmeldeinformationen für technische Benutzerkonten für den CSP zu erhalten.

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: 3.66-31/5.0

Req 32	Das Geheimnis (Schlüssel, Token, Zertifikat) muss häufig rotieren. Geheimnisschutzmechanismen, die dem Stand der Technik entsprechen, müssen verwendet werden.
--------	--

Geheimnisse, die in einer Cloud verwendet werden, sind einem höheren Risiko ausgesetzt, gestohlen zu werden oder durchzusickern. Um die Auswirkungen gestohlener Geheimnisse zu minimieren, müssen sie im Vergleich zu herkömmlichen Implementierungen mit einer kürzeren Lebensdauer erzeugt werden. Es ist praktisch unmöglich, eine bestimmte Lebensdauer von Geheimnissen für jede mögliche System- und Datenklasse vorzugeben, daher wird die endgültige Entscheidung dem Einvernehmen zwischen dem Eigentümer der Anwendung und dem zuständigen Sicherheitsbeauftragten überlassen. Die derzeit gültigen Sicherheitsanforderungen für Geheimnisse sind im PSA-Dokument 3.50 "Kryptographische Algorithmen und Sicherheitsprotokolle" enthalten. Zum jetzigen Zeitpunkt ist eine Rotation der Geheimnisse alle 24 Monate oder bei Anzeichen einer Kompromittierung erforderlich. Die Rotation von Geheimnissen muss so implementiert werden, dass ein reibungsloser Übergang möglich ist, d. h. ohne Dienstunterbrechung.

Die Geheimnisse werden in der Public-Cloud-Umgebung selbst verwendet, daher ist es notwendig, modernste Mechanismen zum Schutz der Geheimnisse einzusetzen. Ein solches Beispiel ist der Schutz von privaten Schlüsseln, die im RAM ruhen, welche gegen Spekulations- und Speicherkanal-Angriffe wie Spectre, Meltdown, Rowhammer und RAM-Bleed geschützt werden müssen. Weitere Informationen über diesen speziellen Schutzmechanismus finden Sie unter: <https://marc.info/?l=openbsd-cvs&m=156109087822676&w=2>.

Beispiele:

- Beispiel für die Dauer von HTTPS-Zertifikaten, die auf Front-End-Webservern oder Proxies installiert sind: Die Gültigkeit eines Zertifikats für mehr als 1 Jahr könnte zu hoch sein. 3 Monate wären wahrscheinlich eine bessere Wahl.
- Die Gültigkeitsdauer eines privaten/öffentlichen Schlüsselpaars bei asymmetrischer Verschlüsselung (RSA-Schlüsselpaare für SSH) von mehr als 2 Jahren ist möglicherweise nicht die beste Idee (und die Rotation ist obligatorisch), selbst wenn die SSH-Software einen Schutz der privaten Schlüssel im RAM bietet.
- Einige weitere typische Beispiele finden Sie unter <https://www.keylength.com/>.

Diese Anforderung steht im Einklang mit Anforderung 16 aus 3.63. ("Betrieb in DT IT") für die Systeme, für die 3.63. gilt.

Motivation: Regelmäßig rotierende Geheimnisse tragen dazu bei, die Auswirkungen potenzieller Sicherheitsverletzungen zu minimieren, die Offenlegung schutzbedürftiger Informationen zu begrenzen und eine proaktive Sicherheitslage aufrechtzuerhalten. Sicherheitsverletzungen sind in den meisten Fällen offengelegte Geheimnisse durch direkte Verwendung im Quellcode, der für Unbefugte über ein codeübergreifendes Repository (GitLab, Github usw.) sichtbar ist, oder die Verbreitung der Schlüssel durch andere unbeabsichtigte Aktionen.

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: 3.66-32/5.0

Req 33 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.

Im Kontext der Cloud bedeutet das:

Auch in der Cloud kann die Erstellung oder Initiierung eines neuen Dienstes ein standardmäßiges/vordefiniertes Authentifizierungsattribut enthalten, z. B. ein Standardkennwort für einen Dienstbenutzer. Wie oben erwähnt, müssen diese Attribute nach der Bereitstellung des Dienstes in der Cloud in einen neuen individuellen Wert geändert werden.

Administratoren oder Nutzer von Cloud-Diensten, insbesondere SaaS, können das initiale Passwort per E-Mail erhalten und sind in diesem Fall verpflichtet, das Passwort nach dem ersten Login zu ändern.

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).

ID: 3.66-33/5.0

Req 34 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 35	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 zugreifen 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 36	Technische Benutzerkonten müssen begrenzte Berechtigungen besitzen. Der API-Zugriff für technische Benutzerkonten muss auf das notwendige Minimum beschränkt sein.
--------	--

Berechtigungen für technische Benutzerkonten müssen so weit eingeschränkt werden, dass technische Benutzerkonten nur auf Daten zugreifen und Funktionen nutzen, die im Rahmen ihrer Arbeit notwendig sind. Das ist sehr wichtig, denn technische Benutzerkonten können die typische MFA nicht als zusätzlichen Sicherheitsmechanismus verwenden, der ihnen einen zusätzlichen Schutz bieten würde.

Je nach ausgewähltem CSP können die Optionen variieren, aber die folgenden Einschränkungen müssen nach Möglichkeit angewendet werden:

- Technische Benutzerkonten dürfen nicht mehr als das absolute Minimum an Rechten haben, die für die von ihnen ausgeführten Aufgaben erforderlich sind
 - Obwohl dies eine gültige Anforderung für alle Benutzerkonten ist, werden technische Benutzerkonten typischerweise von Automatisierungswerkzeugen verwendet, die über vordefinierte API-Aufrufe verfügen und daher nicht mehr Rechte benötigen, als für die nötigen API-Aufrufe.
- Technische Benutzerkonten müssen einen begrenzten Umfang für den Ressourcenzugriff haben (nur eine Teilmenge der Ressourcen)
- Technische Benutzerkonten oder deren Zugriffsschlüssel/Token dürfen nicht von Personen verwendet werden
- Token für technische Benutzerkonten müssen eine begrenzte Lebensdauer haben und periodisch ausgetauscht werden.
- Der Zugriff auf die APIs des CSP muss in Bezug auf die Erreichbarkeit des Netzes eingeschränkt werden.
 - Die APIs des CSP sind über das Internet verfügbar, jedoch ist es in einigen Fällen möglich, den Netzzugang für technische Benutzerkonten auf APIs zu beschränken, so dass Verbindungen nur von bestimmten IP-Adressbereichen oder Standorten möglich sind.

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

Umsetzungsbeispiel:

- Wenn das technische Benutzerkonto den Objektspeicher nur lesen muss, darf es keine Berechtigung zum Ändern, Schreiben oder Löschen von Berechtigungen für den Objektspeicher haben.
- Wenn das technische Benutzerkonto für die Speicherung von Protokollen im Objektspeicher verwendet wird, muss es über entsprechende Erstellungs-/Schreibberechtigungen verfügen, aber darf keine Berechtigungen zum Lesen, Ändern oder Löschen von Objekten haben.
- Wenn das technische Benutzerkonto für die Bereitstellung virtueller Maschinen verwendet wird, darf es nicht über Privilegien für die Änderung von Sicherheitsgruppen haben.
- Wenn das technische Benutzerkonto für die Verwaltung nur einer Teilmenge von virtuellen Maschinen (z. B. VMs mit einem bestimmten Tag) verwendet wird, darf es nicht die Möglichkeit haben, andere virtuelle Maschinen (VMs mit anderen Tags) zu verwalten.
- Wenn das technische Benutzerkonto auf die APIs des CSP von internen Netzen aus zugreift (z. B. von VMs innerhalb der Cloud) und nicht über das Internet, muss der Internetzugriff für dieses technische Benutzerkonto entfernt werden, sofern der CSP diese Einschränkung anbietet.

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

Req 37	Alle Accounts müssen dem Root-Account einer freigegebenen Landingzone untergeordnet sein. Es dürfen keine neuen Root-Accounts erstellt werden.
--------	--

Wie bereits erwähnt, ist die Verwendung von CSP nur über die richtige Landing Zone erlaubt, und da die Landing Zone durch das anfängliche Standard-Root-Konto erstellt wird, müssen alle nachfolgend erstellten Benutzer auch zu diesem Hauptkonto gehören.

Das Erstellen eines anderen persönlichen oder geschäftlichen Root-Kontos auf diesem CSP würde die Etablierung einer zusätzlichen Landing Zone für diesen Benutzer bedeuten, was die Umgehung der für die zuvor beschriebene Landing Zone festgelegten Sicherheitsrichtlinien ermöglichen würde und daher verboten ist.

Beispiel:

Mein Projekt ist speziell, und ich muss X verwenden und wir müssen ein separates Root-Konto haben.

- Eine neue BoM-Entscheidung ist notwendig.

Motivation: Durch das Erstellen eines weiteren persönlichen oder geschäftlichen Stammkontos auf diesem CSP wird eine neue Zielzone für diesen Benutzer erstellt, wodurch Sicherheitsrichtlinien umgangen werden können, die für die zuvor beschriebene Zielzone festgelegt wurden, und daher verboten ist.

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

Req 38	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.

Im Kontext der Cloud bedeutet das: Für die Nutzung eines Dienstes von einem CSP wird je nach CSP und Dienst ein dienstspezifisches Konto/Account oder die Nutzung eines bestimmten Satzes von Berechtigungen benötigt. Diese Dienstkonten oder Berechtigungen entsprechen meist nicht dem Least-Privilege-Prinzip und müssen durch dienstspezifische Konten oder Berechtigungssätze ersetzt werden. Daraus folgt, dass diese Dienstkonten und Berechtigungen gelöscht werden müssen oder, wenn dies nicht möglich ist, sichergestellt werden muss, dass sie deaktiviert sind (niemand kann das Dienstkonto oder die Berechtigungen verwenden).

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.

ID: 3.66-38/5.0

Req 39	Die IAM-Lösung der DTAG muss für die Benutzerauthentifizierung verwendet werden, wenn sie vom CSP unterstützt wird. Wenn nicht, muss eine Automatisierung für die Verwaltung von Identitäten in der Cloud vorhanden sein.
--------	---

Die doppelte Verwaltung von Benutzern bringt Probleme mit sich, wie z. B. die nicht rechtzeitige Erstellung und Löschung von Konten (was zu Datenleaks führen kann), daher ist es notwendig, dass Konten in der Cloud auf Konten im IAM der eigenen DTAG abgebildet werden. In Bezug auf die Techniken: Entra ID (früher bekannt als AAD oder Azure Active Directory), SAML 2.0, OpenID+OAuth (2.0) und LDAPS (nur innerhalb einer VPN-Verbindung) sind praktikable Optionen.

Für den unwahrscheinlichen Fall, dass sich die DTAG-eigene IAM-Lösung für die Verwaltung von Identitäten in der Cloud nicht integrieren lässt, ist es notwendig die Kontoverwaltung zu automatisieren. Eine solche Automatisierung zur Verwaltung von Identitäten muss das "IAM (Identity Access Management) - Framework" (3.69.) erfüllen.

Die bevorzugte Lösung wäre sitzungsbasiert, da keine persönlichen Daten der Mitarbeiter mit dem Cloud-Anbieter ausgetauscht werden.

Es ist erwähnenswert, dass diese Anforderung auch für Anwendungen gilt, die in der Cloud laufen, aber das ist bereits mit anderen Sicherheitsanforderungen (für Betriebssysteme und Anwendungen) abgedeckt.

Beispiel:

- Der Mitarbeiter hat die DTAG verlassen und sein Konto in der Cloud muss gelöscht werden, damit er nicht mehr auf die Cloud-Ressourcen zugreifen kann.

Im Falle eines Systems, in dem 3.63. ("Betrieb in DT IT") gilt, gilt die Anforderung 7 aus 3.63. als speziellere Anforderung.

Motivation: Die Verwendung von zwei oder mehr IAM-Systemen für eine Lösung führt zu einer hohen Komplexität, erhöht das Risiko von Inkonsistenzen und Sicherheitslücken im Vergleich zu einem IAM-System.

Umsetzungsbeispiel: Weitere Informationen unter den folgenden Links:

- Onboarding Guide telekom.de Entra ID – Tenant:<https://wiki.telekom.de/pages/viewpage.action?pageId=1563181642>
- Information Collaboration Network:<https://yam-united.telekom.com/pages/a66ec908-117c-4fa8-94f3-502795da60c5/apps/wiki/abd69725-2c88-4187-8499-9ed6847cd0f8/list/view/5a395001-6a94-43ca-8770-68e920222a52>

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.66-39/5.0

Req 40	Privilegien für die Cloud-Nutzung dürfen nicht direkt mit Benutzern oder Diensten verknüpft werden.
--------	---

Die Terminologie kann zwischen den CSPs variieren, daher wurde hier die gängigste verwendet.

Privilegien für die Nutzung von Cloud-Diensten müssen Rollen zugewiesen werden und niemals einzelnen Benutzern.

Benutzer müssen in Gruppen organisiert werden und diese Gruppennamen müssen ihre Bedeutung klar erkennen lassen (z. B. Administratoren, Betreiber, Reporter). Mehrere Benutzer können sich dieselbe Gruppe teilen.

Gruppen (oder Policies) ermöglichen die Zuordnung zwischen Benutzern und Rollen ("set of privileges"). In einigen Fällen erlaubt dies Benutzern, die mehrere Rollen haben, eine passende Rolle (die alle notwendigen Privilegien erhält) für die Arbeit auszuwählen.

Dieses Konzept vereinfacht die Zuweisung und das Entfernen von Privilegien für bestimmte Benutzer und ermöglicht eine bessere Kontrolle über die Privilegien, und erlaubt es sogar, dass Benutzer von einem Verantwortungsbereich in einen anderen wechseln (z. B. Entwickler -> Betrieb).

Motivation: Das Zuweisen von Berechtigungen zu Rollen oder Gruppen bietet Vorteile wie vereinfachte Verwaltung, Konsistenz, granulare Kontrolle, verbesserte Sicherheit, Skalierbarkeit und verbesserte Überprüfbarkeit, was es zu einer Best Practice für die Verwaltung von Zugriffskontrollen in Cloud-Umgebungen macht.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.66-40/5.0

Req 41	Für administrative Aufgaben muss eine Privileged Access Workstations (PAW) verwendet werden.
--------	--

Eine Privileged Access Workstation (PAW) ist ein isoliertes Betriebssystem (Hardware/virtualisiert), das für den sicheren Zugriff auf privilegierte Konten und Ressourcen verwendet wird.

Bei der Durchführung administrativer Aufgaben in einer öffentlichen Cloud muss eine PAW verwendet werden.

PAWs verbieten normalerweise die Verwendung riskanter Anwendungen wie z. B. Webbrowser und E-Mail-Clients. Die Idee hinter einem PAW besteht darin, alltägliche Aktivitäten wie z. B. das Beantworten von E-Mails von administrativen Aufgaben zu trennen.

Motivation: PAWs bieten erweiterte Sicherheit (aufgrund der Verwendung vertrauenswürdiger Hardware und gehärteter dedizierter Systeme) für Administratoren, die mit Hochrisikoressourcen arbeiten und deshalb anfällig für Kompromittierungen sind.

Umsetzungsbeispiel: Das Nutzen einer PAW-Lösung für administrative Aufgaben.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.66-41/5.0

6. Authentisierungsmerkmal "Passwort"

Req 42	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 43	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 44	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 45	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 46	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 47	Falls Passwörter als Authentisierungsmerkmal genutzt werden, muss eine Änderung des eigenen Passwortes jederzeit durch den Benutzer möglich sein.
--------	---

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

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

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

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.01-29/9.0

Req 48	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 49	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

7. Schutz von Daten und Informationen

Req 50	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 51 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 52	Es muss ein Key Management System zur sicheren Speicherung der Verschlüsselungsschlüssel verwendet werden. Bei vertraulichen Daten muss das Schlüsselverwaltungssystem unter der vollen Kontrolle der DTAG stehen.
--------	--

Ein Angreifer, der es schafft, die Daten aus der Cloud zu erhalten, wird es höchstwahrscheinlich mit verschlüsselten Daten zu tun haben, aber die Daten wären ohne Verschlüsselungsschlüssel (oder ausreichend fortgeschrittene Quantencomputer) nutzlos. Daher ist es wichtig, alle Verschlüsselungsschlüssel in einem entsprechend sicheren Schlüsselverwaltungssystem (KMS) zu speichern. Der Begriff "encryption Key" bezieht sich hier auf den Schlüssel, der für die symmetrische Verschlüsselung verwendet wird (wobei der encryption Key mit dem Entschlüsselungsschlüssel identisch ist, was der häufigste Anwendungsfall für die Datenspeicherung in der Cloud ist), oder auf den privaten Schlüssel aus dem öffentlich-privaten Schlüsselpaar im Falle der asymmetrischen Verschlüsselung; oder anders gesagt - es geht um den Schutz des Schlüssels, der es einem Angreifer ermöglichen würde, verschlüsselte Daten in Klartext umzuwandeln.

KMS kann es in verschiedenen Varianten geben:

- unter voller Kontrolle des CSP (meist transparent für Kunden)
- vom CSP bereitgestellt, aber Schlüssel vom Kunden verwaltet
- DTAG-eigenes KMS, kolloziert beim CSP
- DTAG-eigenes KMS

Für offene und interne Daten ist die Nutzung des vom CSP bereitgestellten KMS grundsätzlich erlaubt. Die letzte Lösung (eigenes KMS der DTAG) ist die einzige akzeptable Lösung und für vertrauliche Daten erlaubt, da sie die Daten auch vor einem unseriösen Cloud-Anbieter oder Geheimdienste schützt.

Nicht alle Systeme und Daten, die in der Cloud gehostet werden, haben die gleichen Anforderungen an die Geheimhaltung, daher ist es notwendig, die richtige Option für das jeweilige System oder die Daten zu wählen. Die BoM-Entscheidung umfasst typischerweise den Umfang der Daten, die in der Cloud gehostet werden dürfen (unter welchen Bedingungen), und es wäre möglich, dass ein Cloud-Anbieter (einige Dienste des Cloud-Anbieters), die trotz der technischen Möglichkeiten nicht für die Speicherung vertraulicher (oder personenbezogener) Daten verwendet werden dürfen.

Bestehende Sicherheitsanforderungen für KMS gelten weiterhin oder anders ausgedrückt - die Verwendung von KMS für die Cloud ändert nicht die Anforderungen für die Schlüsselstärke usw. Außerdem muss die Kommunikation mit dem KMS verschlüsselt werden.

Die meisten SaaS-Cloud-Dienste erlauben oder unterstützen die Verwendung von externer Schlüsselverwaltung nicht, aber für diejenigen, die dies tun, muss eine geeignete Lösung entsprechend der Datenklassifizierung verwendet werden.

Diese Anforderung steht im Einklang mit Anforderung 16 aus 3.63. ("Betrieb in DT IT") für die Systeme, für die 3.63. gilt.

Motivation: Ein KMS ermöglicht eine differenzierte Zugriffskontrolle und Überprüfbarkeit der Schlüsselnutzung und bietet eine robuste Sicherheitsgrundlage für den Schutz schutzbedürftiger Daten im Ruhezustand und bei der Übertragung. KMS verfügen in der Regel über HSMS im Backend, die physischen Schutz, sichere Schlüsselspeicherung und Verschlüsselungsbeschleunigung bieten und so dazu beitragen, die Vertraulichkeit, Integrität und Verfügbarkeit kritischer kryptografischer Vorgänge sicherzustellen.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.66-52/5.0

Req 53 Ein externer Schlüsselgenerator muss verwendet werden, wenn der Hypervisor des CSP nicht in der Lage ist, genügend Entropie bereitzustellen.

Unwahrscheinlich, aber dennoch möglich ist, dass ein bestimmter CSP Hypervisoren verwendet, die den Prozessen nicht genügend Entropie bieten. Das heißt: es gibt keinen geeigneten Zufallszahlengenerator (RNG) innerhalb der VM, der mit dem Host oder einem externen RNG-Gerät verbunden ist. In solchen Fällen muss ein externer Schlüsselgenerator für die Erzeugung von Geheimnissen verwendet werden da die innerhalb der virtuellen Maschinen erzeugten Geheimnisse aufgrund mangelnder Entropie neu erzeugt werden könnten.

Die sichere Übertragung von extern generierten Geheimnissen in die virtuelle Maschine ist eine zusätzliche Herausforderung da es unmöglich ist, eine wirklich sichere Verbindung einzurichten. Daher ist es am besten, die Verwendung eines solchen CSP im Allgemeinen zu vermeiden.

Zum Zeitpunkt der Erstellung dieses Artikels haben Hyperscaler (AWS, Azure und GCP) eine gute Entropiequelle für ihre VMs. Es gab einige kleine Cloud-Anbieter in der Vergangenheit, die Entropie für Gast-VMs nicht mit geeigneten Mitteln zur Verfügung stellten (z. B. Übergabe von `/dev/urandom` als RNG-Gerät). Als Beispiel für einen externen Schlüsselgenerator kann ein KMS verwendet werden.

Motivation: Durch die Verwendung eines externen Schlüsselgenerators kann das Risiko kompromittierter oder schwach generierter Schlüssel verringert werden, da der Prozess außerhalb des Systems oder der Infrastruktur ausgeführt wird, das die Schlüssel verwendet.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.66-53/5.0

Req 54 Verwendete dedizierte Hardwareressourcen müssen beim Freigeben gelöscht werden.

Bei der Verwendung von Bare-Metal-Servern oder -Komponenten (GPUs/FPGAs/Festplatten) wird der Inhalt des Speichers (sowohl flüchtig als auch nicht-flüchtig) in der Regel vom Cloud-Anbieter gelöscht, bevor die Maschine oder eine Ressource an einen anderen Mieter übergeben wird.

Zusätzlich zum Verlassen auf die Datenhygiene des Cloud-Anbieters kann ein Benutzer, um jeden Zweifel auszu-schließen, den flüchtigen Speicher mit Zufallsdaten und/oder Nullen löschen, gefolgt von einem Neustart oder einem einfachen Herunterfahren. Daten im Speicher von Geräten wie GPUs oder FPGAs können nicht immer verschlüsselt werden. Aus diesem Grund ist es empfehlenswert, die Löschung vor der Freigabe der Resource durchzuführen, vor allem weil das sehr einfache und schnelle Operationen sind.

Im Falle von nichtflüchtigem Speicher kann ein Benutzer zumindest die Header der Speichergeräte oder die gesamte unverschlüsselte Bootfestplatte löschen. Da der Speicher in jedem Fall verschlüsselt werden muss, reicht das Löschen des Schlüssels aus, um die Daten unlesbar zu machen. Im Fall von SSDs, bei denen typischerweise nur Sektoren zum Löschen markiert und nicht alle wirklich überschrieben werden, kann sich ein Benutzer nur auf die vom CSP durchgeführten Kontrollen und Verfahren verlassen. Wenn eine nicht verschlüsselte Bootfestplatte für einen dedizierten physischen Server verwendet werden muss verwendet, darf sie KEINE schutzbedürftige Daten enthalten - keine Passwörter, Passwort-Hashes, Schlüssel, Zertifikate, und insbesondere KEINE Entschlüsselungsschlüssel für andere Daten.

In dem unwahrscheinlichen Fall, dass der Cloud-Anbieter die Ressourcen nicht löscht (was im SOC2-Typ-2-Bericht nachgewiesen werden kann), muss der Nutzer der jeweiligen Cloud-Ressourcen für die vollständige Datenlöschung sorgen. Plötzliche Hardwareausfälle können dazu führen, dass der Benutzer nicht in der Lage ist, die Daten nach der Nutzung zu löschen. Daher wäre es am besten, keine Bare-Metal-Ressourcen zu verwenden, wenn der Cloud-Anbieter sich nicht um die Löschung der Ressourcen kümmert.

Motivation: Das sichere Löschen unterstützt den Schutz vertraulicher Informationen, den Schutz des geistigen Eigentums und die Aufrechterhaltung des Kundenvertrauens, indem sichergestellt wird, dass Daten ordnungsgemäß ge-

löscht werden und von Unbefugten nicht wiederhergestellt werden können.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unbemerkt durchführbare Angriffe

ID: 3.66-54/5.0

Req 55

Der Daten-Lebenszyklus muss durch entsprechende Richtlinien konfiguriert werden.

Public Cloud Anbieter bieten die Möglichkeit den Datenlebenszyklus durch entsprechende Richtlinien zu definieren, oft z. B. genutzt für Objektspeicher. Das Konfigurieren eines solchen Zykluses erlaubt es Daten durch verschiedenen Ebenen zu bewegen - mit entsprechenden Restriktionen bis zur Löschung der Daten. Eine Automatisierung dieses Prozesses kann Datenlecks verhindern und verbessert die Einhaltung von regulatorischen Anforderungen. Diese beinhalten:

- Das Bewegen von Daten aus der regulären Nutzung zum Archivspeicher, typischerweise aus wirtschaftlichen Gründen.
- Minimale Lebensdauer von Daten, nötig auf Grund von Regulationen.
- Maximale Lebensdauer von Daten, nötig auf Grund von Regulationen.
- Automatisierte Löschung von Daten am Ende ihres Lebenszykluses.
- Die Möglichkeit komplexere Lebenszyklen zu erschaffen, beispielsweise die Anonymisierung von Daten zu einem bestimmten Zeitpunkt.

Schlüssel, die zur Verschlüsselung der Daten benutzt werden, müssen dem gleichen Lebenszyklus wie diese folgen.

Motivation: Der Datenlebenszyklus optimiert das Datenmanagement, senkt die Speicherkosten, erfüllt gesetzliche Anforderungen, schützt schutzbedürftige Informationen und bewahrt die Datenintegrität während des gesamten definierten Prozesses des Lebenszyklus.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.66-55/5.0

8. Schutz von Verfügbarkeit und Integrität

Req 56 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 57 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 aufzubrauchen, 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 58 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 Verringerung 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 59 Systeme, die eine hohe Verfügbarkeit und Zuverlässigkeit benötigen, müssen entsprechend redundant ausgelegt und eingesetzt werden.

Cloud-Service-Provider haben in der Regel eine sehr robuste Infrastruktur. Das gilt aber nicht für jede einzelne Komponente in der Cloud. Virtuelle Maschinen und Container können sogar noch häufiger als in traditionell betriebenen Systemen nicht mehr verfügbar werden. Systeme, die eine hohe Verfügbarkeit und Zuverlässigkeit in der Cloud benötigen, müssen ihre High Availability (HA)-Mechanismen anpassen, damit sie in Cloud-Umgebungen hochverfügbar und belastbar bleiben. Das bedeutet, dass Systeme und Anwendungen so konzipiert sein müssen, dass sie mit Ausfällen umgehen können. Zu bevorzugen ist die Verwendung von verschiedenen Regionen, Verfügbarkeitszonen oder Rechenzentren des CSP (oder mehreren Cloud-Anbietern) für redundante Anwendungskomponenten, um HA für das in der Cloud bereitgestellte Gesamtsystem zu gewährleisten.

Um ein in der Cloud eingesetztes System gegen Ausfälle und Belastbarkeit zu testen, kann auch in Erwägung gezo-

gen werden, Chaos-Engineering einzusetzen (z. B. Chaos Monkey oder Simian Army).

Die meisten SaaS-Cloud-Dienste erlauben oder unterstützen die Konfiguration bestimmter Regionen nicht oder haben einfach keine unterschiedlichen Bereiche, aber für die Dienste, die dies tun, muss eine geeignete Region oder Bereich verwendet werden, um die gewünschte SLA zu erreichen und die Erwartungen an Hochverfügbarkeit, Geschäftskontinuität und Notfallwiederherstellung zu erfüllen.

Motivation: Redundanz trägt dazu bei, die Auswirkungen von Hardwareausfällen, Softwarestörungen oder Naturkatastrophen zu mindern, eine unterbrechungsfreie Servicebereitstellung zu gewährleisten, Ausfallzeiten zu reduzieren und die Zuverlässigkeit und Leistung des Gesamtsystems zu verbessern.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

ID: 3.66-59/5.0

Req 60	Es muss eine Backuplösung verwendet und sichergestellt werden, dass dessen Wiederherstellung funktioniert.
--------	--

Die Anforderung kann übersprungen werden, wenn keine Notwendigkeit der Datenerhaltung besteht.

Cloud-Anbieter bieten in der Regel eine ausgezeichnete Zuverlässigkeit, Verfügbarkeit und Haltbarkeit der in der Cloud gespeicherten Daten, außer in Fällen, in denen z. B. ihre Rechenzentren abbrennen (was in der Vergangenheit auch schon vorgekommen ist). Andererseits führen sie die Sicherung für Kunden nicht automatisch durch. Daher liegt es in der Verantwortung des Systembesitzers, eine Sicherungs- und Wiederherstellungsstrategie entsprechend den geschäftlichen Anforderungen für das gegebene System zu implementieren. Dies kann unter Berücksichtigung der folgenden Szenarien erfolgen:

- Versehentliches oder absichtliches (Insider-Attacken) Überschreiben/Löschen von Daten
- Datenbeschädigung durch Bugs
- Ransomware-Attacken
- Feuer, Überschwemmungen, Erdbeben oder jede andere Katastrophe, die ein Rechenzentrum, eine Verfügbarkeitszone oder sogar eine Region des Cloud-Anbieters betreffen können

Es ist auch zu erwähnen, dass das Einbinden eines Sicherungsdatenträgers in ein System, das gerade gesichert wird, im Falle eines Ransomware-Angriffs wahrscheinlich die schlechteste Praxis ist, da die Ransomware sowohl das System als auch die Backups sperren würde. Wenn möglich, sollte eine Backup-Lösung einen Backup-Speichertyp verwenden, der das einmalige Schreiben von Daten erlaubt, aber keine bereits geschriebenen Daten verändern darf. Zudem müssen Richtlinien implementiert werden, die ein zu frühes Löschen von Backups verhindern. Außerdem sollte das Backup-System (z. B. Backup-Festplatte oder Storage-Bucket) generell zu einem anderen Mandant mit anderen Anmeldedaten gehören, damit eine Misskonfiguration, Maleware oder ein Angreifer die Backups nicht gleichzeitig mit dem System zerstören kann. Ähnlich hierzu wäre z. B. das unabsichtliche Ausführen von `'rm -rf /'` bei gemountetem Backup-Drive.

Die Backup-Daten müssen alle Daten enthalten, die für die Geschäftskontinuität notwendig sind, z. B. "reguläre Daten", Systemkonfigurationen, Schlüssel (die separat gehandhabt werden müssen), Protokolle, ...

Die Backups müssen vor unbefugtem Zugriff geschützt werden, typischerweise durch den Einsatz von Verschlüsselung und entsprechenden Schutz der Verschlüsselungsschlüssel.

Ein Backup ohne funktionierende Restore-Funktion reicht nicht aus, daher muss das Gesamtkonzept einen Restore-Mechanismus und Restore-Tests beinhalten, die vorzugsweise automatisiert sind. Das Testverfahren für die Wiederherstellung muss so gestaltet sein, dass es keine Möglichkeit gibt, versehentlich Ausfallzeiten oder Datenverluste im Produktionssystem zu verursachen oder eine andere Art von Datenleck zu verursachen.

Abhängig von der Datenklassifizierung können Backups in folgenden Orten gespeichert und gelagert werden:

- In der gleichen Cloud (vom gleichen CSP)
- In einer anderen Cloud (von einem anderen CSP)

- Auf der On-Premises Seite der DTAG (wäre ein ungewöhnlicher Ansatz, aber dennoch möglich)

Die Priorisierung oder Reihenfolge der Systeme, die aus dem Backup wiederhergestellt werden müssen, muss im Voraus festgelegt werden, da dies in der Regel ein zeitaufwändiger Prozess ist und die Durchführung der Priorisierung während eines Vorfalls das Service Level Objective (SLO) und das Recovery Time Objective (RTO) gefährden würde. Weitere Einzelheiten sind in Anforderung 5 im Dokument 3.61 „Betrieb“ zu finden.

Obwohl SaaS-Cloud-Dienste nicht viele Backup-Funktionen anbieten, besitzen sie evtl. die Möglichkeit der Versionierung, Verhinderung von (meist versehentlichem) Löschen und andere Funktionen zum Schutz von Daten. Solche Funktionen müssen entsprechend konfiguriert werden, um die gewünschte Haltbarkeit der Daten zu erreichen.

Motivation: Backups gewährleisten die Ausfallsicherheit der Daten, mindern das Risiko von Datenverlusten und erleichtern die Datenwiederherstellung bei Systemausfällen, Katastrophen oder Sicherheitsvorfällen. Backups dienen als Schutz vor versehentlichen Löschungen, Hardwarefehlern, Ransomware-Angriffen oder anderen unerwarteten Ereignissen, die zu Datenbeschädigung oder -verlust führen können.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

ID: 3.66-60/5.0

9. Architektur und Vernetzung

Req 61	Jede Applikation/jedes System inklusive ihres Umgebungstyps (z. B. Entwicklung, Test, Produktion) in der Cloud muss als Tenant/Projekt von allen anderen Applikationen/Systemen und Umgebungen getrennt werden, wobei auch die Trennung zwischen Applikation/System und jeweiliger Backup zu gewährleisten ist und jeder Tenant/jedes Projekt unabhängig vom Umgebungstyp gleich behandelt werden muss.
--------	---

Applikationen müssen (logisch) voneinander getrennt werden. Eine Trennung wird auch für verschiedene Umgebungen benötigt, so dass es zu keinen ungewollten Aktionen zwischen unterschiedlichen Umgebungen kommen kann, bspw. Produktionsdaten im Entwicklungssystem, oder das Einführen von Testcode in einer Produktionsumgebung.

Die Trennung von Anwendung und Sicherung derselben Anwendung durch die Verwendung eines anderen Mandanten und separater Anmeldeinformationen ist ebenfalls erforderlich, um die Sicherung für den Fall einer Kompromittierung der Anwendung aufzubewahren.

Die gleiche Separierung muss für den Management teil der Applikation gelten, bspw. CI Runner für unterschiedliche Umgebungen, trotz des nutzen einer gemeinsamen multi-tenant CI/CD Chain für Test, Referenz und Entwicklungssysteme.

Dieser Ansatz ermöglicht eine obligatorische Aufgabentrennung und verhindert ungewollten Zugriff auf Daten und Systeme, gleichzeitig erlaubt er es auch die Kommunikation zwischen verschiedenen Diensten zu kontrollieren.

System/Applikation ist ein vage gefasster Begriff und kann einen einzelnen Mikroservice, oder eine ganze IPTV Plattform einschließen.

In diesem Kontext ist es dem Systemverantwortlichen zusammen mit einem Sicherheitsexperten überlassen den bestmöglichen Weg zur Separierung zu definieren.

Ein paar grobe Richtlinien sind:

- Ein einzelner Mikroservice benötigt keinen eigenen Tenant
- Große Systeme wie z. B. eine IPTV Plattform müssen gegebenenfalls in mehrere Tenants nach Funktion (Management, Streaming, Provisionierung, Mediathek) unterteilt werden.

Zusätzlich zur Separierung von Accounts müssen unterschiedliche Tenants/Projekte nach den gleichen Regeln geschützt werden. Es ist verständlich, dass Produktionssysteme den höchsten Schutzbedarf benötigen, jedoch müssen Test- und Entwicklungssysteme gleichwertig geschützt werden. Die Zugangsdaten dieser Systeme müssen sorgfältig geschützt werden und dürfen nicht in Klartext auf Git Repositories gespeichert werden. Sie dürfen nur von zugelassen Arbeitsplatzsystemen aus genutzt werden. Es wird empfohlen Test- und Entwicklungssysteme mit niedrigeren Quoten für das Anschlagen von Alarmen oder Ressourcenüberschreitungen auszustatten. Dies kann Cryptomining vorbeugen, einer gängigen Missbrauchspraxis im Public Cloud Umfeld, häufig durch abhandengekommene Zugangsdaten oder unsichere Arbeitsplatzsysteme begünstigt.

Die vorliegende Anforderung ist mit dem Sicherheitsanforderungskatalog "3.14 - Architektur von Systemen" abgestimmt. Sie gilt daher weiterhin auch in dem Fall, dass der Katalog "3.14 - Architektur von Systemen" ebenfalls zur Anwendung kommt.

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 Tenants/Projekte 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 SaaS-Dienste kann die Trennung durch die Verwendung unterschiedlicher Konten, Ordner oder Abschnitte erreicht werden, abhängig von den Begriffen, die der SaaS-Cloud-Anbieter verwendet.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.66-61/5.0

Req 62 Zentrale Dienste für das Managen von Clouds müssen separiert werden.

Zentrale Dienste wie Logging-Infrastruktur, IAM, Reporting oder Sicherheitsdienste müssen auch in Form von Tenants/Projekten getrennt werden, auch wenn es in ihrer Natur liegt gegebenenfalls mehr rechte zu benötigen als eine typische in der Cloud gehostete Applikation. (IAM muss in der Lage sein Accounts für jedermann unter der gleichen Root Domäne für eine Organisation zu erstellen.)

Motivation: Die Trennung zentraler Dienste in bestimmten Mandanten/Projekten kann dazu beitragen, die potenziellen Auswirkungen von Sicherheitsverletzungen oder Betriebsproblemen in einem Konto auf das gesamte System zu minimieren. Darüber hinaus bieten separate Mandanten/Projekte granulare Zugriffskontrollen, einen besseren Einblick in die Ressourcennutzung und -kosten und ermöglichen eine unabhängige Verwaltung und Governance der einzelnen Dienste, wodurch eine robustere und sicherere Gesamtarchitektur gefördert wird.

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
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.66-62/5.0

Req 63 Applikationen müssen in multi-tier Modellen gebaut werden.

Dieses Vorgehen ist eine bereits bewährte Methode und soll an dieser Stelle nur dazu dienen daran zu erinnern, dass dies auch in Cloud-Umgebungen zu beachten ist.

Klassische Applikationen benötigen immer noch Firewalls als Separierungselement zwischen Netzen, speziell während der Übergangszeit zu Public Clouds.

Aus diesem Grund muss die klassische Netzsegmentierung mit den Mitteln der Cloud nachgeahmt werden und entsprechende Sicherheitsmechanismen müssen implementiert werden. Auf der Public Cloud wird dies mit Hilfe von Sicherheitsgruppen und virtuellen Netzen umgesetzt.

Cloud Native Applikationen müssen dem Mikrosegmentierungsansatz folgen um eine Trennung zwischen verschiedenen Ebenen zu realisieren. Das resultiert in flacheren Netzen, in denen jede Komponente durch entsprechende Sicherheitsrichtlinien und Sicherheitsgruppen der Cloud geschützt wird.

Sicherheitsanforderungen aus anderen Dokumenten sind mit einzubeziehen, z. B. aus den Containeranforderungen :

- Container, die verschiedenen Sicherheitszonen zugeordnet sind (z. B. DMZ-Zone, Anwendungs- / Datenbankzone) müssen auf verschiedenen Hosts / Host-Pools bereitgestellt werden. Ein Pool bezieht sich auf eine Gruppe von mindestens einer oder mehreren VMs. Im Falle der Verwendung von Container as a Service (CaaS) - Plattformen können diese Pools für mehrere Anwendungen gemeinsam genutzt werden. Für kritische Anwendungen müssen dedizierte Hosts / Host-Pools. Wenn der einzige exponierte Dienst ein Ingress-Controller (z. B. Nginx) ist, der hinsichtlich Sicherheit gehärtet ist, können Sie dies implementieren, indem Sie nur Container-spezifische Maßnahmen verwenden, wie z. B. Pod Security Policies / Network Security Policies.

Motivation: Die Aufteilung der Anwendung in verschiedene Ebenen , wie z. B. Darstellung, Anwendungslogik und Da-

tenspeicherung, hilft bei der Implementierung von Sicherheitsmaßnahmen und Schutz auf jeder Ebene. Aktualisierung oder Änderung bestimmter Ebenen sind möglich, ohne dass sich dies auf das gesamte System auswirkt.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.66-63/5.0

Req 64	Ressourcen müssen durch Virtual Private Clouds (VPC) getrennt werden. Netzkommunikation von Applikationen/Diensten muss durch den Einsatz von Netz Filterelementen beschränkt werden. Falls ein CSP erweiterte Methoden zum Schutz von Netzen anbietet, müssen diese genutzt werden.
--------	---

Virtual Private Clouds sind ein Konzept zur Separierung (von Netzen) von Ressourcen eines Systems (oder einer Gruppe von Systemen) innerhalb der Public Cloud von anderen Ressourcen. Für Ressourcen werden Richtlinien für Konnektivität/Erreichbarkeit definiert. Diese Richtlinien sind über verschiedene Rechenzentren, Verfügbarkeitszonen/regionen der Public Cloud heraus definierbar. Um einfache und effektive Netzabgrenzung zu gewährleisten, müssen VPCs verwendet werden. Wenn VPCs verwendet werden kann dies die Notwendigkeit für den Einsatz von VPNs für jedes einzelne Rechenzentrum des CSPs minimieren. Zusätzlich kann der Netzwerkverkehr durch die Verwendung von geeigneten Routingtabellen des VPCs kontrolliert werden. Das VPC Konzept erlaubt es Kunden der Cloud eigene IP-Bereiche für Ressourcen zu benutzen.

Die häufigste Implementierung von Netz Filterelementen sind Security Gruppen. Security Gruppen sind im Zusammenspiel mit VPCs der Grundstein für das Einschränken der Kommunikationspfade innerhalb der Cloud. Security Gruppen sollten so restriktiv wie möglich sein und nur benötigte Kommunikation erlauben.

Zusätzlich zu Security Gruppen bieten CSPs meistens einen DoS/DDoS Schutz, Rate Limiting und andere Netzsicherheitsfeatures an - diese müssen genutzt werden.

Manche CSPs bieten den VPC Dienst nicht wörtlich an, es ist jedoch möglich das gleiche mithilfe von virtuellen Netzen zu implementieren.

Motivation: VPCs fügen eine zusätzliche Sicherheitsebene hinzu, da sie eine Trennung sowohl auf Netzebene (Netz und Routing) als auch auf Zugriffsebene bieten. Nur zugelassene Benutzer können Systeme innerhalb einer bestimmten VPC bereitstellen und den Verbindungspfad dafür konfigurieren.

Diese Trennung trägt dazu bei, unbefugten Zugriff zu verhindern, die Auswirkungen von Sicherheitsvorfällen zu begrenzen und das Netzmanagement zu optimieren, was eine bessere Ressourcenzuweisung und eine verbesserte allgemeine Sicherheitslage ermöglicht.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.66-64/5.0

9.1. Anbindung der Cloud

Req 65	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 Zu-

griffe 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 66 Die Erreichbarkeit von Management Diensten für Applikationen/Dienste muss eingeschränkt sein.

SSH und RDP sind die verbreitetsten Dienste zum Managen von Applikationen/Diensten in der Cloud und spielen eine wichtige Rolle zum Absichern von Cloud Applikationen. Sollte ein Angreifer Zugriff auf einen Management-Dienst erlangen, kann er relativ einfach ein System oder mehrere mit wenig Aufwand kompromittieren. Management (Admin)-Dienste einer Anwendung in der Cloud dürfen nicht uneingeschränkt erreichbar sein. Deshalb ist es wichtig den Zugriff und die Angriffsfläche auf diese Dienste zu minimieren, sie sollten nicht via Internet erreichbar sein. Sollten sie doch via Internet erreichbar sein, so muss der Zugriff auf vertrauenswürdige Nutzer eingeschränkt werden und/oder zentral verwaltete Sprungserver als Eingangstor genutzt werden.

Das Benutzen von unveränderlichen Images setzt keinen Management-Zugang voraus und reduziert die Angriffsfläche.

Bietet ein SaaS-Cloud-Anbieter eine solche Funktion an, kann der Zugriff auf das Administrationsportal auf bestimmte geografische Standorte, IP-Adressen, bestimmte Wochentage oder bestimmte Tageszeiten beschränkt werden. Dabei sollte man beachten, administrative Benutzer, insbesondere sogenannte Konten für den Notfallzugriff, nicht vollständig auszuschließen.

Motivation: Wenn gängige Remote-Management-Dienste allgemein zugänglich gemacht werden, sind sie potenziellen Bedrohungen durch böswillige Akteure ausgesetzt, die versuchen, sich unbefugten Zugriff auf Systeme zu verschaffen oder Angriffe zum Erraten von Passwörtern zu starten. Die Begrenzung der Angriffsfläche ist ein wichtiger Schritt, um die Möglichkeit solcher Angriffe zu mindern.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.66-66/5.0

9.2. Anbindung der Cloud - Externe Anbindung

Datenverkehr, der aus der Cloud herausgeht oder zu unserem Standort innerhalb der Cloud gelangt.

Req 67	Dedizierte physikalische oder dedizierte virtuelle Verbindungen müssen für die Konnektivität zwischen Applikationen auf der Public Cloud und On-Premise Ressourcen der Deutschen Telekom genutzt werden. Das gleiche gilt für Applikationen, die auf unterschiedlichen Public Clouds gehostet werden. Internetzugriff ist hierbei nur cloud-native, sowie internet-native Anwendungen vorbehalten, sofern diese eine Freigabe durch die Telekom Security erhalten haben.
--------	--

Typischerweise werden die Lokalisationen von Cloud Service Provider und DTAG via Glasfaser verbunden - dedizierte physikalische Verbindung. Dedizierte virtuelle Verbindungen werden durch einen VPN Endpunkt innerhalb der DTAG Lokalisationen mit einem VPN Endpunkt innerhalb der Public Cloud verbunden. Die Verbindung von zwei Public Clouds muss auch via VPN erfolgen.

Eine Applikation auf der Public Cloud, die eine permanente Konnektivität von/zu DTAG Ressourcen benötigt, unabhängig davon, ob sie innerhalb von DTAG Lokalisationen oder einer Public Cloud ausgeführt wird, muss hierfür einen VPN benutzen. Nicht jede Applikation braucht eine eigene VPN Verbindung, es kann die gleiche Verbindung genutzt werden, die schon zwischen CSP und DTAG benutzt wird.

Die möglichen Methoden sind die folgenden in Reihenfolge:

1. Dedizierte physikalische Verbindung (verlässlicher falls exklusiv benutzt)
2. Dedizierte virtuelle Verbindung
3. VPN via Internet (weniger verlässlich)
4. (Beschränkt) Einfache Internetverbindung; Benötigt Security Freigabe.

VPN Verbindungen, die ein geteiltes backbone Netz mit anderen Kunden oder via Internet benutzen sind typischerweise weniger verlässlich im Falle von z. B. DDoS Angriffen.

Einfache Internetverbindung ist nur bei Cloud/Internet-native Anwendungen erlaubt. Desweiteren ist es nötig die Kommunikation mit IP ranges einzuschränken und auf ein Minimum zu begrenzen. Diese Methode ist typischerweise für Tests/Trails gedacht und kommt in der DTAG nicht häufig vor.

Diese dedizierten Verbindungen mögen verschlüsselt sein, jedoch haben sie keinen Einfluss auf folgende Anforderung: Alle nicht öffentlichen Daten (non-public) müssen während der Übertragung verschlüsselt werden. Der Datenfluss muss an jeder Stelle verschlüsselt erfolgen. Eine VPN Verbindung muss immer verschlüsselt sein. Die Redundanz muss entsprechend der gewünschten Verfügbarkeit ausgelegt sein um einer Einschränkung des Dienstes vorzubeugen.

Motivation: Eine dedizierte Verbindung zur Cloud wird verwendet, um eine zuverlässige, sichere und leistungsstarke Verbindung zu erreichen und gleichzeitig den Datenschutz zu verbessern und die Latenz im Vergleich zu öffentlichen Internetverbindungen zu reduzieren.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Störung der Verfügbarkeit

ID: 3.66-67/5.0

Req 68	Es müssen DTAG-interne Prozeduren definiert werden, die es ermöglichen, jegliche Verbindungen zwischen dem CSP und der DTAG-eigenen Infrastruktur zu unterbrechen.
--------	--

Malware, insbesondere Ransomware, kann sich sehr schnell über das Netzwerk verbreiten und sich auch auf Daten auswirken, die über das Netzwerk verfügbar sind, selbst auf Speichersystemen, die eine Authentifizierung erfordern. In bestimmten Fällen ist es am besten, die Netzwerkkommunikation zu blockieren. Das gilt nicht nur für interne Systeme, sondern auch für Cloud-Umgebungen.

Motivation: Im Falle von Vorfällen wie Ransomware-Angriffen muss es möglich sein, Cloud-Umgebungen sofort abzuschneiden, um eine weitere Ausbreitung zu verhindern.

Umsetzungsbeispiel: Das für das Abschaltszenario definierte Verfahren muss die notwendigen Schritte zum Unterbrechen der Kommunikation berücksichtigen, indem je nach Verbindungstyp entweder Kabel abgezogen, Netzwerkports deaktiviert, VPNs heruntergefahren, der gesamte Datenverkehr in der Firewall blockiert oder eine andere verfügbare Methode verwendet wird. Das Szenario muss berücksichtigen, dass die Ransomware-Infektion in der Cloud-Umgebung beginnen kann, was eine Isolierung der Cloud-Umgebung erfordert, aber auch die Möglichkeit, dass die Infektion im DTAG-Netzwerk begann und sich auf die Cloud-Umgebung ausbreitet.

In den Fällen, in denen die Konnektivität zwischen der Cloud und der DTAG nur über das Internet erfolgt (wie SaaS), kann die Sperrung der Konnektivität auch durch Sperrung der betroffenen Konten erfolgen.

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: 3.66-68/5.0

Req 69	Verbindungen zwischen Public Cloud und Ressourcen innerhalb von DTAG Netzen müssen durch ein unabhängiges Netzfilterelement unter Kontrolle der DTAG geschützt werden. Ein Dienst in der Cloud darf keinen direkten Internetzugang in Kombination mit Zugriff auf DTAG interne Netze haben.
--------	---

Verbindungen zwischen Public Clouds und internen Netzen der DTAG (z. B. CN-DTAG) müssen durch ein Sicherheitselement geschützt werden. Abhängig vom Anwendungsfall sind zu benutzen:

- stateful firewall (als absolutes Minimum)
- web application firewall
- application-level gateway
- API gateway
- DoS/DDoS Schutz
- ...

Das Sicherheitselement in diesem Kontext kann aus mehreren physischen oder virtuellen Teilen bestehen, die als eine Einheit fungieren. Der Schutz des eingesetzten Produkts muss bidirektional funktionieren, also DTAG Netze von Angriffen aus der Cloud schützen, sowie auch Ressourcen innerhalb der Public Cloud vor Schadsoftware und böswilligen Insidern schützen. Es wird vorausgesetzt, dass Anwendungen auf der Public Cloud Funktionen wie Security Gruppen und andere von der Cloud bereitgestellte Sicherheitsfunktionen nutzen. Aus diesem Grund müssen die Regeln für die Verbindung von DTAG internen Netzen Richtung Public Cloud nicht besonders detailliert sein. Für die andere Richtung, Public Clouds zu DTAG internen Netzen, muss die Implementierung vollständig durch ein geeignetes Produkt realisiert werden.

Für HTTP(S) basierte Dienste sollte das Sicherheitselement über einen Schutz gegen die OWASP Top 10 Web-schwachstellen verfügen - als Minimum.

Die Konfiguration eines solchen Sicherheitselements sollte vollautomatisiert möglich sein, sodass es mit der schnellen Provisionierung im Cloud-Umfeld Schritt halten kann (es sollte dynamische IP-Zuweisung bewältigen können).

Interne Netze der DTAG sind meistens nicht mit modernen Verfahren wie z. B. Mikrosegmentierung aufgebaut und Applikationen in der Cloud müssen sich nach diesem Aufbau richten, sollten sie sich mit solchen Systemen verbinden müssen. Applikationen dürfen nicht gleichzeitig mit dem Internet und DTAG internen Netzwerken verbunden werden, da hier sonst zwei Sicherheitsebenen entfallen. Dies würde es Angreifern erleichtern, DTAG interne Netze zu infiltrieren, z. B. durch Hintertüren wissentlich oder unwissentlich in Applikationen versteckt. Für spezielle Anwendungsfälle wie z. B. das Management oder die Überwachung einer Internetapplikation muss eine Lösung im Einzelfall gefunden

werden.

Ein Dienst, der in der Cloud verwendet wird und Zugriff sowohl auf das Internet als auch auf interne DTAG-Netze hat, muss über mehrere VMs, Container oder allgemein über mehrere Ebenen aufgeteilt sein (multi-tier Architektur).

Motivation: Interne Netze der DTAG sind nicht auf moderne Weise mit Blick auf Mikrosegmentierung aufgebaut. Anwendungen, die in der Cloud bereitgestellt werden, müssen Richtlinien für die Konnektivität zu bestehenden internen DTAG-Netzen befolgen, wenn sie eine solche Konnektivität benötigen. Anwendungen in der Cloud dürfen nicht gleichzeitig über direkte Internetverbindungen und Verbindungen zu internen Netzen der DTAG verfügen, da es in diesem Fall keine (mindestens) 2 Sicherheitsebenen gäbe. Dies würde es Angreifern ermöglichen, durch eine Hintertür, die absichtlich oder unbeabsichtigt in einer in der Cloud laufenden Anwendung platziert wird, viel einfacher in das DTAG-Netz und die Ressourcen einzudringen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Unbemerkt durchführbare Angriffe

ID: 3.66-69/5.0

9.3. Anbindung der Cloud - Interne Anbindung

Kommunikation innerhalb der Cloud und deren Sicherheit.

Req 70	Netzverkehr zwischen Ressourcen eines einzigen Cloud Providers müssen die sicherst mögliche Kommunikationsmöglichkeit nutzen.
--------	---

Die Kommunikation zwischen Cloud-Diensten kann auf verschiedene Arten implementiert werden, wobei die Verwendung eines öffentlichen Endpunkts die unsicherste Methode ist und die Kommunikation mit Sicherheitsgruppen bei der Verwendung privater Endpunkte als die sicherste angesehen werden kann.

Es muss die sicherste Option verwendet werden.

Die folgende Tabelle gibt einen hierarchischen Überblick über mögliche Optionen (von Sicher zu Unsicher):

1. Kommunizieren innerhalb eines einzelnen VNET/VPC
2. Private Endpunkte mit Sicherheitsgruppen des Dienstes oder Ressource der Cloud verwenden (z. B. VNET-Integration des Dienstes, VPC-Endpunkt, privater Link)
3. Verwendung dedizierter Verbindungen wie VNET-Peerings/VPC-Peerings (nur innerhalb der Telekom-Umgebung)
4. Öffentliche Endpunkte verwenden (am unsichersten)

Motivation: Die Verwendung der sichersten Art der Interaktion mit Cloud-Diensten ist von entscheidender Bedeutung, um schutzbedürftige Daten zu schützen, Vorschriften einzuhalten und Sicherheitsrisiken zu mindern.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.66-70/5.0

Req 71	Netz Filterelemente müssen verwendet werden, um Ressourcen auf Netzebene zu trennen.
--------	--

Um Ressourcen auf Netzebene zu trennen, müssen Netz Filterelemente (Sicherheitsgruppen, Cloud-Firewall, Security Tags) verwendet werden.

Die Notwendigkeit des Schutzes von Ressourcen ergibt sich aus verschiedenen Faktoren wie verarbeiteten und gespeicherten Daten, exponierten Diensten und verwendeten Anwendungen. Ebenso müssen Ressourcen, auf denen

personenbezogene Daten verarbeitet werden, durch den Stand der Technik (z. B. Firewalls oder Sicherheitsgruppen) vor unerwünschten Zugriffen oder Datenflüssen aus demselben Netz oder anderen Netzen geschützt werden.

Neben Sicherheitsgruppen können auch andere Mechanismen der Cloud wie Network Access Control Lists (NACLs) als zusätzliche Maßnahme verwendet werden.

Motivation: Es ist wahrscheinlicher, dass ein weniger geschütztes System kompromittiert wird. Dies darf nicht dazu führen, dass andere Systeme mit höherem Schutzbedarf durch dieses kompromittierte System im Netz leichter angegriffen werden können.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.66-71/5.0

Req 72	Standardregeln für Netz Filterelemente (jede Kommunikation ist erlaubt) dürfen nicht verwendet werden.
--------	--

Regeln für Netz Filterelemente wie Sicherheitsgruppen oder Cloud-Firewalls sind unterteilt in Regeln für die eingehende und ausgehende Kommunikation. Die standardmäßige Ausgangs-/Eingangsregel ermöglicht die Kommunikation für jeden Port und jede Adresse. Dies wird nicht auf die minimal erforderliche Kommunikation reduziert. Daher müssen je nach Anwendung Sicherheitsgruppen/Cloud-Firewall und Regeln erstellt und konfiguriert werden.

Motivation: Eine freizügige Kommunikation widerspricht dem Need-to-know-Prinzip.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.66-72/5.0

Req 73	In Netz Filterelementen und Filterregeln muss nur die notwendige Kommunikation konfiguriert werden.
--------	---

Die Regeln für Netz Filterelemente (z. B. Sicherheitsgruppen, Cloud Firewall) sind in Regeln für die Eingangs- und Ausgangskommunikation unterteilt. Standardmäßig erlauben die Ausgangsregeln die Kommunikation für jeden Port und jede Adresse; dies muss auf die minimal erforderliche Kommunikation reduziert werden. Jede notwendige Eingangskommunikation muss mit einer spezifischen Erlaubnisregel definiert werden.

Es wird empfohlen, Verweise auf eine Security Group (Namen) anstelle von spezifischen IP-Adressen oder IP-Bereichen in den Security Group-Regeln zu verwenden.

Security Groups sind zustandsbehaftet.

Bei der Verwendung von Dualstack (IPv4 und IPv6) ist zu beachten, dass die Regeln für beide Protokollversionen einzustellen sind.

Motivation: Eine freizügige Kommunikation widerspricht dem Need-to-know-Prinzip.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.66-73/5.0

10. Protokollierung und Überwachung

Req 74 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 75 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.

Umsetzungsbeispiel: Sicherheitsrelevante Log-Quellen, die aktiviert werden müssen:

- AWS: CloudTrail- und VPC-Flow-Protokolle.
- Azure: Aktivitätsprotokoll und NSG-Datenflussprotokolle.
- GCP: Cloud Operations Suite, Cloud-Audit-Logs und VPC-Flow-Logs.
- OTC: Cloud Trace, VPC flow logs

Sicherheitsrelevante Protokollquellen für Anwendungen, die berücksichtigt werden sollten:

- AWS: CloudWatch
- Azure: Log Analytics, Applications Insights
- GCP: Cloud Logging, Cloud Monitoring, Error Reporting
- OTC: Cloud Eye

ID: 3.66-75/5.0

Req 76	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 Vereinba-

rungen 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 Löschrufen 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 77	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 78	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 79	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 Reaktions-

onslösung für Sicherheitsvorfälle implementiert hat. Einige Cloud-Anbieter erzeugen zusätzlich dedizierte Protokollierungsdaten über sicherheitsrelevante Aktivitäten innerhalb der separaten Kunden-Mandanten ihrer SaaS Applikation (beispielsweise zu Änderungen von Konfigurationseinstellungen, Berechtigungsvergaben oder Benutzer-Konten innerhalb der Mandanten) und stellen diese den Cloud-Kunden zu Verfügung. Diese sogenannten Audit-Logs werden kontinuierlich zur weiteren Analyse, Angriffserkennung und Alarmbehandlung an ein SIEM (Security Information and Event Management) übertragen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unbemerkt durchführbare Angriffe

ID: 3.01-37/9.0

Req 80	Sicherheitsrelevante Ereignisse müssen protokolliert werden und müssen sowohl an einen separaten Log-Speicher als auch an das Security Information and Event Management System (SIEM) des zuständigen SOC's für die 24-7-Überwachung weitergeleitet werden.
--------	---

Die allgemeinen Sicherheitsanforderungen an Protokollierung gelten immer noch und sind auch relevant für Cloud-Umgebungen. Sicherheitsrelevante Ereignisse wie Cloud-Alarme, Cloud-Management- und API-Call-Logs, Konfigurationsänderungen, Account-Zugriffe, Zugriffe auf schutzbedürftige Daten, Netz-Logs, System-Logs, etc. müssen richtig protokolliert werden mithilfe der Protokollierungs- und Überwachungsinfrastruktur des CSPs; für alle verwendeten Servicetypen – IaaS, PaaS und SaaS. Unterstützende Systeme wie IAM und KMS, die in der Cloud verwendet werden, müssen ebenfalls in das Protokollierungskonzept einbezogen werden.

Das Protokollieren und Weiterleiten von sicherheitsrelevanten Ereignissen muss so für alle Tenants/Accounts/Systeme durch die Landing Zone konfiguriert werden, dass es umgehend nach der Erzeugung stattfindet und nicht durch Administratoren/Nutzer der Tenants/Accounts/Systeme deaktiviert werden kann. Wenn das nicht durch die Landing Zone sichergestellt werden kann, dann muss die Landing Zone Lösungen anbieten, die von den Tenants/Accounts/Systemen umgesetzt werden (z. B. Dokumentation der Konfiguration der Log-Weiterleitung, Nutzung von vorkonfigurierten Images). Die Landing Zone muss Kontrollen schaffen, dass die Weiterleitung aktiviert ist.

Die Überwachung von sicherheitsrelevanten Ereignissen ist eine Vorbedingung für die Angriffserkennung auf Cloudressourcen wie z. B. Datenverlust und Ressourcenverbrauch. Die Überwachung muss 24-7 für alle Umgebungen (einschließlich Test- und Entwicklungsumgebungen) erfolgen, da, zusätzlich zu traditionellen Angriffen mit Malware und Ransomware auf Produktionsumgebungen, das Schürfen von Kryptowährungen durch Angreifer über das Wochenende ebenso eine Bedrohung ist, die einen großen finanziellen Schaden verursachen kann.

Die gleichzeitige Weiterleitung von Logs zum einen an einen separaten Log-Speicher und zum anderen an das SIEM hilft bei den Fällen, bei denen das SIEM Logs nur für eine zu kurze Zeit vorhält, wie z. B. im Fall des CDC, das die Sicherheitsüberwachung für die DT IT übernimmt (Telekom Security Cyber Defense Center – das CDC kommt gewöhnlich in Deutschland zum Einsatz). In diesem speziellen Fall speichert der separate Logserver die Logs für forensische Analysen, um Beweise für legale Maßnahmen gegen Angreifer zu haben.

Die Protokollierungsrichtlinie muss den Gesetzen, Vorschriften und Unternehmensrichtlinien entsprechen. Gemäß den aktuellen Gesetzen, Vorschriften und Unternehmensrichtlinien ist das Protokollieren von solchen Ereignissen nur für festgelegte Anwendungsfälle erlaubt und verboten für andere wie verhaltensüberwachende Maßnahmen von Mitarbeitern.

Einige Beispiele für Ereignistypen/-Logs:

- Cloud-Alarme: GuardDuty bei AWS oder SecurityCenter bei Azure
- Cloud-Management- und API-Call-Logs: AWS CloudTrail oder Azure Activity Logs
- Netz-Logs: alle Verbindungen zum und vom Internet müssen mittels Proxy protokolliert werden und wenn möglich der gesamte relevante Netzverkehr - VPCFlowlogs
- System-Logs: syslog/auditd und winlog

Falls für ein System die Sicherheitsanforderungen aus 3.63 („Betrieb in DI IT“) relevant sind, findet die Anforderung 25 aus 3.63 als spezifischere Anforderung Anwendung.

Motivation: Wenn Protokolldaten nur lokal gespeichert werden, können sie von einem Angreifer manipuliert werden, dem es gelingt, das System zu kompromittieren, um seinen Angriff und etwaige Manipulationen, die er am System vorgenommen hat, zu verschleiern. Aus diesem Grund muss die Weiterleitung unmittelbar nach dem Eintreten des Ereignisses erfolgen.

Nur wenn Log-Daten analysiert werden, können Bedrohungen identifiziert werden. Die Analyse muss 24/7 erfolgen, da Angreifer ihre Angriffe nicht außerhalb der Geschäftszeiten einstellen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.66-80/5.0

Req 81 Der Incident-Response-Prozess, um entsprechend auf Sicherheitsereignisse und -vorfälle zu reagieren, muss eingeführt werden, inklusive der Bereitstellung von forensischen Beweisen.

Ein klar spezifizierter Incident-Response-Prozess ist obligatorisch, um die Auswirkungen von andauernden oder erfolgreichen Angriffen zu minimieren. Der Prozess definiert Zuständigkeiten, Kontaktpersonen und Aufgaben für die Angriffsminderung, die Analyse vom potenziellen und wirklichen Schaden, Verfahren, um die Systemsicherheit wiederherzustellen, und das Erhalten von Beweisen für den Gesetzesvollzug.

Die beidseitige Betrachtung – ein System, das in der Cloud deployt ist, und verfügbare APIs des Cloud Providers – ist notwendig für den Incident-Response-Prozess, z. B. es kann vorteilhaft sein Snapshots von den betroffenen VMs zu machen, wenn es um kompromittierte virtuelle Maschinen geht; so können sie als Beweis erhalten bleiben.

In Abstimmung mit dem zuständigen SOC müssen die Landing Zone Betreiber Incident-Response-Kapazitäten gegenüber dem SOC (mit angemessenen kurzen Reaktionszeiten und einer 24-7-Verfügbarkeit) bereitstellen um in der Lage zu sein Angriffe direkt zu stoppen und weitere Schäden zu vermeiden. Die Kapazitäten müssen alle Umgebungen abdecken (inklusive Test- und Entwicklungsumgebungen) und der Zugriff auf alle Tenants/Accounts/Ressourcen muss möglich sein, sogar ohne die Systemverantwortlichen (z. B. mittels des Break-Glass-Account). Prozesse müssen definiert, eingeführt und regelmäßig geprüft werden, so dass es immer möglich ist die Kontrolle über kompromittierte Ressourcen zu erlangen und forensische Beweise richtig zu sammeln. Beispiele sind:

- Isolieren von kompromittierten virtuellen Maschinen
- Aktualisieren anderer relevanter Security Groups
- Widerrufen von missbräuchlich verwendeten Nutzern, Rollen und Rechten
- Stoppen von boshaften Diensten oder Serverless-Funktionen
- Exportieren weiterer relevanter Daten wie Kopien von virtuellen Maschinen, Containern und Speicher zum forensischen Labor des zuständigen SOC

Falls der Angriff vom Systemverantwortlichen, aber nicht vom SOC, erkannt wurde, muss das zuständige SOC über die Sicherheitsereignisse und -vorfälle informiert werden und es ist zu erwarten, dass das zuständige SOC ausreichend Informationen bereitstellen wird, wie mit der Untersuchung fortgefahren wird.

Eine Veranschaulichung von einigen guten und schlechten Praktiken ist nachfolgend aufgelistet.

Beispiele von guter Forensik:

- Erzeugen von Snapshots von infizierten Containern und/oder virtuelle Maschinen mit allen relevanten Logs.
- Isolieren von betroffenen Workloads und sie vollständig isoliert halten (vollständige Netz- und Speichertrennung von der gesunden Umgebung) und warten auf weitere Anweisungen eines Sicherheitsexperten.

Beispiele von schlechter Forensik oder Zerstörung von forensischen Daten; solche Handlungen dürfen niemals passieren:

- Löschen von Containern und/oder virtuellen Maschinen, weil alles bereits protokolliert ist.
- Alles "normal" (wie es ist) weiterlaufen lassen, wenn das System infiziert/kompromittiert wird.

Falls diese Anforderung erfüllt ist, kann Anforderung 8 aus 3.63 („Betrieb in DT IT“) ausgelassen werden.

Motivation: Sicherheitsvorfälle müssen schnell und kompetent bearbeitet werden, um potenzielle Schäden für Unternehmen, Mitarbeiter und Kunden zu erkennen und abzuwenden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.66-81/5.0

11. Querverweise und Quellenangaben

Das vorliegende Dokument nimmt anteilig Bezug auf folgende Quellen:

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf>

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>

12. Glossar

Definitionen für Public-, Private-, Community- und Hybrid-Cloud, sowie für IaaS, PaaS und SaaS orientieren sich an den Ausführungen des NIST.

Public Cloud

Die Cloud-Infrastruktur wird für die offene Nutzung durch die Allgemeinheit bereitgestellt. Die Cloud-Infrastruktur kann sich im Besitz, in der Verwaltung und im Betrieb einer geschäftlichen, akademischen oder staatlichen Organisation oder einer Kombination aus diesen befinden. Die Cloud-Infrastruktur existiert innerhalb der Räumlichkeiten des Cloud-Anbieters.

Private Cloud

Die Cloud-Infrastruktur wird für die ausschließliche Nutzung durch eine einzelne Organisation bereitgestellt, die mehrere Verbraucher (z. B. Geschäftseinheiten) umfassen kann. Die Cloud-Infrastruktur kann sich im Besitz, in der Verwaltung und im Betrieb der Organisation, einer dritten Partei oder einer Kombination aus diesen befinden. Die Cloud-Infrastruktur kann dabei innerhalb oder außerhalb der Räumlichkeiten der Organisation existieren.

Community Cloud

Die Cloud-Infrastruktur wird für die ausschließliche Nutzung durch eine bestimmte Nutzergemeinschaft bereitgestellt, die sich wiederum aus Organisationen zusammensetzt, die gemeinsame Anliegen haben (z. B. Mission, Sicherheitsanforderungen, Richtlinien und Compliance-Erwägungen). Die Cloud-Infrastruktur kann sich im Besitz, in der Verwaltung und im Betrieb einer oder mehrerer Organisationen aus der Community, einer dritten Partei oder einer Kombination aus diesen befinden. Die Cloud-Infrastruktur kann dabei innerhalb oder außerhalb der Räumlichkeiten der beteiligten Organisationen existieren.

Hybrid Cloud

Die Cloud-Infrastruktur setzt sich aus zwei oder mehr unterschiedlichen Cloud-Infrastrukturen (Private, Community oder Public) zusammen, die weiterhin als autarke Entitäten auftreten, aber durch standardisierte oder proprietäre Techniken miteinander verbunden sind und es ermöglichen, Daten und Anwendungen untereinander zu portieren (z. B. Cloud-Bursting als Lastausgleich zwischen Clouds).

IaaS

Die bereitgestellte Leistung besteht aus Rechenkapazität, Speicherkapazität, Netz und anderen grundlegenden Computer-Ressourcen, auf deren Basis der Konsument beliebige Software bereitstellen und ausführen kann, einschließlich Betriebssysteme und Anwendungen. Der Konsument verwaltet oder kontrolliert nicht die zugrunde liegende Cloud-Infrastruktur, hat aber die Kontrolle über Betriebssysteme, Datenspeicher und bereitgestellte Anwendungen; sowie möglicherweise eingeschränkte Kontrolle über ausgewählte Netzkomponenten (z. B. Host-Firewalls).

PaaS

Die bereitgestellte Leistung besteht darin, dem Konsumenten zu ermöglichen, eigene oder erworbene Anwendungen in der Cloud-Infrastruktur bereitzustellen, die mittels Programmiersprachen, Bibliotheken, Diensten und Tools erzeugt wurden, die der Cloud-Anbieter unterstützt. Der Konsument verwaltet oder kontrolliert nicht die zugrunde liegende Cloud-Infrastruktur, einschließlich des Netzes, der Server, der Betriebssysteme oder der Datenspeicher, hat aber die Kontrolle über die bereitgestellten Anwendungen und möglicherweise auch über Konfigurationseinstellungen der Laufzeitumgebung, in der die Anwendungen ausgeführt werden.

SaaS

Die bereitgestellte Leistung besteht darin, dem Konsumenten vorgefertigte Anwendungen eines Anbieters bereitzustellen, die auf einer Cloud-Infrastruktur ausgeführt werden. Die Anwendungen sind von verschiedenen Client-Geräten aus ansprechbar, entweder über eine Thin-Client-Schnittstelle, wie etwa einem Webbrowser (z. B. webbasierte E-Mail), oder über eine Programmierschnittstelle. Der Konsument verwaltet oder kontrolliert nicht die zugrunde liegende Cloud-Infrastruktur, einschließlich des Netzes, der Server, der Betriebssysteme, der Datenspeicher oder der individuellen Anwendungsfunktionen; mit der möglichen Ausnahme zu einer eingeschränkten Kontrolle über benutzerspezifische Anwendungseinstellungen.

CSP steht für Cloud Service Provider. Beispiele für einen CSP sind Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP).

VPC steht für "Virtual Private Cloud" und ist eine virtuelle Netzumgebung innerhalb eines öffentlichen Cloud-Dienstes (z. B. AWS, Azure, GCP), die es Benutzern ermöglicht, ihre Cloud-Ressourcen in einem isolierten und privaten Netz bereitzustellen und zu verwalten.

VNET steht für "Virtual Network" und ist eine virtualisierte Netzinfrastruktur innerhalb der Azure-Cloudplattform. VNET ermöglicht es Benutzern, ihre isolierten Netzumgebungen zu erstellen und zu verwalten, IP-Adressbereiche zu definieren und den Datenverkehrsfluss zwischen Azure-Ressourcen und dem Internet oder lokalen Netzen zu steuern, um eine sichere und effiziente Kommunikation innerhalb der Azure-Cloudumgebung zu gewährleisten.

Persönliches Benutzerkonto ist ein Benutzerkonto, das von einer Person verwendet wird.

Technisches Benutzerkonto ist ein Benutzerkonto, das von einer Maschine verwendet wird. Es wird auch als M2M-Benutzerkonto (Machine-to-Machine) bezeichnet oder einfach als "service account". Es wird hauptsächlich in M2M-Kommunikations-Szenarien verwendet, in denen die Kommunikation zwischen zwei Maschinen hergestellt wird, normalerweise ohne menschliche Interaktion.

Der Begriff **Landing Zone** bezieht sich auf eine Konfiguration der Cloud-Umgebung, die typischerweise Sicherheits- und Compliance-Aspekte erfüllt, Identitäts- und Zugriffsmanagement, Vernetzung, Abrechnung, usw. Im Kontext dieses Dokuments kann die Landing Zone auch als ein Konzept betrachtet werden, das eine zentrale Verwaltung von Identitäten und Projekten innerhalb des Cloud Service Providers (CSP) für die gesamte DTAG-Gruppe erlaubt, sowie bestimmte Einschränkungen für alle Konten zu setzen (z. B. minimale Passwortlänge oder MFA-Durchsetzung) und verwendet werden kann, um eine zentrale Sicherheitsprotokollierung zu erzwingen, etc. In bestimmten SaaS-Cloud-Diensten wird der Begriff Landing Zone oft auch als Administrationsportal oder Administrations-Cloud-Konsole bezeichnet.