

Sicherheitsanforderung

Private Clouds

Deutsche Telekom Gruppe

Version	1.0
Datum	01.12.2021
Status	Freigegeben

Impressum

Herausgeber
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Deutschland

Dateiname	Dokumentennummer 3.86	Dokumententyp Sicherheitsanforderung
Version 1.0	Stand 01.12.2021	Status Freigegeben
Fachlicher Ansprechpartner Telekom Security psa.telekom.de	Gültigkeitsdauer 01.12.2021 - 30.11.2026	Freigegeben von Stefan Pütz, Leiter SEC-T-TST

Zusammenfassung

Ziel dieses Dokuments ist es, eine Sicherheitsgrundlage für die Architektur einer sicheren Private Cloud-Umgebung zu schaffen, speziell im Hinblick auf moderne cloud-native Workloads. Darüber hinaus ist dieses Dokument in Teilen für Cloud-Kunden bestimmt, die eben jene Cloud-Plattformen nutzen. Alle hier im Dokument aufgeführten Anforderungen sind für den modernen Cloud-Einsatz und Cloud-native Workloads gedacht und mit dem Zero-Trust-Ansatz kompatibel. Die Anforderungen decken verschiedene Größen von Cloud-Umgebungen und multiple Cloud-Angebotsmodelle ab. Der Schwerpunkt liegt jedoch auf den typischsten Anwendungsfällen, nämlich kleinen bis mittleren Cloud-Implementierungen mit IaaS-Angeboten. Die Anforderungen sind im Allgemeinen technologieunabhängig, aber wo immer möglich werden Verweise auf Open-Source-Lösungen gegeben.

Copyright © 2021 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.	Cloud-Subtypen	6
2.1.	Trennung von Cloud-Funktionen	6
2.2.	Verwaltung und Orchestrierung der Cloud-Infrastruktur	8
2.3.	Große und kleine Cloud-Installationen	9
2.4.	Undercloud und Overcloud	9
3.	Cloud-Infrastruktur-Netzwerk und Cloud-Management	10
3.1.	Cloud-APIs	13
3.2.	Rund um das Cloud Management	15
4.	Anforderungen für Bare Metal	26
4.1.	Bare Metal as a Service	26
4.2.	PCI-Passthrough	27
4.3.	SR-IOV	28
5.	Hypervisor und Server	31
5.1.	Allgemeine Serveranforderungen	31
5.2.	Hypervisor-Trennung	33
5.3.	Hypervisor-Schutz	35
6.	Speicherung	39
6.1.	Trennung der Speicherung	39
6.2.	Speicherverschlüsselung	39
6.3.	Zugang zum Speicher	41
7.	Overlay-Netzwerk	43
7.1.	Allgemeine Anforderungen an das Overlay-Netz	44
8.	Cloud-Nutzung	46
8.1.	Zweckgebundene Trennung der Cloud-Infrastruktur	46
8.2.	Trennung von Systemen/Anwendungen, die in der Cloud laufen	47
8.3.	Mandantenspezifisch	49
9.	Referenzen	52
10.	Glossar	53

1. Einleitung

Laut NIST (National Institute of Standards and Technology) ist Cloud Computing ein Modell für den allgegenwärtigen, bequemen und bedarfsgerechten Netzzugang zu einem gemeinsam genutzten Pool konfigurierbarer Rechenressourcen (z.B. Netzwerke, Server, Speicher, Anwendungen und Dienste), die mit minimalem Verwaltungsaufwand und ohne Interaktion mit dem Dienstanbieter schnell bereitgestellt und zur Verfügung gestellt werden können. Dieses Cloud-Modell besteht aus fünf wesentlichen Merkmalen, drei Dienstmodellen und vier Bereitstellungsmodellen.

Eine private Cloud-Installation ist eine Reihe von Hardwareressourcen wie Server, Switches, Router, Firewalls und möglicherweise externe Speicherkomponenten, die von einer Automatisierungssoftware gesteuert werden. Diese ermöglichen eine programmierbare Nutzung der verfügbaren Ressourcen.

Umfang

Dieses Dokument behandelt die folgenden Themen:

- Sicherheitsanforderungen für Cloud-Infrastrukturen, einschließlich Rechen-, Speicher- und Netzressourcen (auch für PaaS und SaaS)
- Sicherheitsanforderungen für Cloud-Management und Orchestrierung
- Sicherheitsanforderungen für Mandanten (Cloud-Nutzer)

für die folgenden Arten von Cloud-Umgebungen:

- Private Cloud-Installationen, die der DTAG gehören und von ihr für interne Arbeitslasten betrieben (oder kontrolliert) werden, wobei die Arbeitslasten ebenfalls von der DTAG betrieben (oder kontrolliert) werden (d. h. kein direktes Serviceangebot für Nicht-DTAG-Mitarbeiter), unabhängig von der Größe (zentrale "große" Cloud-Umgebungen oder "kleine" Edge-Cloud-Umgebungen)

Die folgenden Cloudtypen werden in diesem Dokument nicht behandelt:

- Public Cloud

Software im Geltungsbereich dieses Dokuments:

- OpenStack
- VMWare Cloud
- Andere Lösungen, die den oben Erwähnten ähnlich sind

Software außerhalb des Geltungsbereichs dieses Dokuments:

- Docker
- Kubernetes
- Andere Containertechnologien

Vorabklärungen

Der Begriff Knoten wird oft als synonym für Server verwendet.

Die Begriffe "Server" oder "Knoten" beziehen sich in der Regel auch auf mehrere physische Server. Dennoch wurde im Text aus Gründen der Klarheit der Singular verwendet.

Die meisten in diesem Dokument angeführten Umsetzungsbeispiele beziehen sich auf OpenStack, da dies die Open-Source Cloud-Lösung ist, die weitesten verbreitet und deren gesamte Dokumentation öffentlich zugänglich ist.

Wie in der Cloud-Welt (*aaS-Welt) üblich, bezieht sich das Wort Dienst meist auf den Cloud-Dienst, der vom Cloud Provider für dessen Kunden angeboten wird. Manchmal wird der Begriff Dienst jedoch auch für einen internen Dienst als allgemeines Stück Software verwendet, das auf dem Server läuft (z. B. ein Daemon). Die Begriffe Funktion und Merkmal bezeichnen notwendige Funktionen der Cloud oder des Cloud-Dienstes.

2. Cloud-Subtypen

Im nächsten Teil werden die folgenden Begriffe häufig verwendet:

- (normale) Cloud: Cloud, in der jeder Server genau einen Dienstyp ausführt (d. h. der Server führt eine Rechen-, Speicher-, Netzwerk- oder Cloud-Managementfunktion aus)
- Konvergente Clouds sind Clouds, bei denen mehr als eine Funktion der Cloud auf demselben physischen Server läuft (Beispiel: kombinierter Rechen- und Speicherserver)
- hyperkonvergente Clouds sind konvergente Clouds, bei denen Cloud-Managementfunktionen neben den Cloud-Funktionen für die Mandanten ausgeführt werden (Beispiel für OpenStack: OpenStack-Kontrolldienste wie Keystone und Glance laufen auf dem/den gleichen Server(n) mit Speicher und/oder virtuellen Maschinen der Mandanten)

2.1. Trennung von Cloud-Funktionen

Req 1	Ein physischer Server darf nicht mehr als eine Art von Cloud-Funktion ausführen.
-------	--

Cloud-Funktionen, die für Cloud-Management, Rechen-, Speicher- und Netzwerkfunktionen verwendet werden, müssen auf unterschiedlichen physischen Servern laufen. Bei konvergenten und hyperkonvergenten Cloud-Umgebungen ist es zulässig, mehrere Cloud-Funktionen auf demselben physischen Server zu mischen.

Motivation: Die physische Trennung verschiedener Cloud-Funktionen verringert das Risiko der Angriffsausbreitung und erhöht die Angriffserkennung, wenn sie mit anderen Sicherheitsmaßnahmen kombiniert wird. Cloud-Installationen sind in der Regel groß und jede Cloud-Funktion (Verwaltung, Datenverarbeitung, Speicherung und Vernetzung) erfordert aufgrund ihres Umfangs manchmal selbst mehr als einen physischen Server. Der Begriff Management-Cloud-Funktionen wird manchmal auch als Steuerungsebene bezeichnet, während Rechen-, Speicher- und Netzwerkfunktionen manchmal als Datenebene bezeichnet werden. Diese Art der Trennung verbessert auch die Verfügbarkeit, da ein Ausfall eines einzelnen Servers weniger Cloud-Funktionen beeinträchtigt.

Umsetzungsbeispiel: Installation dieser Funktionen auf separaten physischen Servern (oder physischen Servergruppen):

- Verwaltung von Cloud-Funktionen (MySQL, Keystone, Glance API, Nova API, ...)
- Storage-Cloud-Funktionen (OpenStack Swift)
- Rechenleistung (Nova Compute, KVM, OpenVSwitch)
- Netzwerk (Neutron)

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Verfügbarkeit

ID: 3.86-1/1.0

Req 2	In konvergenten Clouds muss jede Cloud-Funktion in einer separaten virtuellen Maschine ausgeführt werden.
-------	---

Cloud-Funktionen, die für die Cloud-Verwaltung, Speicher- und Netzwerkfunktionen verwendet werden, müssen in separaten virtuellen Maschinen ausgeführt werden. Das Mischen mehrerer Cloud-Funktionen in derselben virtuellen Maschine ist nur für hyperkonvergente Cloud-Umgebungen mit Einschränkungen zulässig.

Kunden dürfen unter keinen Umständen direkt mit Ressourcen arbeiten können, die nicht innerhalb von VMs laufen. Zum Beispiel darf ein Objektspeicher-Gateway nicht auf Bare Metal gehostet werden, auf dem andere Cloud-Funktionen laufen, wenn keine Virtualisierung vorhanden ist.

Es gibt keine genaue Definition für konvergente Clouds. In der Regel können alle Clouds, die bis zu einem Dutzend Server haben, in diese Kategorie fallen (–manchmal auch als Ein-Rack-Implementierungen bezeichnet).

Motivation: Die Trennung verschiedener Cloud-Funktionen auf Ebene des Hypervisors kann nicht so effektiv sein wie die physische Trennung, bietet aber dennoch ein angemessenes Maß an Risikominderung bei der Angriffsausbreitung und erhöht die Chancen der Angriffserkennung.

Umsetzungsbeispiel: Bei einer typischen konvergenten Cloud-Konfiguration werden Speicher- und Rechenfunktionen auf denselben physischen Rechnern gemischt. In diesem Fall erfordern die Speicherfunktionen ein höheres Maß an Schutz, so dass die Verschlüsselung der Daten im Ruhezustand und bei der Übertragung für alle Speicherfunktionen verpflichtend ist. Container werden im Allgemeinen nicht als ausreichend angesehen, obwohl in einigen spezifischen Fällen andere Sicherheitsmaßnahmen das Fehlen einer hardwarebasierten Virtualisierung ausgleichen können.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-2/1.0

Req 3	In hyperkonvergenten Clouds muss jede Cloud-Funktion logisch getrennt sein und für jede Funktion unterschiedliche Verschlüsselungsschlüssel verwenden. Die Schlüssel dürfen nicht auf den für die Cloud-Umgebung verwendeten Maschinen gespeichert werden.
-------	--

Für hyperkonvergente Clouds sind möglicherweise zusätzliche Sicherheitsmaßnahmen erforderlich, einschließlich Systeme zur Erkennung und Verhinderung von Eindringlingen (IDS, IPS).

Obwohl es keine strenge Definition des Begriffs "hyperkonvergente Cloud" gibt, gilt dieser Begriff für sehr kleine Cloud-Installationen, bei denen eine Erweiterung um zusätzliche Server nicht vorgesehen ist (z. B. bis zu 5 Server). Damit fallen auch Edge-Cloud-Installationen in diese Kategorie, die nur einen Mandanten hosten.

Motivation: Ein Angreifer könnte sich zwar Zugang zu Daten verschaffen, wäre aber nicht in der Lage, etwas mit den Daten anderer virtueller Maschinen, einschließlich derer der Cloud-Kontrollfunktionen, anzustellen. Ein direkter Angriff auf andere Maschinen wäre leichter zu erkennen, wenn geeignete Sicherheitsmaßnahmen auf Hypervisoren und innerhalb virtueller Maschinen angewendet werden.

Umsetzungsbeispiel: Die Trennung von Cloud-Funktionen in hyperkonvergenten Clouds ist in der Regel möglich, indem verschiedene Arten von Cloud-Funktionen in separaten virtuellen Maschinen ausgeführt werden. Jede Cloud-Funktion (und virtuelle Maschine) muss ihren eigenen Verschlüsselungsschlüssel für die Datenspeicherung verwenden. Darüber hinaus muss ein Schlüsselverwaltungssystem vorhanden sein und der Prozess muss so gestaltet werden, dass gewährleistet ist, dass eine virtuelle Maschine nur ihren eigenen, für die Laufzeit erforderlichen Schlüssel abrufen kann.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

2.2. Verwaltung und Orchestrierung der Cloud-Infrastruktur

In einigen Fällen können mehrere Cloud-Umgebungen (Rechenzentren) zu einer großen Cloud zusammengeschlossen werden. In einem solchen Fall ist ein sogenanntes Umbrella-Management erforderlich, das an einem oder mehreren sicheren Standorten untergebracht werden muss, z. B. einem oder mehreren TMDC-Standorten, wobei ein Standort ausreicht, aber aus Redundanzgründen mehrere empfohlen werden. Die Standorte selbst müssen über ein sicheres Netz verbunden sein z. B. kann ein DCN verwendet werden, während VPN über das Internet zulässig, aber nicht empfehlenswert ist, da keine garantierte Verfügbarkeit besteht.

Wird nur der Verbund zwischen Cloud-Umgebungen genutzt, muss die Konnektivität zwischen den Verwaltungssystemen aller Cloud-Umgebungen entsprechend gesichert werden.

Req 4	Zentrale Cloud-Management-Systeme müssen an sicheren Standorten untergebracht und über ein sicheres Netz verbunden sein.
-------	--

Das Hosting zentraler Verwaltungssysteme an sicheren Standorten und die Verbindung von Cloud-Umgebungen mit dem zentralen Cloud-Verwaltungssystem über ein sicheres Netzwerk ermöglichen einen besseren Schutz und eine höhere Verfügbarkeit.

Der Begriff "sicheres Netz" lässt sich hier am besten als ein Netz mit Verschlüsselung und geeigneter Sicherheitsfilterung beschreiben. Eine Implementierung dafür könnte ein VPN oder eine Reihe von Tunneln (oder Zugangslisten und Firewalls) mit Verschlüsselung und Überprüfung von Clients und Servern durch Zertifikate sein.

Motivation: Wenn eine zentrale Cloud-Verwaltung verwendet wird, kann ein Angriff viel verheerender sein, da ein Eindringen in das zentrale Verwaltungssystem ausreichen könnte, um alle Cloud-Umgebungen zu gefährden.

Umsetzungsbeispiel: Beispiele für zentralisierte Systeme, die in vielen Cloud-Umgebungen verwendet werden, sind KMS (Key Management System) und zentrale Identitätsanbieter.

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-4/1.0

Req 5	Im Falle eines zentralen Cloud-Managements müssen kritische und lokal benötigte Funktionen in jeder Cloud-Umgebung gehostet werden.
-------	---

Alle Funktionen, die für die Funktionalität einer bestimmten Cloud-Umgebung entscheidend sind, müssen lokal in dieser Cloud-Umgebung gehostet werden, um das Risiko zu mindern, dass die Verwaltbarkeit aller Cloud-Umgebungen durch den Ausfall des zentralen Cloud-Management-Systems verloren geht.

Motivation: Wenn wichtige Funktionen nicht lokal gehostet werden, könnte ein entfernter Standort seinen Betrieb einstellen, falls die Verbindung zur zentralen Cloud-Verwaltung vorübergehend unterbrochen wird.

Umsetzungsbeispiel: Einige Beispiele für solche wichtigen Funktionen sind Keystone, Glance und Netzwerk-Boot-Server.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-5/1.0

2.3. Große und kleine Cloud-Installationen

Während bei größeren Cloud-Installationen (an zentralen Standorten) nicht davon ausgegangen wird, dass sie hyperkonvergent sind, sind konvergente Szenarien von Fall zu Fall zu prüfen. Extrem kleine Cloud-Installationen, die in der Regel als Edge Clouds bezeichnet werden (Beispiel: < 5 Server), können das hyperkonvergente Konzept nutzen. Die entsprechenden Sicherheitsmerkmale müssen von Fall zu Fall angepasst werden, abhängig von vielen Faktoren, einschließlich der physischen Sicherheit des Standorts, an dem sich die Cloud befindet.

2.4. Undercloud und Overcloud

Einige Cloud-Anbieter stellen die Cloud-Plattform in Form von zwei Cloud-Umgebungen bereit, wobei eine kleine Cloud für die Bereitstellung einer größeren Cloud verwendet wird, die wiederum von echten Cloud-Kunden genutzt wird. Mit diesem Ansatz soll die Menge an Technologien und Software, die für die Wartung der gesamten Cloud-Plattform erforderlich ist, minimiert werden. Ein bemerkenswertes Beispiel ist OpenStack von RedHat.

Undercloud ist eine minimalistische OpenStack-Installation auf einer einzigen oder wenigen Maschinen, die den Rest der verfügbaren Hardware als eigene Cloud behandelt.

Overcloud besteht aus dem Rest der Hardware mit einer separaten OpenStack-Installation (die vollständig durch die Undercloud verwaltet wird). Alle Server der Overcloud (alle OpenStack-Kontroll-, Rechen- oder Speicherknoten der Overcloud) werden in der Undercloud als Rechenknoten (Bare Metal) behandelt.

Daraus ergibt sich die Notwendigkeit, dass die Undercloud vollen administrativen M2M-Zugriff auf alle Maschinen in der Overcloud hat, damit sie ohne menschliche Interaktion verwaltet werden können. Es ist typisch, dass Undercloud-Verwaltungsknoten über passwortlose und nicht-interaktive SSH-Verbindungen auf alle Overcloud-Maschinen zugreifen können (entweder als Root-Benutzer oder als normaler Benutzer, der passwortlose sudo-Rechte hat). In solchen Fällen sind einige Sicherheitsanforderungen aus diesem Dokument, die sich auf die Kontrolle des Zugriffs auf die Overcloud-Hardware durch die obligatorische Verwendung von zentralem IAM beziehen, nicht notwendig, da alle Benutzer zunächst die Undercloud durchlaufen müssen.

3. Cloud-Infrastruktur-Netzwerk und Cloud-Management

Das Cloud-Infrastrukturnetz (auch Underlay-Netz genannt) der Cloud ist das interne Cloud-Netz, das für die IP-Konnektivität zwischen allen Hardware-Komponenten und der Cloud-Software erforderlich ist, einschließlich:

- Rechenknoten
- Storage-Knoten
- Netzwerkknoten
- Serververwaltung (BMC - Basedboard Management Controller, z. B. IPMI oder Redfish)
- Netzwerkgeräte (Switches, Router, Firewalls, ...)
- Cloud-Management-Funktionen

Dies gilt nicht für Mandanten-Netzwerke.

Req 6	Die Konnektivität zwischen dem Cloud-Infrastrukturnetz und externen Netzen muss über Geräte mit zustandsabhängiger L3/L4-Filterung hergestellt werden.
-------	--

Das Gerät (Router, L3-Switch, Firewall, Server) ist in diesem Zusammenhang funktionell eine Firewall mit zustandsabhängiger L3/L4-Filterung. Dieses Gerät stellt die Demarkationslinie zwischen Verteilungsnetz und Cloud-Infrastruktur dar. Der größte Teil des Datenverkehrs für die Cloud-Infrastruktur wird innerhalb der Cloud-Umgebung abgewickelt. Dieses Gerät muss eine grobe Filterung (Zugriffskontrolllisten - ACLs) implementieren, um von außen kommenden böswilligen Datenverkehr zu blockieren und den ausgehenden Datenverkehr zu kontrollieren; es wird jedoch nicht erwartet, dass dieses Gerät auch den Verkehr der einzelnen Mandanten kontrolliert.

Die Verwaltungsfunktionen der Cloud-Infrastruktur müssen vor Datenverkehr von außen geschützt werden. Nur ein minimaler Satz von Cloud-Infrastrukturkomponenten muss von außen zugänglich sein.

Motivation: Die Kontrolle des ein- und ausgehenden Datenverkehrs kann Versuche der Datenextraktion verhindern, wenn einige Komponenten der Cloud kompromittiert werden.

Umsetzungsbeispiel: Beispiele für Cloud-Infrastrukturkomponenten, die normalerweise nicht von außen zugänglich sein müssen:

- Verbindungen zu BMC-Schnittstellen (IPMI/Redfish) von Servern von außen sind nicht zulässig.
- eine direkte Verbindung von außen zum internen Speichernetz der Cloud ist nicht zulässig
- Der Zugang zu den notwendigen Cloud-APIs ist erlaubt, erfordert aber dennoch zusätzliche Kontrollen, wie WAF (Web Application Firewall)

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-6/1.0

Req 7	Cloud-Infrastrukturnetze der Cloud-Infrastruktur dürfen von externen und Mandanten-(Overlay-)Netzen nicht direkt erreichbar sein.
-------	---

Im weitesten Sinne ist eine direkte IP-Konnektivität von externen Netzen oder Mandanten-(Overlay-)Netzen zur Cloud-Infrastruktur nicht zulässig.

Dies ist eine Erweiterung der vorhergehenden Anforderung mit demselben Ziel.

Motivation: Die Kontrolle des ein- und ausgehenden Datenverkehrs kann Versuche der Datenextraktion verhindern, wenn einige Komponenten der Cloud kompromittiert werden.

Umsetzungsbeispiel: Der Zugriff auf interne Systeme einer Cloud-Infrastruktur muss kontrolliert und geschützt über andere Sicherheitseinrichtungen wie Firewalls auf höherer Ebene, WAFs (Web Application Firewalls) oder Proxys (natürlich nicht transparent) erfolgen.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-7/1.0

Req 8	Die verschiedenen Verkehrsarten in der Cloud-Infrastruktur müssen in speziellen logischen oder physischen Netzen voneinander getrennt werden.
-------	---

Mindestens die folgenden Verkehrsarten müssen in der Cloud-Infrastruktur durch eine logische (z. B. VLAN) oder physische Trennung getrennt werden:

- Produktionsverkehr (Netzverkehr von Mandanten)
- Infrastrukturmanagement und Orchestrierung (Verwaltung und Orchestrierung der Cloud selbst)
- regulärer Speicherverkehr (zwischen Speicher- und Rechenknoten)
- Replikation des internen Speicherverkehrs (zwischen Speicherknoten, im Falle von Ceph als Replikationsnetzwerk bezeichnet)
- BMC-Netzwerk (Serververwaltung über dedizierten IPMI/Redfish-Anschluss)
- allgemeiner Geräteverwaltungsdatenverkehr (hauptsächlich Switch- und Router-Verwaltung)

Wenn Bare Metal as a Service (BMaaS) angeboten wird, ist eine weitere Trennung des Datenverkehrs erforderlich.

Die aufgelisteten Verkehrsarten unterscheiden sich stark in Bezug auf ihre Funktionalität, Leistungs-/Verfügbarkeitsanforderungen und Schutzniveaus.

Motivation: Die Trennung der verschiedenen Verkehrsarten würde einen Angreifer daran hindern, weiter vorzudringen, und könnte gleichzeitig die Erkennungsmöglichkeiten verbessern, wenn andere Sicherheitsmaßnahmen angemessen eingesetzt werden.

Umsetzungsbeispiel: Zusätzlich zu den aufgelisteten Verkehrsarten, die getrennt werden müssen, ermöglicht die Priorisierung bestimmter Verkehrsarten (Beispiel: höhere Priorität für Infrastrukturmanagement- und Orchestrierungsverkehr gegenüber Produktions-/Nutzerverkehr) auch eine einfachere Handhabung von Überlastungen, die das Ergebnis von ([D]DoS-)Angriffen oder fehlerhaltender Kunden-Workloads sind.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

Req 9	Wenn es kein Out-of-Band-Verwaltungsnetz gibt, müssen der Infrastrukturverwaltungsdatenverkehr, der Orchestrierungsdatenverkehr, der BMC-Datenverkehr und der allgemeine Geräteverwaltungsdatenverkehr eine höhere Priorität haben, um die Erreichbarkeit und Verwaltbarkeit der Cloud-Infrastruktur im Falle einer Netzüberlastung zu gewährleisten.
-------	---

Die Priorisierung des Datenverkehrs in diesen Netzen muss an allen erforderlichen Stellen erfolgen. Dies gilt für alle Geräte (netzbezogen oder Server), die im Überbelegungsmodus arbeiten - was in Cloud-Umgebungen sehr häufig der Fall ist.

Motivation: Die Verwaltbarkeit der Cloud-Infrastruktur hat in einer Cloud-Umgebung höchste Priorität. In Überlastungsfällen (verursacht durch Bugs, Fehler, regelmäßige Netzüberlastung oder [D]DoS-Angriffe) ermöglicht eine verwaltbare Infrastruktur die Fehlersuche, Vorfallsanalyse, Entschärfung und Beseitigung der Grundursachen, was wiederum die Wiederherstellung der in der Cloud laufenden Arbeitslasten ermöglicht.

Umsetzungsbeispiel: Priorisierung des Datenverkehrs entweder durch QoS oder durch Ratenlimits (oder beides).

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-9/1.0

Req 10	Die Verwaltungsdienste und -systeme der Cloud-Infrastruktur müssen durch MFA für den menschlichen Zugang geschützt sein.
--------	--

Die Implementierung von MFA (mindestens 2FA) zur Authentifizierung ist für die Verwaltung hochsensibler Infrastrukturen obligatorisch.

Außerdem ist es erwähnenswert, dass ein direkter Zugriff auf die Verwaltungssysteme der Cloud-Umgebung oder einen anderen Teil der Cloud-Infrastruktur im Allgemeinen nicht zulässig ist. Es ist üblich, dass die Cloud über M2M-Konten von einem zentralen Punkt aus verwaltet wird (z. B. Ansible-Server).

Wenn MFA aufgrund der gewählten Technologie nicht möglich ist, muss ein Jump-Host vorgeschaltet werden, der sich mit den AAA-Aspekten menschlicher Nutzer befasst, einschließlich MFA.

(Diese Anforderung steht nicht im Widerspruch zur Existenz von Notzugangskonten, die auch als "break glass accounts" bezeichnet werden).

Motivation: Die Authentifizierung über nur einen Faktor wird für die Verwaltung hochsensibler Infrastrukturen als nicht ausreichend angesehen.

Umsetzungsbeispiel: Verwendung von MFA wie TOTP (Time-based One-Time Password) oder hardwarebasierte Geräte.

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-10/1.0

Req 11	Die Verwaltungsdienste der Cloud-Infrastruktur müssen durch eine gegenseitige starke Authentifizierung für Machine-to-Machine (M2M)-Konten geschützt sein.
--------	--

Als Äquivalent zur MFA für menschliche Nutzer muss eine starke Authentifizierung für Maschine-zu-Maschine-Nutzer implementiert werden. Dies umfasst in der Regel die Authentifizierung beider Parteien in der Kommunikation.

Motivation: Die Authentifizierung über einfache M2M-Authentifizierung (z. B. einfache Token) wird für die Verwaltung hochsensibler Infrastrukturen als nicht ausreichend angesehen.

Umsetzungsbeispiel: Ein mögliches Beispiel könnte sein:

- Server, der seine Authentizität durch ein Zertifikat nachweist
- Client, der ein Zertifikat oder Token verwendet, das nachgewiesen werden kann und dessen maximale Lebensdauer auf einen ausreichend kurzen Zeitraum festgelegt 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
- Unbemerkt durchführbare Angriffe

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-11/1.0

3.1. Cloud-APIs

Req 12	Der Zugang zu Cloud-API-Endpunkten muss durch Firewalls oder Proxys auf höherer Ebene kontrolliert und geschützt werden, und zwar sowohl für den Zugang von externen Netzen als auch von Mandanten. Die Kommunikation muss verschlüsselt sein. Authentifizierung ist obligatorisch.
--------	---

Gemäß der Anforderung, dass keine direkte IP-Konnektivität von externen Netzen und Tenant-Netzen zu Cloud-API-Endpunkten bestehen darf, wäre der Zugang für Verwaltungsfunktionen von in der Cloud laufenden Anwendungen und für externe Personen und/oder Maschinen erforderlich. Der Zugang zu Cloud-API-Endpunkten muss über Firewalls auf höherer Ebene (über L4 - TCP), WAFs oder Proxys erfolgen.

Die Kommunikation von Endkunden (sowohl von externen als auch von Mandanten-Netzwerken) zur Firewall/WAF/zum Proxy und von der Firewall/WAF/dem Proxy zu den exponierten Cloud-API-Endpunkten muss verschlüsselt werden, einschließlich der Überprüfung von Zertifikaten in beide Richtungen, um Man-in-the-Middle-Angriffe zu verhindern. Interne Cloud-APIs müssen für die Mandanten natürlich nicht erreichbar sein.

Neben allen regulären APIs gilt dies auch für Nova Metadata Server. In typischen modernen Open-Stack-Implementierungen gibt es einen Nova-Metadaten-Proxy, der diese Anforderung für Nova-Metadaten-Server erfüllt. Derzeit gibt es keine Verschlüsselung für Nova-Metadaten, so dass dieser Endpunkt nicht verschlüsselt werden muss.

Für webbasierte Benutzeroberflächen (z. B. Dashboards) müssen spezielle Webanwendungsschecks verwendet werden.

Für den Zugang zu allen API-Endpunkten muss eine starke Authentifizierung verwendet werden, entsprechend den bestehenden Sicherheitsanforderungen für Webanwendungen und Webdienste (z. B. Dokument 3.02 - "Web Services").

Motivation: Cloud-API-Endpunkte haben eine große Angriffsfläche mit geringem eingebautem Schutz gegen unerwartete Eingaben und potenziell großen Auswirkungen, wenn sie verletzt werden.

Umsetzungsbeispiel: Die Sicherung von Cloud-APIs mit Proxys, die Begrenzung von API-Anfragen (einschließlich der Beschränkung möglicher API-Aufrufe auf das Notwendigste) und die Filterung von Eingaben sind entscheidend, um mögliche Angriffe über Cloud-APIs zu verhindern. Firewalls, WAFs und Proxys können mit Protokollierung und Überwachung integriert werden, so dass Angriffe frühzeitig erkannt und angemessen abgewehrt werden.

In einigen sehr speziellen Anwendungsfällen, in denen APIs nicht ordnungsgemäß gesichert werden können, während es nur eine sehr kleine Anzahl interner Mandanten gibt, kann eine weitere zusätzliche Maßnahme eingesetzt werden - das Verstecken von API-Endpunkten hinter Jump-Hosts, vorausgesetzt, die Anwendungsfälle der Mandanten lassen dies zu. Dann wäre der Zugriff auf Cloud-API-Endpunkte für den Tenant nur von Jump-Hosts aus möglich, wobei jeder Tenant einen Jump-Host erhalten könnte, der bei der Erstellung des Tenants erstellt 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
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-12/1.0

Req 13	Der Zugang zu Verwaltungsschnittstellen, APIs, Dashboards und Systemen muss durch Firewalls oder Proxys auf höherer Ebene kontrolliert und geschützt werden (vorzugsweise versteckt hinter einem Jump Host), während die Kommunikation verschlüsselt sein muss.
--------	---

Die vorherige Anforderung an die Sicherheit von Cloud-APIs gilt auch für alle unterstützenden Systeme, die von den Verwaltern der Cloud-Infrastruktur verwendet werden.

Motivation: Cloud-API-Endpunkte haben eine große Angriffsfläche mit relativ geringem eingebautem Schutz gegen unerwartete Eingaben und potenziell großen Auswirkungen, wenn sie verletzt werden.

Umsetzungsbeispiel: Es wird bevorzugt, dass die gesamte administrative Kommunikation über den Jump-Host abgewickelt wird. Wenn ein Ansatz mit Jump Host nicht möglich ist, können strenge VPN oder ACLs verwendet werden, um den Zugriff auf administrative Cloud-Schnittstellen, APIs, Dashboards usw. nur für Cloud-Administratoren zu beschränken.

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
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-13/1.0

Req 14	Zugriffe auf APIs und Web-UIs, die Mandanten und Anwendungen angeboten werden, müssen auf das notwendige Minimum beschränkt werden.
--------	---

Man kann den administrativen Zugriff filtern und ihn von den API-Anfragen der normalen Benutzer auf WAF / Reverse Proxy trennen, wo nur bestimmte APIs erlaubt sind.

Motivation: APIs und Web-UIs (wie Dashboards) bieten sowohl administrative als auch normale Benutzerfunktionen. Wenn den Mandanten in APIs nur Funktionen für normale Benutzer zur Verfügung gestellt werden, haben sie keine Möglichkeit, im Falle eines Verstoßes oder einer Eskalation der Rechte administrative Funktionen auszuführen.

Umsetzungsbeispiel: Die WAF-Regeln sollten auf der Grundlage der Dokumentation erstellt werden (z. B. können `https://service/admin/*`-Links für den regulären Mandantenzugriff verboten werden), aber in Fällen, in denen die Dokumentation und die APIs nicht einfach genug sind, können Regeln mithilfe des Lernmodus erstellt 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
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-14/1.0

3.2. Rund um das Cloud Management

Eine Cloud-Umgebung erfordert eine Vielzahl anderer Systeme, die für den sicheren Betrieb der Cloud-Umgebung vorhanden sein müssen. Die meisten dieser Systeme (z. B. Protokollierung, Überwachung, Authentifizierung usw.) sind gut bekannt und werden in anderen Sicherheitsdokumenten ausführlich behandelt.

Bei der Vorbereitung, der Konfiguration, der Installation und dem Betrieb von Cloud-Infrastrukturen gilt es, die grundlegenden Prinzipien zu wiederholen:

- die Angriffsfläche von Systemen und Diensten muss begrenzt werden
- die Systeme müssen dem Prinzip der minimalen Installation folgen
- alle sensiblen Daten müssen während der Übertragung und Speicherung (und wenn möglich auch während der Nutzung) verschlüsselt werden
- die Berechtigungen der Benutzer (Menschen und M2M) müssen dem Least-Privilege Prinzip folgen
- die Kommunikationspartner müssen angemessen authentifiziert und autorisiert sein
- die Systeme müssen entsprechend ihrer Vertraulichkeitsstufe getrennt werden
- die eingehende, ausgehende und interne Kommunikation muss kontrolliert und gefiltert werden
- Infrastruktur, Systeme und Dienste müssen überwacht und regelmäßig getestet werden
- die Systeme müssen regelmäßig aktualisiert und gepatcht werden
- ein Verfahren für das Management von Zwischenfällen muss vorhanden sein

Req 15	Es muss ein interner vertrauenswürdiger Softwarespeicher vorhanden sein und dieser muss verwendet werden.
--------	---

Das Repository darf nicht über das Internet zugänglich sein, und die ursprünglich aus dem Internet heruntergeladenen Anbieterpakete müssen auf bekannte Malware und Schwachstellen gescannt werden, bevor sie dem Rest der Cloud-Infrastruktur zur Verfügung gestellt werden. Das Repository muss in Bezug auf die Netzwerkerreichbarkeit geschützt sein (damit nur die erforderlichen Systeme auf das Repository zugreifen können) und die Authentizität muss mit einem HTTPS-Zertifikat überprüft werden. Die Pakete selbst müssen signiert sein.

Cloud-Infrastrukturen dürfen nicht direkt die im Internet gehosteten Repositories von Anbietern nutzen. Bei einem internen Repository benötigen die Cloud-Verwaltungssysteme keinen Zugang zum Internet. Dies gilt insbesondere für bestimmte Cloud-Software, die manchmal PyPI (Python Package Index) oder ähnliche Repositories für die Installation und Aktualisierung benötigt.

Das Repository muss regelmäßig aktualisiert werden und aktuelle Patches enthalten, um das Patching-Verfahren zu unterstützen.

Motivation: Softwarepakete für die Cloud-Umgebung stammen aus verschiedenen Quellen (z. B. Linux-Distribution, OpenStack, SDN, GitHub, ...) und können kompromittiert werden. Um die Bedrohung zu verringern, muss für die Bereitstellung von Software für die Cloud-Infrastruktur und die Verwaltungssysteme ein internes Repository verwendet werden, dessen Betrieb intern erfolgt.

Umsetzungsbeispiel: Intern gehosteter Satellite-Server für RedHat-basierte Distributionen oder apt-mirror für Debian/Ubuntu-basierte Distributionen.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-15/1.0

Req 16	Die Integrität von Softwarepaketen muss nach der Übermittlung und vor ihrer Installation oder Verwendung überprüft werden.
--------	--

Es muss ein geeigneter Algorithmus verwendet werden, um die Integrität von Softwarepaketen nach der Übertragung (z. B. nach dem Herunterladen) und unmittelbar vor der Installation oder Verwendung (falls keine Installation, sondern nur eine Ausführung erforderlich ist) zu überprüfen. Im Falle von Paketen, die von Drittentwicklern stammen, müssen nach Möglichkeit vom Entwickler signierte Pakete verwendet werden.

Motivation: Dadurch wird das Risiko einer Manipulation bei der Übertragung oder Installation verringert.

Umsetzungsbeispiel: Bei Linux-Paketen, die mit der Linux-Distribution geliefert werden, ist dies in der Regel in den Paketmanagern (DNF und RPM in RedHat-basierten Distributionen oder apt in Debian/Ubuntu-basierten Distributionen) standardmäßig aktiviert.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-16/1.0

Req 17	Es muss einen Patch-Management-Prozess für die gesamte Cloud-Umgebung geben.
--------	--

Der Patchmanagementprozess in einer Cloud-Umgebung muss so implementiert werden, dass das Patchen aller Cloud-Komponenten unter Einhaltung der SLA für die Mandanten möglich ist. Wenn die SLA dies erfordert, muss der Patching-Prozess so konzipiert sein, dass eine Live-Migration virtueller Maschinen für das Patching von Rechenknoten möglich ist, oder dass Cloud-Management-APIs während des Patchings zur Verfügung stehen, so dass die Mandanten in der Lage sind, Arbeitslasten, die von der Aktualisierung betroffen sind, neu zu planen. Bei anderen SLA-Typen könnte man sich auch dafür entscheiden, die gesamte Cloud-Umgebung auf einmal zu aktualisieren und alle Arbeitslasten neu zu starten.

Alle Komponenten der Cloud-Umgebung müssen in das Patch-Management-Verfahren einbezogen werden, z. B. Management, Orchestrierung, Rechen-, Speicher- und Netzwerkfunktionen. Alle unterstützenden Systeme (Überwachung, Protokollierung, Jump Hosts usw.) müssen ebenfalls in das Verfahren einbezogen werden.

Auch in solchen Fällen, in denen eine kurzfristige Korrektur erforderlich ist, muss das reguläre Prüfverfahren eingehalten werden.

Motivation: Da täglich neue Sicherheitslücken auftauchen, ist es notwendig, den Patching-Prozess so zu gestalten, dass er schnell durchgeführt werden kann.

Umsetzungsbeispiel: Das Patching-Verfahren sollte so gestaltet werden, dass das Patching aller Rechenknoten innerhalb von 24-48 Stunden nach Aufdeckung einer kritischen Sicherheitslücke und Verfügbarkeit eines Patches abgeschlossen werden kann.

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-17/1.0

Req 18	Die Firmware aller Geräte muss regelmäßig gepatcht werden. Besondere Aufmerksamkeit (häufigeres Patchen) ist für Geräte erforderlich, die von Mandanten direkt genutzt werden (entweder Bare-Metal-Server, PCIe-Passthrough-Geräte oder SR-IOV-Geräte).
--------	---

Firmware muss genauso behandelt werden, wie jede andere Software - sie muss regelmäßig gepatcht werden. Häufig fungiert der Hypervisor als Pufferzone zwischen einem Tenant Space und der Hardware. Es ist schwieriger, Schwachstellen in der Firmware auszunutzen, wenn ein Hypervisor dazwischen liegt. Die Verwendung eines Hypervisors kann nicht als Ersatz für Firmware-Patches angesehen werden, da neue Angriffe wie SPECTRE und Meltdown Patches für den Mikrocode und Abschwächungen für das Betriebssystem erfordern, um das Risiko erfolgreicher Angriffe zu verringern. Bei der Verwendung von Bare-Metal-Hardware (auch durch SR-IOV) bietet der Hypervisor keinen zusätzlichen Schutz, und das unverzügliche Patchen der Firmware ist die einzige Verteidigungslinie.

Es müssen geeignete Verfahren für rechtzeitige Firmware-Patches vorhanden sein, die alle Workload-Migrationen (live oder nicht-live) berücksichtigen.

Motivation: Heutzutage wird die Firmware der Geräte (BIOS, UEFI, PCIe-Karten, Festplatten, IPMI, ...) immer komplexer und enthält Bugs, die für Angriffe genutzt werden können (z.B. um das System zu übernehmen oder Daten von anderen Mandanten zu stehlen).

Umsetzungsbeispiel: Das Patching-Verfahren sollte so gestaltet werden, dass es möglich ist, CVEs mit hoher Punktzahl in etwa 24-48 Stunden zu patchen.

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-18/1.0

Req 19	Die Anpassung der Cloud-Infrastruktur darf von den Mandanten nicht verzögert oder blockiert werden (weder technisch noch administrativ).
--------	--

Es ist zwingend erforderlich, dass die SLA die Tatsache widerspiegelt, dass kein Mandant das Patchen der zugrunde liegenden Infrastruktur blockieren oder verhindern kann.

Kunden, die die Cloud unter der Annahme nutzen wollen, dass Patching oder andere Wartungsarbeiten durch sie verzögert oder blockiert werden kann, dürfen unter keinen Umständen auf die Cloud migrieren.

Motivation: Patching schützt alle anderen Workloads und die Cloud-Infrastruktur, und es wäre extrem unvernünftig und gefährlich, die Sicherheit der gesamten Cloud und aller anderen Systeme nur wegen eines Mandanten zu gefährden.

Umsetzungsbeispiel: Bei bestimmten Technologien und Arbeitslasten kann dies durch eine Live-Migration erreicht werden, und bei solchen, für die es keine technischen Möglichkeiten gibt, kann dies durch eine Klausel in den SLA-Bedingungen abgedeckt 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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-19/1.0

Req 20	Ein Schlüsselverwaltungssystem (Key Management System - KMS) muss vorhanden sein und für den Umgang mit Schlüsselmaterial verwendet werden.
--------	---

Die Verwaltung von Schlüsselmaterial spielt eine entscheidende Rolle bei der Sicherheit von Cloud-Systemen. Zu den Geheimnissen in diesem Sinne gehören:

- Schlüssel
- Passwörter
- Zertifikate

Hier finden Sie eine Liste von Anwendungsbeispielen für KMS:

- Speicherverschlüsselung
- Schlüsselverwaltung für SSH-Zugang
- Verschlüsselung der API-Kommunikation
- Verschlüsselung von Mandantendaten

- Bescheinigungen für Pächter
- geheime Verwaltung für Mandanten

Es ist praktisch unmöglich, eine sichere Cloud-Plattform oder sichere Tenant-Workloads in der Cloud ohne KMS zu betreiben. Das KMS kann als Teil der Cloud-Plattform oder separat bereitgestellt werden. Selbst wenn das KMS nicht als Teil der Cloud-Plattform bereitgestellt wird, ist es daher notwendig, dass das KMS erreichbar und auf automatisierte Weise nutzbar ist (wie andere Cloud-APIs).

Hinweis: Die Erfüllung dieser Anforderung ist eine Voraussetzung für die Erfüllung vieler anderer Anforderungen aus diesem Dokument.

Motivation: KMS ermöglicht die Erzeugung, Speicherung und Verteilung von Geheimnissen in einer Cloud-Umgebung. Würden Geheimnisse auf Systemen in der Cloud im Klartext gespeichert, könnten sie möglicherweise von unbefugten Benutzern eingesehen werden.

Umsetzungsbeispiel: Eine Lösung wie HashiCorp Vault kann als Teil der Cloud-Infrastruktur installiert 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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-20/1.0

Req 21	Eine geeignete Entropiequelle muss verfügbar sein und für die Erzeugung von Geheimnissen und kryptografischen Schlüsseln verwendet werden.
--------	--

Eine gute Entropie ist die erste Verteidigungslinie für die Schaffung guter Geheimnisse und kryptografischer Schlüssel. Es ist notwendig, einen hochwertigen Generator innerhalb der Cloud zu haben und ihn den Mandanten zur Verfügung zu stellen, damit sie ihn in ihren virtuellen Maschinen nutzen können. Die Nutzung von Entropie-Diensten, die von Drittanbietern bereitgestellt werden, ist nicht gestattet (z. B. Pollinate von Canonical).

Motivation: Schlüssel und Geheimnisse, die mit unzureichender Entropie generiert werden, können von Angreifern reproduziert bzw. mitgelesen werden, was es ihnen ermöglicht, die Sicherheit von Systemen in der Cloud oder sogar der gesamten Cloud-Plattform zu gefährden.

Umsetzungsbeispiel: Eine gute Entropiequelle kann ein benutzerdefinierter, selbst gehosteter Server/Dienst sein, oder ein geeigneter RNG, der von CPUs und Hardware angeboten wird und über virtio-rng oder einen ähnlichen Mechanismus an virtuelle Maschinen durchgereicht werden kann (z.B. Übergabe von `/dev/urandom` als RNG-Gerät).

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-21/1.0

Req 22	Die gesamte Cloud-Infrastruktur, einschließlich Verwaltung, Orchestrierung und aller unterstützenden Systeme, muss über definierte Metriken für die Ressourcenzuweisung verfügen und die Metriken müssen gemessen und überwacht werden.
--------	---

Es wird erwartet, dass zumindest die folgenden Metriken genau überwacht werden:

- Gesundheitszustand des Systems
- CPU-Auslastung
- RAM-Auslastung
- Netzauslastung
- Nutzung von Plattenspeicher (Kapazität)
- Festplattenverkehrsnutzung
- Dateisystemauslastung

Motivation: Im Gegensatz zur Überwachung der Auslastung dedizierter Systeme, die in erster Linie ein betriebliches Anliegen ist, kann und muss die Überwachung der Auslastung in einer Cloud-Umgebung zur Erkennung und Eindämmung von Angriffen genutzt werden.

Umsetzungsbeispiel: Jedes Überwachungssystem (z.B. Nagios oder Prometheus+Grafana) kann verwendet werden, wenn es die aufgeführten Metriken überwachen kann.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-22/1.0

Req 23	Die gesamte Cloud-Infrastruktur, einschließlich Verwaltung, Orchestrierung und aller unterstützenden Systeme muss Protokolle über sicherheitsrelevante Ereignisse liefern.
--------	--

Die Protokollierung ist für alle Systeme obligatorisch - für Rechen-, Speicher- und Verwaltungsknoten, die die Cloud-Infrastruktur bilden, aber auch für unterstützende Systeme (Repository, KMS, Jump Hosts, ...). All diese Systeme müssen Sicherheitsereignisse erzeugen, speichern und weiterleiten:

- Aufgaben von Konten mit hohen Privilegien
- Aufgaben der Benutzerverwaltung
- Systemstatus wie CPU-, RAM-, Netzwerk- und Festplattennutzung sowie die Auslastung des Dateisystems
- Mandantenverwaltung (Anlage, Änderung, Löschung)
- Netzverwaltung (Erstellung, Änderung, Löschung, einschließlich Sicherheitsgruppen)
- ... (die Liste ist nicht vollumfänglich)

Motivation: Eine angemessene Protokollierung von Sicherheitsereignissen ist eine Voraussetzung für die Entdeckung von Angriffen und eine angemessene Schadensbegrenzung.

Umsetzungsbeispiel: Angemessene Konfiguration der Protokollierung (z. B. mindestens WARN-Level und in einigen Fällen INFO).

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-23/1.0

Req 24	Sicherheitsrelevante Protokollierungsdaten müssen umgehend nach deren Erzeugung an einen separaten Log-Server weitergeleitet werden. Darüber hinaus müssen die Protokolle einer geeigneten SIEM-Lösung zur Sammlung, Speicherung und Analyse sicherheitsrelevanter Ereignisse zur Verfügung gestellt werden. Das SIEM muss Sicherheitsereignisse korrelieren und Alarme für Angriffe generieren.
--------	--

Die Speicherung von Protokollen reicht nicht aus, sie müssen analysiert und richtig korreliert werden. Ein einzelnes System kann ein Ereignis erkennen und protokollieren, aber die Informationen reichen möglicherweise nicht aus, um einen laufenden Angriff zu erkennen. Dies gilt vor allem in Cloud-Umgebungen, in denen ein einzelner Mandant auf viele Server verteilt ist. Die Erkennung von Anomalien sollte zusätzlich zur Definition der Regeln für die Protokollfilterung, Überwachung und Alarmierung eingesetzt werden.

Daher muss zusätzlich zur zentralen Protokollierungslösung eine SIEM-Lösung (Security Information and Event-Management) eingesetzt werden, um Sicherheitsereignisse zu analysieren und zu korrelieren, Anomalien zu erkennen und im Falle von Problemen Alarm zu schlagen. Dies ermöglicht die erfolgreiche Implementierung eines Incident-Management-Prozesses.

Aufgrund der Angriffsfläche einer Cloud-Umgebung ist es erforderlich, dass die Protokollerfassung, -analyse und -korrelation sowie die Alarmierung in Echtzeit oder nahezu in Echtzeit (mit möglichst geringer Verzögerung) erfolgen, um laufende Angriffe zu erkennen und zu entschärfen.

Unter der Annahme, dass die SIEM-Lösung vom zuständigen SOC (Security Operations Center) zur Verfügung gestellt wird, ist die Cloud-Plattform dafür verantwortlich, die Protokolle und ausreichende Informationen für die Analyse und Alarmierung bereitzustellen und weiterzuleiten sowie ausreichende Informationen und Hilfe bei der Einrichtung von Alarmen zu bieten.

Motivation: Die Speicherung von Protokollen auf den Servern, von denen sie stammen, reicht nicht aus, da der Angreifer die Protokolle leicht manipulieren und die Beweise für einen erfolgreichen Angriff löschen kann. Daher müssen alle Protokolle an das zentrale System weitergeleitet werden.

Umsetzungsbeispiel: SyslogNG, CheckMK, Nagios, Splunk etc. können als zentrales System eingesetzt 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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-24/1.0

Req 25	Das Cloud-Orchestrierungs-Framework muss alle sicherheitsrelevanten Ereignisse protokollieren (einen Prüfpfad erstellen).
--------	---

Das Cloud-Orchestrierungs-Framework (einfach ausgedrückt: die internen Teile der Cloud, die für die Verwaltung der Ressourcen zuständig sind) wird von den Mandanten über APIs, Dashboards usw. genutzt und dient der Manipulation (Erstellen, Anzeigen, Ändern, Löschen) von Ressourcen des jeweiligen Mandants. Zu den Ereignissen des Cloud-Orchestrierungs-Frameworks gehören alle Aktionen, die Ressourcen in der Cloud manipulieren.

Zusätzlich zur regelmäßigen Protokollierung von Cloud-Infrastruktur-Ereignissen muss die Cloud-Infrastruktur einen Prüfpfad (in der Praxis geschieht dies in der Regel durch die Erstellung von Protokollen) für alle Aktionen, die auf allen Cloud-Ressourcen durchgeführt werden, bereitstellen.

Die sicherheitsrelevanten Ereignisse, die vom Cloud-Orchestrierungs-Framework stammen, müssen weitergeleitet und mit den übrigen Protokollen und Sicherheitsereignissen zusammengeführt werden.

Motivation: Die Protokollierung von Orchestrierungsereignissen für Mandanten ist eine Voraussetzung für deren Sicherheit (z. B. wer hat wann eine bestimmte Cloud-Ressource erstellt, geändert oder gelöscht).

Umsetzungsbeispiel: Einige Beispiele umfassen die Protokollierung von:

- Anlegen, Löschen und Ändern von Tenants (Benutzer, Projekte, Rollen)
- Anlegen, Löschen und Ändern von Mandantennetzen
- Erstellung, Löschung und andere Aktionen der virtuellen Maschine
- Anlegen, Löschen, Ändern und Lesen von Objektspeicherbereichen und Objekten

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-25/1.0

Req 26	Es muss eine zentrale Lösung für die Authentifizierung und Autorisierung von Benutzern (sowohl Menschen als auch M2M) verwendet werden.
--------	---

Alle Systeme der Cloud-Infrastruktur (und unterstützende Systeme) müssen ein zentrales System zur Benutzerverwaltung nutzen und möglichst auf eine der bestehenden IAM-Lösungen der DTAG abgebildet werden.

Für den unwahrscheinlichen Fall, dass keine DTAG-eigene IAM-Lösung für die Verwaltung von Identitäten integriert werden kann, ist es notwendig, die Kontenverwaltung zu automatisieren. Eine solche Automatisierung für die Verwaltung von Identitäten muss die "IAM (Identity Access Management) - Framework" (3.69.) Anforderungen 01-57 und 65 erfüllen.

Die Verwendung eines Online-/Live-Zentralsystems wird empfohlen, aber je nach Verfügbarkeit des zentralen Identitätsmanagementsystems (teilweise aufgrund der Zuverlässigkeit der Verbindung) könnte der Cloud-Betreiber eine andere Art der zentralen Nutzerverwaltung wählen, damit die Cloud auch bei Ausfall des zentralen Identitätsmanagementsystems verwaltbar bleibt.

Der gleiche Ansatz gilt auch für Mandantenkonten für den Zugriff auf Cloud-APIs.

Motivation: Die zentrale Verwaltung von Konten und Rechten ermöglicht eine einfachere Wartung im Vergleich zu einem Ansatz, bei dem Konten und Rechte auf jedem System einzeln verwaltet werden. Der Sicherheitsvorteil besteht darin, dass ein Benutzerkonto und seine Rechte nur auf einem zentralen System bekannt sind, auf die erforderlichen

Systeme und Geräte übertragen werden können (Provisioning), zentral verwaltet (Reconciliation) und zentral gelöscht werden können (Deprovisioning). Dies reduziert das Risiko von vergessenen Accounts (z.B. Mitarbeiter, die das Unternehmen verlassen oder die Rolle gewechselt haben).

Umsetzungsbeispiel: Beispiele für ein solches zentrales Identitätssystem in der DTAG sind clAM, WiW und ZAM, die eine Kontoverwaltung und Rechteverwaltung bieten. Was die Technologien betrifft, so sind Active Directory Identitätsverbund, AFDS Shared (AAD wird in naher Zukunft erwartet), SAML 2.0, OpenID+OAuth (2.0) und LDAPS (nur innerhalb einer VPN-Verbindung) praktikable Optionen.

TACACS+ oder Radius können auch für bestimmte Netzwerkgeräte 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
- Unbemerkt durchführbare Angriffe

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-26/1.0

Req 27 Cloud-Infrastruktursysteme müssen auf automatisierte Weise gehärtet werden.

Alle Betriebssystemkomponenten, Anwendungen und Geräte müssen gehärtet werden, um die Angriffsfläche zu minimieren. Die Härtungsaufgaben, die nicht automatisiert werden können, müssen für jedes System manuell durchgeführt werden, bevor das System für andere Komponenten erreichbar wird oder in die Produktion aufgenommen wird.

Motivation: In einer Cloud-Umgebung, in der häufig Änderungen vorgenommen werden, ist es schwierig, ein gutes Niveau der Sicherheitshärtung manuell aufrechtzuerhalten; daher ist es notwendig, den Härtungsprozess zu automatisieren. Die automatisierte Härtung ermöglicht Konsistenz, ist weniger fehleranfällig und ermöglicht sogar schnellere Änderungen der Cloud-Infrastruktur.

Umsetzungsbeispiel: Einige Beispiele für Härtungswerkzeuge, die verwendet werden können, sind:

- Ansible
- Chef
- Puppet

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-27/1.0

Req 28 Die Überprüfung der Einhaltung der Sicherheitsvorschriften muss automatisch erfolgen.

Aufgrund der Vielfalt der Systeme, die in der Cloud gehostet werden, und der Komplexität der Cloud-Plattform ist es erforderlich, auf allen Servern und Geräten die Einhaltung der einschlägigen Sicherheitsanforderungen zu überprüfen.

fen.

Die Implementierung muss als Teil der CI/CD-Kette vor der Bereitstellung (wenn CI/CD und Automatisierung verwendet werden) und während der Lebensdauer regelmäßig erfolgen. Wie bei der Härtung muss auch hier die Automatisierung so weit wie möglich genutzt werden, um das Risiko zu vermeiden, dass Konformitätsprüfungen und/oder Systeme übersehen werden.

Motivation: Regelmäßige Überprüfungen der Einhaltung der Vorschriften validieren den aktuellen Sicherheitsstatus von Systemen und können Schwachstellen in Sicherheitskonfigurationen oder ungepatchte Systeme mit bekannten Sicherheitslücken aufdecken.

Umsetzungsbeispiel: Einige Beispiele für Tools zur Überprüfung der Einhaltung von Vorschriften sind:

- CIS-Benchmarks
- Ansible
- InSpec
- Orpheus (Telekom intern)
- TASTE-OS (Telekom-intern, eine Liste aller TOS-Instanzen finden Sie unter <https://yam.telekom.de/docs/DOC-685659>)

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-28/1.0

Req 29	Die Cloud-Infrastruktur sollte Maßnahmen zur Erkennung und zum Schutz vor Missbrauch wie Ransomware und Crypto-Mining bieten.
--------	---

Die für die Erkennung von Ransomware und Cryptocurrency-Mining relevanten Metriken zur Überwachung der Betriebsressourcen und entsprechende Schwellenwerte müssen definiert werden. Die Schwellenwerte müssen überwacht und überschrittene Schwellenwerte müssen ausgewertet werden und eine Benachrichtigung auf automatisierte Weise erstellen.

Die Erkennung kann in Kombination mit der Zusammenarbeit von Mandanten durchgeführt werden.

Motivation: Zusätzlich zum regulären Schutz vor Malware muss die Notwendigkeit des Schutzes vor Ransomware hervorgehoben werden, die in einer Cloud-Umgebung viel weitreichendere Auswirkungen haben würde, da sie alle in der Cloud laufenden Systeme gleichzeitig beeinträchtigen kann.

Das Mining von Kryptowährungen würde der DTAG durch die unbefugte Nutzung der Geräte zusätzliche Kosten verursachen.

Umsetzungsbeispiel: Als Vorsichtsmaßnahme sollte zumindest eine Erkennung und Alarmierung in Form einer Erkennung von verdächtigen Aktivitäten mit hohem IO erfolgen. Darüber hinaus sollte die Erkennung von Cryptocurrency-Mining zumindest durch Überwachung der CPU-Nutzung 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
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-29/1.0

4. Anforderungen für Bare Metal

4.1. Bare Metal as a Service

Die Verwendung von Bare Metal (entweder als komplette Server oder als spezifische Hardware) hat bestimmte Vorteile für Mandanten, die besondere Funktionen, eine größere Kontrolle über die Hardware oder eine höhere/stabile Leistung benötigen. Auch wenn man davon ausgeht, dass die Cloud so aufgebaut ist, dass sie den Mandanten die meisten Funktionen, die beste Kontrolle und die beste Leistung bietet, gibt es einige Anwendungsfälle, die sich nicht für einen virtualisierten Ansatz eignen. Es muss besonders darauf geachtet werden, dass die Sicherheit bei Bare-Metal-Cloud-Angeboten nicht beeinträchtigt wird, da die von der Virtualisierung gebotenen Sicherheitsfunktionen manchmal als selbstverständlich angesehen werden und in Vergessenheit geraten können.

Req 30	Bare-Metal-Knoten müssen vor der ersten Nutzung, nach einer Neuzuweisung oder vor der Außerbetriebnahme bereinigt und die hardwarebasierten Einstellungen auf kundenspezifische oder Standardwerte zurückgesetzt werden.
--------	--

Bevor ein Mandant einen Bare Metal Node nutzen kann, muss dieser vollständig gelöscht werden (einschließlich Festplatten, UEFI/BIOS-Firmwareeinstellungen, BMC-Schnittstelle usw.). Zusätzlich zur regelmäßigen Löschung ist es notwendig, die Firmware jedes einzelnen Hardwareteils zu überprüfen (mittels Prüfsumme oder einer anderen verfügbaren Methode). Bei häufigen Mandantenwechseln kann dies die Lebensdauer des Flash-Speichers (UEFI/BIOS/Firmware oder SSDs) verkürzen. Es ist erwähnenswert, dass einige moderne Speichergeräte (insbesondere Flash-Speicher) ein schnelles Löschen des Inhalts ermöglichen, indem der Verschlüsselungsschlüssel auf sichere Weise gelöscht wird.

Das Löschen des Bare-Metal-Knotens und das Zurücksetzen der Einstellungen sollte am besten nach jeder Nutzung erfolgen, d. h. wenn die Ressource für einen generischen Pool freigegeben werden soll. Erst als letzter Schritt sollte ein Kurzschluss herangezogen werden, um den gesamten RAM-Inhalt vollständig zu löschen. Kann ein Gerät nicht vollständig gelöscht werden, darf er nicht wiederverwendet werden, und im Falle eines Hardwareausfalls (insbesondere bei Festplatten) muss die Hardware ordnungsgemäß außer Betrieb genommen werden (im Falle von Festplatten - Entmagnetisierung und/oder Zerstörung) gemäß der Standardverfahren.

Die folgende Liste ist nicht vollständig, umfasst aber die Komponenten mit dem größten Risiko:

- BMC-Schnittstelle (IPMI/Redfish) - Firmware/Software und Einstellungen (wie Benutzername und Kennwörter/Schlüssel)
- UEFI/BIOS - Firmware und Einstellungen
- Erweiterungskarten (NIC, GPU, FPGA, RAID/HBA/generische Speicherkarten) - Firmware und in einigen Fällen Einstellungen
- Laufwerke (Firmware und Inhalt)

Je nach Anwendungsfall müssen zusätzliche Vorkehrungen getroffen werden, z. B. darf es dem Benutzer nicht erlaubt sein, ein UEFI/BIOS-Kennwort für den Supervisor festzulegen, das anschließend nicht zurückgesetzt werden kann, da dies den Computer für andere unbrauchbar machen würde.

Dieses Verfahren gewährleistet die Entfernung aller sensiblen Daten. Das Verfahren verhindert auch die Implementierung von Malware auf dem Bare-Metal-Rechner, wenn diese an anderer Stelle auf dem Rechner platziert wird. Durch das Zurücksetzen von Einstellungen wie BMC wird sichergestellt, dass ein Angreifer anschließend keinen Zugriff mehr auf den Computer hat. Das Zurücksetzen der UEFI/BIOS-Einstellungen ist von Vorteil, da es sicherstellt, dass jeder Rechner mit der gleichen (sicheren) Grundeinstellung ausgestattet ist.

Motivation: Die auf dem zuvor verwendeten Bare-Metal-Knoten verbliebenen Daten können sensible Daten (Geheimnisse oder persönliche Daten) enthalten, auf die nicht mehr zugegriffen werden soll, insbesondere nicht von jemand anderem.

Umsetzungsbeispiel: Der Prozess der Hardware-Stillegung kann als ein Schritt implementiert werden, der bei jeder Hardware-Freigabeoperation durchgeführt wird.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-30/1.0

4.2. PCI-Passthrough

PCI Passthrough ist eine Technologie, die es einer virtuellen Maschine ermöglicht, direkt auf ein PCI[e]-Gerät oder ein Subdevice zuzugreifen (durch die Verwendung von SR-IOV). Dies geschieht durch die direkte Zuordnung des Speicheradressraums des PCI-Geräts oder -Subdevices zur virtuellen Maschine.

Req 31	Die Verwendung von PCI-Passthrough ist nicht erlaubt, es sei denn, es gibt keine anderen Möglichkeiten, die Hardware zu nutzen.
--------	---

PCI-Passthrough bringt auch die nativen Funktionen und die Leistung der gegebenen Hardware (GPUs, NICs, FPGAs, ...) mit geringem oder unbedeutendem Overhead in die virtuelle Maschine, was es für Anwendungsfälle wie maschinelles Lernen, KI, Cloud-Gaming, Netzwerk-Paketverarbeitung usw. sehr attraktiv macht. Anwendungen, die PCI-Passthrough nutzen, haben in der Regel einen großen Fußabdruck und die Verwendung von Bare-Metal-Maschinen wird im Vergleich zu PCI-Passthrough bevorzugt.

Motivation: PCI-Passthrough umgeht den Hypervisor und die Sicherheitsmaßnahmen des Hypervisors und ermöglicht einen direkten Zugriff auf das Gerät, der für Angriffe auf den Hypervisor oder andere Tenants missbraucht werden kann.

Umsetzungsbeispiel: Verwendung von Open vSwitch anstelle von dedizierten Ports auf der Netzwerkkarte mit PCI-Passthrough.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-31/1.0

Req 32	Hardware, die mit PCI-Passthrough verwendet wird, muss nach ihrer Freigabe sicher für die weitere Verwendung vorbereitet werden.
--------	--

Wie bei der Stilllegung von Bare-Metal-Hardware muss die Hardware, die für PCI-Passthrough verwendet wurde, gelöscht und zurückgesetzt werden.

Motivation: Hardware, insbesondere FPGAs und GPUs, enthalten noch Reste der vorherigen Nutzung im Arbeitsspeicher (RAM) oder im Flash-Speicher. Diese Reste können sensible Daten enthalten, die für einen anderen Mandanten nicht zugänglich sein dürfen. Außerdem können die Reste einige unsichere Einstellungen enthalten, die vom Vorbesitzer in Form einer bösartigen Software hinterlassen wurden.

Umsetzungsbeispiel: Verwendung der vom Treiber unterstützten Funktion zum Löschen des Inhalts und Zurücksetzen der Einstellungen, nachdem das Gerät freigegeben wurde.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unbemerkt durchführbare Angriffe

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

Req 33 Alle PCIe-Passthrough-Geräte (mit oder ohne SR-IOV) müssen gehärtet sein.

Die häufigsten Anwendungsfälle von PCIe-Passthrough-Geräten und die bekannten Risiken werden in den Anforderungen in diesem Kapitel behandelt. Selbst für diese häufigsten Anwendungsfälle, aber noch wichtiger für alle anderen allgemeinen Anwendungsfälle, ist es notwendig, die Sicherheit des spezifischen PCIe-Geräts in der vom Hersteller oder der Gemeinschaft beschriebenen, strengsten Weise zu härten.

Motivation: Eine unsichere Konfiguration von Geräten kann dazu führen, dass sie von Mandanten in einer Weise ausgenutzt werden, die nicht beabsichtigt war.

Umsetzungsbeispiel: Die Aushärtung sollte gemäß der Beschreibung des Herstellers oder den Richtlinien der Gemeinschaft 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
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-33/1.0

4.3. SR-IOV

SR-IOV steht für Single Root I/O Virtualization und teilt in der Praxis ein PCI[e]-Gerät in Untergeräte auf, insbesondere in eine physische Funktion (PF, typischerweise vom Hypervisor aus zugänglich) und eine oder mehrere virtuelle Funktionen (VF, typischerweise von VMs genutzt). Die Verwendung von VF innerhalb einer VM erfolgt nach wie vor mittels PCI-Passthrough.

Beispiel:

Ein typisches Beispiel für die Verwendung von SR-IOV sind Netzwerkkarten. Sobald SR-IOV aktiviert ist, wird eine Netzwerkkarte in eine PF aufgeteilt, die vom Hypervisor gesteuert wird, während mehrere VFs für die Verwendung in VMs verfügbar sind. Der Hypervisor steuert die PF, daher steuert der Hypervisor den Verbindungsstatus (physische Netzwerkschnittstelle - oder Laser, wenn Glasfaser verwendet wird), verwaltet die Zuordnung von VFs zu VLANs (oder welche andere Art der Trennung verfügbar ist) und die Zuordnung von VFs zu VMs. PF und jede VF erhalten ihren eigenen PCI-Adressraum. Durch die Verwendung von PCI Passthrough oder einer entsprechenden VF erhält eine VM Zugriff auf eine oder mehrere VFs und jede VF wird als Netzwerkkarte mit etwas eingeschränkten Funktionen dargestellt. Die VM kann den Verbindungsstatus über die VF nicht ändern und auch nicht die MAC-Adresse oder das VLAN (oder eine andere verwendete Kapselung) dieser spezifischen VF. In Kombination mit der Konfiguration geeigneter VLANs auf der anderen Seite (Switch oder Router) kann sichergestellt werden, dass VMs auf die erwarteten Netzwerke beschränkt bleiben. SR-IOV für NICs wird in der Regel verwendet, wenn VMs eine Bare-Metal-ähnliche Leistung benötigen, aber wenn mehrere VMs dieselbe physische Verbindung nutzen, gelten immer noch die Gesetze der Physik (man kann nicht zwei VMs haben, die jeweils 10 Gbit/s auf einer einzigen 10 Gbit/s-Verbindung nutzen).

Allgemeine Liste der Sicherheitsmängel bei SR-IOV:

- die Live-Migration virtueller Maschinen (im Falle eines Compute-Node-Patching) ist komplizierter oder unmöglich
- virtuelle Maschinen, die auf der gleichen Hardware gehostet werden, können sich gegenseitig beeinflussen

Die Liste der Sicherheitsmängel für NIC SR-IOV:

- es gibt keine standardmäßige hostbasierte Verkehrsfilterung (wie Sicherheitsgruppen)
- Die standardmäßige Hypervisor-basierte Virtualisierung von Netzwerken kann nicht zur Trennung des Datenverkehrs verwendet werden.
- virtuelle Maschinen, die auf der gleichen Hardware gehostet werden, können sich gegenseitig durch PAUSE-Frame-Injektion beeinflussen
- Die Firmware des NIC und der PF-Treiber haben eine größere Angriffsfläche im Falle von Sicherheitsproblemen

Die hier aufgeführten Sicherheitsanforderungen für SR-IOV gelten auch für Container, wenn PCIe-Geräte direkt von Containern verwendet werden.

Req 34 Bei Verwendung von Bare-Metal-Netzwerken oder Netzwerken über PCI-Passthrough (mit oder ohne SRIOV), bei denen die NIC keine L3/L4-Filterung durchführen kann, muss die L3/4-Verkehrsfilterung auf einem Switch oder einem Router implementiert werden.

Moderne NICs, die L3/L4-Filterung im PCI-Passthrough (mit oder ohne SR-IOV) durchführen können, können für die L3/L4-Verkehrsfilterung verwendet werden. Wenn jedoch auf dem Hypervisor oder der NIC keine Verkehrsfilterung möglich ist (abgesehen von den Regeln, die der Mandant innerhalb der VM oder eines Containers definiert), müssen Tagging (z. B. VLANs) und/oder ACLs auf einem Switch oder Router neben dem jeweiligen Bare-Metal- oder Hypervisor-Knoten konfiguriert werden, damit der Mandant sicher von anderen Mandanten isoliert ist.

Motivation: Die Verwendung von SR-IOV ermöglicht zwar ein gewisses Maß an Filterung oder Mandantentrennung auf der NIC, ist aber nicht immer ein ausreichender Ersatz für die herkömmliche L3/L4-Filterung durch Overlay-Netzwerke (die von den NIC-Funktionen abhängt). Die Verkehrsfilterung pro virtuelle Funktion (pro VF) ermöglicht die Trennung von Mandanten und den Schutz von Mandanten gemäß den vom Mandanten definierten Sicherheitsgruppen.

Umsetzungsbeispiel: Die Konfiguration von L3/L4-Filtern auf Routern oder Switches kann z.B. durch ein Ansible-Plugin in OpenStack Neutron für die Switch-Konfiguration (oder jedes andere fähige SDN) erreicht werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-34/1.0

Req 35 Bei Verwendung von PCI-Passthrough mit oder ohne SR-IOV für die Vernetzung muss die Trennung des Datenverkehrs zwischen den Mandanten durch die NIC erzwungen werden.

Zusätzlich zu den vorgenannten Anforderungen an die Verkehrsfilterung auf der Switch-/Router-Seite ist es auch erforderlich, eine strikte Mandanten-Trennung auf den NICs vorzunehmen. Moderne NICs, die L3/L4-Filterung für Overlay-Verkehr unterstützen, tun dies in der Regel ordnungsgemäß, aber bei weniger leistungsfähiger Hardware kann dies durch die Verwendung separater physischer Ports, VLANs, VXLAN oder ähnliche Mittel erreicht werden, die sowohl von der NIC als auch vom benachbarten Switch/Router unterstützt werden.

Motivation: Ohne eine vollständige Trennung des Datenverkehrs durch die NIC wäre ein Mandant in der Lage, den Netzwerkverkehr von/für andere Mandanten zumindest zu beobachten (oder zu injizieren).

Umsetzungsbeispiel: Jeder Port für jede VM auf dem Hypervisor muss als separate VF konfiguriert werden, mit einer entsprechenden eindeutigen VLAN-Kennung, die von dem Switch/Router erkannt wird, an dem das Overlay-Netzwerk abgeschlossen/geroutet wird.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-35/1.0

Req 36	Bei der Verwendung von SR-IOV NIC muss eine Entschärfung der PAUSE-Frame-Injektion implementiert werden.
--------	--

Anwendungen, die SR-IOV verwenden, erwarten in der Regel eine bessere Netzwerkleistung und -zuverlässigkeit im Vergleich zu herkömmlichen virtualisierten Netzwerken, und ein Angriff mit PAUSE-Frames könnte eine wirksame Maßnahme zur Dienstverweigerung darstellen. Daher muss die Flusskontrolle deaktiviert werden, um die Injektion von PAUSE-Frames abzuschwächen. Alternativ könnte man einen virtualisierungsfähigen Netzwerk-Flusscontroller verwenden.

Motivation: Eine fehlverhaltende (oder böswillige) VM kann die Netzwerkverfügbarkeit anderer virtueller Maschinen auf demselben Host durch die Injektion von PAUSE-Frames unterbrechen, was zu einer Dienstverweigerung führt.

Umsetzungsbeispiel: Deaktivierung der Flusskontrolle.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Verfügbarkeit

ID: 3.86-36/1.0

Req 37	Hosts, die PCIe-Passthrough mit SR-IOV für die Vernetzung verwenden, dürfen keine Verkehrsarten auf demselben physischen Gerät mischen.
--------	---

Dies gilt im Allgemeinen auch für konvergente und hyperkonvergente Clouds, so dass erwartet wird, dass im Allgemeinen zumindest unterschiedliche physische Ports verwendet werden, um Cloud-Management und Overlay-Verkehr zu trennen.

Motivation: Um zu verhindern, dass Schwachstellen in SR-IOV ausgenutzt werden, durch die ein Mandant die Infrastruktur auf einfachere Weise kompromittieren kann, ist es notwendig, die Verkehrsarten zwischen den physischen Instanzen der Geräte zu trennen (z. B. wäre der bevorzugte Ansatz eine vollständige Netzwerkkarte).

Umsetzungsbeispiel: Eine NIC kann den internen Cloud-Verwaltungsdatenverkehr und die andere NIC den Datenverkehr (Overlay-Datenverkehr) übertragen, wodurch die Möglichkeit eines Angriffs vom Mandantenbereich auf die Infrastruktur verringert wird.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-37/1.0

5. Hypervisor und Server

5.1. Allgemeine Serveranforderungen

Req 38	Ein Server (unter besonderer Berücksichtigung von Hypervisoren) muss vor der ersten Verwendung, nach einer Neuzuweisung oder vor der Außerbetriebnahme vollständig gelöscht werden.
--------	---

Um den Server für die erste Nutzung vorzubereiten, muss der Server gelöscht, die Firmware aktualisiert und/oder überprüft und das Betriebssystem von Grund auf neu installiert werden. Der gleiche Ansatz gilt, wenn der Server seine Funktion ändert (z. B. wenn er für allgemeine Arbeitslasten der Mandanten anstelle von Netzwerkschutzmechanismen verwendet wird). Die Außerbetriebnahme des Systems erfordert eine vollständige Löschung der Daten auf den Servern, gefolgt von einem Herunterfahren, um alle Daten aus dem flüchtigen Speicher (RAM) zu entfernen.

Motivation: Server für allgemeine Zwecke sind sehr vielseitig, aber diese Vielseitigkeit kann auch von einem Angreifer missbraucht werden, der damit seine Präsenz auf andere Cloud-Subsysteme ausdehnen könnte.

Umsetzungsbeispiel: Der Prozess der Außerbetriebnahme von Servern kann als ein Schritt implementiert werden, der bei jeder Hardware-Freigabe, Neuzuweisung oder vor der ersten Verwendung durchgeführt 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
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-38/1.0

Req 39	Alle Server (Hypervisor oder Bare Metal, die für die Cloud-Plattform verwendet werden) müssen durch eine Firewall geschützt sein.
--------	---

Alle Server (außer den Bare-Metal-Servern, die den Mandanten zur Verfügung gestellt werden) stehen unter der Kontrolle des Cloud-Betreibers und sind direkt mit dem Cloud-Infrastrukturnetz verbunden; sie müssen durch lokale Firewalls (wie iptables) gegen mögliche Angriffe von anderen Servern geschützt werden. Diese lokale Firewall muss so konfiguriert werden, dass sie nur die notwendige Kommunikation zulässt, einschließlich Regeln für den Eingangs-, Weiterleitungs- und Ausgangsverkehr. Alle Verstöße müssen protokolliert (und zur Erkennung von Bedrohungen an das zentrale System weitergeleitet) werden.

Bare-Metal-Server, die den Mandanten zur Verfügung gestellt werden, wären geschützt und von anderen Mandanten auf dem benachbarten Switch getrennt, da der Cloud-Betreiber die lokale Firewall des Mandanten nicht kontrollieren kann.

Motivation: Die Erkennung von eingehendem Datenverkehr, der nicht notwendig ist (und daher von der Firewall nicht zugelassen wird), kann auf ein bereits angegriffenes Gerät im Cloud-Infrastrukturnetz hinweisen, während die Erkennung von unerwünschtem weitergeleitetem oder ausgehendem Datenverkehr auf einen Einbruchversuch oder eine Verletzung des Hypervisors hinweisen kann. Eine frühzeitige Erkennung erhöht die Fähigkeit zur erfolgreichen Abwehr und kann die Ausbreitung des Angriffs begrenzen.

Umsetzungsbeispiel: Aktivierung einer Firewall (z. B. iptables) mit Protokollierung und Weiterleitung der Protokolle an das zentrale System, das die Protokolle auf verdächtige Aktivitäten überwacht.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-39/1.0

Req 40 Eine MAC-Lösung muss auf allen Rechnern implementiert werden.

Die Aktivierung von MAC-Lösungen (Mandatory Access Control) wie SELinux oder AppArmor im Durchsetzungsmodus reicht nicht aus, da sie auf ordnungsgemäß konfigurierte Profile angewiesen sind. Ein sehr strenges MAC-Profil (das nur notwendige Systemaktionen zulässt) muss für Hypervisor-Software, unterstützende Systeme und andere kritische Systemdienste verwendet werden.

Alle MAC-Verstöße müssen protokolliert werden, einen Alarm auslösen und wie Sicherheitsereignisse behandelt werden. Selbst wenn es dem Angreifer gelingt, mit der MAC-Lösung und den richtigen Profilen bis zur Hypervisor-Ebene vorzudringen, wird der Zugriff auf die Systemressourcen etwas eingeschränkt, und die MAC-Lösung verhindert die weitere Ausbreitung des Angriffs und erhöht die Chancen auf eine frühzeitige Erkennung.

Motivation: MAC-Lösungen bieten ein strengeres Zugriffsmodell als die Standardfunktionen des Linux-Kernels.

Umsetzungsbeispiel: Aktivieren des Durchsetzungsmodus für SELinux und Verwendung geeigneter Profile für Software wie KVM und libvirt.

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-40/1.0

Req 41 Eine Integritätsschutzlösung muss auf allen Hosts implementiert werden.

Im Falle eines Angriffs können Systemdateien (sowohl Binärdateien als auch Konfigurationsdateien) und Daten auf den Hosts manipuliert werden. Das größte Augenmerk muss auf Computer-Hosts (Hypervisoren) gerichtet werden. Mit Integritätsschutzlösungen (z. B. AIDE, Tripwire, OSSEC) kann die Integrität zumindest von Binärdateien und Konfigurationsdateien überprüft und Verstöße gemeldet werden. Integritätsverletzungen müssen als Sicherheitsereignisse behandelt werden.

Einige Lösungen können auch auf das Vorhandensein von Rootkits prüfen und ihre Verwendung wird empfohlen (nicht die Verwendung von Rootkits, sondern von Lösungen, die Rootkits erkennen). Die Überprüfung von Konfigurationsdateien ist notwendig, da ein Angreifer lediglich Konfigurationsänderungen nutzen könnte, um sich unbemerkt zu verbreiten.

Motivation: Ein Angreifer, der sich Zugang zum System verschafft hat, kann zusätzliche Software installieren oder die Konfiguration so ändern, dass er den Zugang beim Neustart nicht verliert.

Umsetzungsbeispiel: Eine Kombination von Paketverwaltungsprogrammen und Konfigurationsverwaltungswerkzeugen kann, je nach Gesamtimplementierung, ein ausreichendes Maß an Integritätsprüfungen bieten.

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-41/1.0

5.2. Hypervisor-Trennung

Die Hardware-Trennung war die bevorzugte Wahl für die Trennung in virtualisierten Umgebungen, aber es ist praktisch unmöglich, den gleichen Ansatz in einer typischen Cloud-Bereitstellung zu implementieren. Cloud-Plattformen bieten bereits verschiedene Schutzmechanismen, die als Plattformdienste ausgeführt werden, wodurch die Notwendigkeit der Implementierung von DoS-, DDoS- und anderen Schutzmechanismen in jeder Anwendung reduziert wird.

Hinweis: Eine einfache Firewall für virtuelle Maschinen (in OpenStack als Sicherheitsgruppen bekannt) ist obligatorisch, wird aber in den meisten Fällen nicht als ausreichend angesehen, um als Netzwerkschutzmechanismus bezeichnet zu werden.

Req 42	Software, die als Plattformdienst angeboten wird und völlig andere Funktionen erfüllt, muss auf verschiedenen Hosts oder Hypervisoren installiert werden.
--------	---

Zusätzlich zu den allgemeinen Arbeitslasten von Mandanten kann die Cloud-Plattform verschiedene Dienste anbieten. Zu den beiden häufigsten Beispielen gehören Netzschutzmechanismen und Verwaltungsfunktionen (z. B. die Handhabung von Geheimnissen), aber dies gilt für jede Art von künftigen Angeboten, die nicht unter die allgemeinen Arbeitslasten fallen.

Die Cloud-Plattform muss es den Mandanten ermöglichen, Hosts für bestimmte Anwendungsfälle bereitzustellen, während die Mandanten (in Absprache mit ihrem jeweiligen Sicherheitsbeauftragten) dedizierte Hosts für Szenarien auswählen müssen, die von den allgemeinen Arbeitslasten abweichen.

Motivation: Plattformdienste, die Netzwerkschutzmechanismen anbieten, sind einem höheren Risiko ausgesetzt, da sie rohem oder grob gefiltertem Verkehr von außen ausgesetzt sind (Internetverkehr oder Verkehr von potenziell bösen Clients). Die Ausführung von Schutzmechanismen auf denselben Hypervisoren wie reguläre Tenant-Workloads würde das Risiko einer Beeinträchtigung der Tenant-Workloads erhöhen, entweder durch eine Verletzung des Hypervisors, Angriffe über Seitenkanäle oder einfach nur durch Aushungern von Ressourcen. Auch wenn eine Trennung nicht alle potenziellen Bedrohungsvektoren beseitigen kann, würde sie die Angriffsfläche drastisch reduzieren und die Erkennung und Eindämmung erleichtern.

Umsetzungsbeispiel: Verwendung dedizierter Hosts für Netzschutzmechanismen bzw. Funktionen zur Handhabung von Geheimnissen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-42/1.0

Req 43	Die von der Cloud-Plattform angebotenen Dienste müssen Schutz vor Netzwerkangriffen in Form von DoS- und DDoS-Schutz, Web Application Firewalls (WAFs), Proxies usw. bieten.
--------	--

Private Clouds müssen vom Mandanten konfigurierbare Netzschutzmechanismen bieten. Die Liste ist nicht vollständig, aber sie muss mindestens Folgendes umfassen:

- DoS-Schutz
- DDoS-Schutz
- WAF (Web Application Firewall)
- Proxy
- Firewall

Motivation: Zusätzlich zu den direkt genutzten Funktionen muss die Cloud-Plattform den Mandanten die Möglichkeit bieten, ihre Workloads zu sichern.

Umsetzungsbeispiel: Sie können als Software, die auf Hypervisoren läuft, als Software auf dedizierten Bare-Metal-Servern, als Teil gemeinsam genutzter Netzwerkhardware (Router, Switches, Firewalls) oder als dediziertes Gerät (dedizierte Geräte) implementiert werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-43/1.0

Req 44	Die Dienste der Cloud-Plattform sollten zumindest über ein Secret Management (oder weitere Verwaltungsfunktionen mit breiter Reichweite) verfügen.
--------	--

Diese Dienste müssen nicht integraler Bestandteil der Cloud-Plattform sein, sind aber in den meisten Fällen zwingend erforderlich, um die sichere Nutzung der Cloud durch die Mandanten zu ermöglichen. Daher können die Dienste von der Cloud-Plattform oder separat bereitgestellt werden, müssen aber von den Arbeitslasten der Mandanten nutzbar sein.

Motivation: Zusätzlich zu den direkt genutzten Funktionen muss die Cloud-Plattform den Mandanten die Möglichkeit bieten, ihre Workloads zu sichern.

Umsetzungsbeispiel: Das typischste Beispiel für moderne Anwendungen, die eine zusätzliche Sicherheitsebene erfordern, ist die Verwaltung von Geheimnissen, und es wird erwartet, dass die Cloud-Plattform mindestens die folgenden Funktionen bietet:

- Erstellung, Verwendung, Verwaltung, Widerruf und Löschung von Geheimnissen (Schlüssel, Passwörter)
- Zertifikatsverwaltung
- könnte CI/CD-Runner mit der Fähigkeit zur Verwaltung der Produktionsumgebung umfassen, je nach Einrichtung der CI/CD-Kette

Ein sehr beliebtes Beispiel für ein Tool zur Verwaltung von Geheimnissen ist Hashicorp Vault. Ein Beispiel für ein Tool zur Zertifikatsverwaltung ist Certbot, das einen geheimen Speicher und das ACME-Protokoll für die Interaktion zwischen der Zertifizierungsstelle und Servern, die Zertifikate verwenden (z. B. Webserver), nutzt.

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-44/1.0

Req 45	Jeder Mandant ist verpflichtet, Netzschutzmechanismen und Funktionen zur Verwaltung von Geheimnissen entsprechend den verfügbaren Plattformtechnologien ordnungsgemäß zu nutzen.
--------	--

Dies sind die beiden häufigsten Einsatzszenarien für die Netzschutzdienste:

- Netzwerkschutzdienste werden von der Cloud-Plattform bereitgestellt und der Mandant konfiguriert den Netzwerkschutz in geeigneter Weise für seine Anwendung, und dies ist die bevorzugte Art des Schutzes
- Netzwerkschutzdienste werden von der Cloud-Plattform nicht bereitgestellt, oder sie werden von der Cloud-Plattform bereitgestellt, aber der Mandant kann sie nicht nutzen; daher sollte der Mandant nach der Bewertung durch den zuständigen PSM einen speziellen Satz dedizierter Hypervisor für die Ausführung von Netzwerkschutzmechanismen zuweisen

In ähnlicher Weise benötigen die Mandanten in der Cloud in der Regel die Verwaltung von Geheimnissen (z. B. Schlüssel, Passwörter, Zertifikate) und andere Verwaltungs- und Unterstützungsfunktionen (z. B. Konfigurationsmanagement), die bei Bedarf verfügbar sind, um ihre Arbeitslasten zu unterstützen. Daher gibt es zwei häufigste Einsatzszenarien:

- die geheime Verwaltung wird von der Cloud-Plattform bereitgestellt, und der Mandant nutzt sie in geeigneter Weise für seine Anwendung, was die bevorzugte Art der Nutzung ist (dies gilt auch, wenn Verwaltungsdienste separat verfügbar sind - sie sind nicht direkt Teil der Cloud-Plattform, können aber wie diese genutzt werden)
- die geheime Verwaltung und zusätzliche Verwaltungsfunktionen werden nicht von der Cloud-Plattform bereitgestellt oder werden von der Cloud-Plattform bereitgestellt, aber der Mandant kann sie nicht nutzen, daher muss der Mandant nach der Bewertung durch den zuständigen PSM eine spezielle Gruppe dedizierter Hypervisor für die Ausführung der geheimen Verwaltung und anderer erforderlicher Dienste zuweisen

Hinweis: Der Hypervisor kann nicht für mehrere Funktionen gleichzeitig verwendet werden, z. B. können in diesem Fall die Netzwerkschutzfunktionen und die Verwaltung der Geheimnisse nicht auf demselben Server ausgeführt werden.

Motivation: Die Sicherheit von Anwendungen in der Cloud ist nicht gegeben, wenn die Sicherheitsfunktionen nicht richtig genutzt werden.

Umsetzungsbeispiel: Nutzung der von der Plattform angebotenen Sicherheitsdienste, um die Sicherheit der Anwendung zu gewährleisten.

ID: 3.86-45/1.0

5.3. Hypervisor-Schutz

Req 46	Management-Tools, die eine direkte Kommunikation zwischen einer VM und einem Hypervisor ermöglichen, dürfen nicht verwendet werden.
--------	---

Es gibt Tools, die eine direkte Kommunikation zwischen einer virtuellen Maschine und einem Hypervisor ermöglichen, z. B. VMWare Tools.

Motivation: Obwohl die Tools für die direkte Kommunikation zwischen einer virtuellen Maschine und einem Hypervisor manchmal gewisse Vorteile bieten, können sie auch für Angriffe auf den Hypervisor missbraucht werden.

Umsetzungsbeispiel: Tools innerhalb einer virtuellen Maschine dürfen nicht installiert (und verwendet) werden, und alle Funktionen, die eine solche Kommunikation auf dem Hypervisor ermöglichen, müssen deaktiviert 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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-46/1.0

Req 47	Die Nutzung von Systemressourcen muss für jede virtuelle Maschine eingeschränkt werden.
--------	---

Die Ressourcen, die eingeschränkt werden müssen, sind:

- vCPU-Anzahl und/oder CPU-Anteil
- Speicher (RAM)
- Netzwerk-Bandbreite
- Netzwerk-Paketrate
- Speicherplatz
- Speicherbandbreite
- Speicher IOPS

In Ermangelung von Möglichkeiten für feinkörnige Beschränkungen irgendeiner Art müssen Überwachung und automatische Abhilfemaßnahmen vorhanden sein.

Motivation: Abtrünnige virtuelle Maschinen können mehr Ressourcen verbrauchen, als sie sollten, wenn sie nicht eingeschränkt werden. Dieses Verhalten kann dazu führen, dass andere virtuelle Maschinen, die auf demselben Hypervisor laufen, unter Ressourcenmangel leiden, was die Verfügbarkeit anderer Systeme beeinträchtigt. Im schlimmsten Fall kann es den Hypervisor komplett lahmlegen und zu einem unvorhersehbaren Verhalten des Hypervisors oder des Rechenknotens führen.

Umsetzungsbeispiel: OpenStack in seiner Standardkonfiguration, unter der Annahme, dass die Sicherheitshärtung angewendet wurde.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Verfügbarkeit

ID: 3.86-47/1.0

Req 48	Die Überbuchung von Ressourcen muss so umgesetzt werden, dass sie die Stabilität und Sicherheit der Cloud nicht beeinträchtigt.
--------	---

Die Überbuchung von Ressourcen muss sich in den SLAs der Cloud-Plattform widerspiegeln und vom Cloud-

Betreiber gegenüber den Anwendungseigentümern klar dargelegt werden, und sie muss zusammen mit der Ressourcenbeschränkung (aus der vorherigen Anforderung) verwendet werden, damit die Hypervisor bei erhöhter Last nicht zum Stillstand kommen.

Systeme, die einen hohen Anteil an Überbuchungen aufweisen, müssen genau überwacht werden und sollten vorzugsweise über automatisierte Mechanismen zur Schadensbegrenzung verfügen (z. B. Live-Migration).

Motivation: Die Cloud wird in der Regel mit einer Überbuchung von Systemressourcen konzipiert und betrieben, was sich auf die Stabilität, Verfügbarkeit und Sicherheit der in der Cloud laufenden Hypervisoren und Arbeitslasten auswirken kann. Herkömmliche Netzwerkfunktionen, die in der Cloud virtualisiert ausgeführt werden, sind in der Regel weniger widerstandsfähig gegenüber Ressourcenmangel (z. B. weil sie eine vollständige Sitzungsliste im RAM aufbewahren und keine Verzögerungen beim Laden von Einträgen tolerieren können), während Cloud-native Anwendungen solche Ereignisse durch Skalierung abmildern.

Umsetzungsbeispiel: Falls erforderlich, kann man die Cloud in mehrere Typen unterteilen, die auf Überbuchung basieren, z. B. Hypervisoren, die Überbuchung verwenden, und solche, die keine Überbuchung verwenden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Verfügbarkeit

ID: 3.86-48/1.0

Req 49	Rechenknoten (Hypervisoren) müssen den virtuellen Maschinen ausreichend Entropie zur Verfügung stellen.
--------	---

Zusätzlich zu den bestehenden Sicherheitsanforderungen in dem Dokument, in dem die Entropiequelle für die Erzeugung von Geheimnissen beschrieben wird, muss hervorgehoben werden, dass Hypervisoren den virtuellen Maschinen geeignete Entropie zur Verfügung stellen müssen, z. B. über ein virtuelles Gerät, das an virtuelle Maschinen übergeben wird.

Wenn ein Mechanismus mit transparentem Zugriff auf den Zufallszahlengenerator von den virtuellen Maschinen aus nicht verwendet werden kann, müssen die Mandanten über das Problem informiert werden und der Cloud-Betreiber muss Zugang zu einer geeigneten Entropiequelle (Zufallszahlengenerator) gewähren.

Motivation: Schlüssel und Geheimnisse, die mit unzureichender Entropie generiert werden, können von Angreifern reproduziert/ausgespäht werden, was es ihnen ermöglicht, die Sicherheit von Systemen in der Cloud oder sogar der gesamten Cloud-Plattform zu gefährden.

Umsetzungsbeispiel: Standardmäßig kann in KVM ein virtio-rng-Gerät an virtuelle Maschinen übergeben werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-49/1.0

Req 50	Die Verschlüsselung des virtuellen Maschinenspeichers muss aktiviert und verwendet werden, wenn dies möglich ist.
--------	---

Mit geeigneter Hardware, die AMD Secure Encrypted Virtualization (SEV) oder gleichwertig unterstützt, und der entsprechenden Software (Kernel und libvirt, die SEV unterstützen) ist es möglich, den Speicher der virtuellen Maschine

(Gastmaschine) zu verschlüsseln und die Benutzer vor Angriffen oder unseriösen Administratoren zu schützen. Dies ist besonders nützlich für Umgebungen, die sich nicht an hochsicheren Standorten befinden. Eine solche Speicher-verschlüsselung hat Auswirkungen auf die Live-Migration und ist daher nicht für alle Workloads geeignet.

<https://www.zdnet.com/article/the-openstack-train-keeps-chugging-on/>

<https://arxiv.org/pdf/1901.01759.pdf>

Motivation: Durch die Speicherverschlüsselung wird auch die Möglichkeit eines Angriffs auf den Hypervisor oder andere Mandanten durch Angreifer, die bereits einen Mandant kompromittieren konnten, erheblich verringert.

Umsetzungsbeispiel: Einschalten von AMD SEV.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-50/1.0

6. Speicherung

Die Speicherung in der privaten Cloud kann als Software-Stack auf Servern, als dediziertes SAN oder NAS-Gerät(e) oder als Kombination realisiert werden. In diesem Dokument wird der Schwerpunkt auf die beliebteste Lösung gelegt - die Installation von Speichersoftware auf Servern. Eine solche Lösung, die häufig in OpenStack-Clouds eingesetzt wird, ist Ceph.

6.1. Trennung der Speicherung

Req 51	Für verschiedene Cloud-Funktionen muss getrennter Speicher (logisch und/oder physisch) verwendet werden.
--------	--

Die logische und/oder physische Trennung des Speichers ist ein erster Schritt zur Sicherung des Speichers und der gespeicherten Daten.

Im Falle einer physischen Trennung muss sichergestellt werden, dass kein Zugriff von unerwünschten Teilen der Cloud möglich ist. Wird beispielsweise eine Speicherlösung in Form von zwei Clustern bereitgestellt, von denen einer für sensible Daten und der andere für alles andere bestimmt ist, dürfen die Hypervisoren, die reguläre Arbeitslasten ausführen müssen, nicht auf den Speichercluster mit sensiblen Daten zugreifen können. Dies gilt auch für die logische Trennung, die als ausreichend angesehen wird, wenn die Protokolle eine ausreichend starke Authentifizierung ermöglichen.

Verschiedene Cloud-Funktionen können nicht denselben Pool verwenden, z. B. dürfen Cloud-Verwaltungsfunktionen nicht denselben Pool wie reguläre Rechenknoten verwenden, Netzschutzfunktionen dürfen nicht denselben Pool wie reguläre Arbeitslasten verwenden usw.

Jeder getrennte Speicherpool muss über eindeutige Anmeldedaten für die Authentifizierung verfügen, aber wenn möglich, sollten für jedes Volume, jeden Bucket und/oder jedes Objekt separate Anmeldedaten für die Authentifizierung verwendet werden.

Speicher, die den Kunden direkt angeboten werden (z. B. Objektspeicher), müssen einen anderen Pool verwenden als interne Cloud-Funktionen (z. B. Volumes für Rechenknoten).

Motivation: Eine getrennte Speicherung kann versehentliche oder absichtliche Datenverluste verhindern oder zumindest minimieren.

Umsetzungsbeispiel: Implementierung eines separaten Speicherpools für jeden unterschiedlichen Zweck (Objektspeicher, Volumes usw.) und Verwendung eindeutiger Anmeldedaten für die Authentifizierung für jeden Speicherpool, und wenn möglich, wären auch separate Anmeldedaten für die Authentifizierung für jedes Volume, jeden Bucket und/oder jedes Objekt vorzuziehen.

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-51/1.0

6.2. Speicherverschlüsselung

Req 52	Daten auf physischen Festplatten müssen verschlüsselt werden und Verschlüsselungsschlüssel dürfen nicht auf Speicherknoten gespeichert werden.
--------	--

Speicherserver müssen die Daten auf allen Datenträgern verschlüsseln. Externe Speichersysteme müssen, wenn sie verwendet werden, ebenfalls eine Festplattenverschlüsselung verwenden.

Wenn man Verschlüsselungsschlüssel auf den Speicherservern (z. B. sogar auf verschlüsselten Betriebssystemfest-

platten) speichern würde, könnte ein Angreifer die Schlüssel leicht abrufen und die Daten entschlüsseln.

Die Verschlüsselung kann hardware- oder softwarebasiert sein.

(Eine vollständige Verschlüsselung der Betriebssystemfestplatten ist nicht erforderlich, wenn die Betriebssystemfestplatten keine sensiblen Daten oder Geheimnisse enthalten. Dies ermöglicht das unbeaufsichtigte Booten des Betriebssystems, das dann die erforderlichen Schlüssel vom KMS beziehen sollte).

Motivation: Dies verhindert die Möglichkeit von Datenlecks, wenn Festplatten gestohlen, verlegt oder im Rahmen der Garantie zurückgegeben werden, obwohl die ordnungsgemäße Außerbetriebnahme von Festplatten (Löschen und/oder Entmagnetisierung) weiterhin gilt.

Umsetzungsbeispiel: Speicherung der Festplattenverschlüsselungsschlüssel im KMS oder HSM bei Verwendung der vollständigen Festplattenverschlüsselung.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-52/1.0

Req 53 Alle Netzwerkverbindungen zum Speicher müssen verschlüsselt sein.

Alle Netzverbindungen (Zugriff) auf Daten, entweder von Hypervisoren oder Objektspeicher-Proxys für Kunden, müssen verschlüsselt werden.

Motivation: Dies verhindert, dass Angreifer im Netz an Daten im Klartext gelangen.

Umsetzungsbeispiel: Verwendung von TLS für alle Verbindungen zum Speichersystem.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-53/1.0

Req 54 Die Speicherreplikation muss verschlüsselt werden.

Selbst wenn ein dediziertes Netzwerk für die Speicherreplikation verwendet wird, muss die Speicherreplikation verschlüsselt werden.

Motivation: Die Verschlüsselung der Speicherreplikation verhindert, dass Angreifer über das Netz an Daten im Klartext gelangen können.

Umsetzungsbeispiel: Verwendung von TLS für alle internen Verbindungen im Speichersystem (einschließlich Replikation).

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

6.3. Zugang zum Speicher

Req 55	Die direkte Nutzung von Speicherplatz durch Cloud-Kunden (Mandanten) ist nur über einen Proxy erlaubt.
--------	--

Typisch für die direkte Speichernutzung ist die Objektspeicherung, bei der Cloud-Kunden über HTTPS-Verbindungen direkt auf Daten zugreifen, um Objekte zu lesen, zu schreiben, zu ändern und zu löschen.

Der Proxy kann als Web Application Firewall (WAF) realisiert werden, er muss Clients authentifizieren und autorisieren und bösartige Anfragen blockieren. Die Verbindungen vom Client zum Proxy und vom Proxy zum Backend-Speichersystem müssen verschlüsselt werden.

Motivation: Der Speicherserver, der Teil der Speichersoftware ist, z. B. der Webserver im Falle der Objektspeicherung, ist im Allgemeinen nicht ausreichend geschützt, weshalb ein Proxy, der eine zusätzliche Schutzschicht bietet, zwischen den Webserver der Speichersoftware und den Cloud-Kunden geschaltet werden muss.

Umsetzungsbeispiel: Nginx kann als WAF verwendet werden, um Clients zu authentifizieren und zu autorisieren und bösartige Anfragen zu blockieren.

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-55/1.0

Req 56	Der Speicher darf nicht direkt von öffentlichen Netzen aus zugänglich sein.
--------	---

Der Speicherzugriff, auch im Falle der Objektspeicherung über einen Proxy, ist nur für Cloud-Kunden (Mandanten) zulässig. Daher darf der Proxy gemäß der vorstehenden Anforderung nur Verbindungen akzeptieren, die aus dieser Cloud-Umgebung stammen (Verbindungen aus verschiedenen Instanzen derselben Cloud, z. B. Rechenzentren und verschiedenen Standorten/Regionen, sind zulässig). Die Verbindungen können erforderlichenfalls öffentliche IP-Adressen verwenden, aber die Konnektivität muss auf IP-Bereiche beschränkt werden, die zur Cloud oder zu anderen internen Systemen der DTAG gehören.

Motivation: Die Einschränkung des Netzwerkzugriffs auf den Speicher trägt dazu bei, die Angriffsfläche zu verringern.

Umsetzungsbeispiel: Der Proxy kann den Zugriff nur aus IP-Bereichen zulassen, die zur Cloud oder zu anderen internen Systemen der DTAG gehören.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-56/1.0

In Bezug auf alle anderen Sicherheitsanforderungen ist darauf hinzuweisen, dass ein externer Proxy für nicht sensible Daten (z. B. CDN-Lieferung von Softwarepaketen) nicht immer verschlüsselte Verbindungen zu den Clients verwenden muss. Sensible Daten benötigen jedoch eine verschlüsselte Verbindungen.

Auf weitere Einzelheiten wird verzichtet, da der externe Proxy als separate Anwendung betrachtet wird und je nach beabsichtigtem Anwendungsfall bewertet werden muss (z. B. soll der externe Proxy die Authentifizierung auf Anwendungsebene, die Autorisierung usw. übernehmen).

Motivation: Für verschiedene Anwendungsfälle (z. B. CDN - Content Delivery Network), bei denen Objektspeicher für öffentliche Netze offen sein müssen, d. h. von Endkunden oder dem Internet aus zugänglich sein müssen, muss ein zusätzlicher separater Proxy eingerichtet werden, da die Authentifizierung voraussichtlich anders erfolgen wird - z. B. auf Anwendungsebene.

Umsetzungsbeispiel: Der bevorzugte Weg ist, einen solchen Proxy als Anwendung in der Cloud-Umgebung zu betreiben.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-57/1.0

7. Overlay-Netzwerk

Das Cloud-Infrastrukturnetz (auch als Underlay-Netz bezeichnet) dient in der Cloud-Umgebung der Konnektivität zwischen Hypervisoren und wird als Transportmittel für das Overlay-Netz verwendet. Das Cloud-Infrastrukturnetz umfasst im erweiterten Sinne auch die gesamte notwendige Kommunikation innerhalb der Cloud, z. B. die Verwaltungsebene und den Speicherverkehr, wobei anzumerken ist, dass dies nicht ganz zutrifft, da es nicht das Netz von Cloud-Mandanten transportiert, sondern vielmehr deren Anforderungen an die Ressourcenverwaltung und ihre in der Cloud gespeicherten Daten. Das Cloud-Infrastrukturnetz wird in der Regel als eine Kombination aus getrennten Netzen und VLANs bereitgestellt, was jedoch die Anzahl der möglichen Netze, die für die Mandanten nutzbar sind, begrenzt.

Das Overlay-Netz wird, anders als das Cloud-Infrastrukturnetz, in der Regel als VXLAN oder eine Reihe von Tunneln (meist GRE) bereitgestellt. Dieser Ansatz ermöglicht die Schaffung einer ausreichenden Anzahl von Mandantennetzwerken, wobei jeder Mandant mehrere Netzwerke erstellen kann. Die Steuerung des Overlay-Netzwerks erfolgt über einen Software-Defined Network (SDN)-Controller. Die beliebtesten SDN-Softwarelösungen sind OpenStack Neutron und Tungsten Fabric (auch bekannt als Juniper Contrail in der kommerziellen Version). Der SDN-Controller verwaltet in diesem Sinne virtuelle Netzwerke, und die Mandanten erhalten scheinbar private Netzwerke für ihre eigene Nutzung, d. h. sie sehen den Datenverkehr von anderen Mandanten nicht, es sei denn, sie stellen ihre virtuellen Maschinen externen Netzwerken (außerhalb der Cloud, nicht des Unternehmens) wie dem Internet zur Verfügung. Dieses Konstrukt ermöglicht eine nahtlose Konnektivität zwischen virtuellen Maschinen, die auf verschiedenen Hypervisoren laufen, ohne dass Details über das interne Cloud-Infrastrukturnetz in der Cloud preisgegeben werden.

Req 58	DDoS- (und DoS-)Schutz muss zumindest für den Schutz der in der Cloud-Umgebung gehosteten Internet- und Kundendienste verwendet werden. Auch Cloud-APIs müssen gegen DoS und DDoS geschützt werden.
--------	---

In der Cloud gehostete Dienste, die offen für das Internet oder für Kunden sind, sind am anfälligsten für verschiedene DoS- und DDoS-Angriffe. Für diesen Schutz gibt es 2 Lösungen:

- netzwerkbasierter DDoS-Schutz
- Inline-Appliance für DDoS-Schutz

Eine hardwarebasierte Inline-DDoS-Schutz-Appliance bietet im Vergleich zu einem netzwerkbasierten DDoS-Schutz zusätzliche Vorteile wie eine wesentlich schnellere Erkennung und Eindämmung von DDoS-Angriffen. Daher wird eine Inline-Appliance bevorzugt für kritische Dienste eingesetzt, die mit dem Internet oder Kunden in Kontakt stehen.

Virtualisierte DDoS-Abwehrlösungen, die auf Cloud-Rechenknoten betrieben werden, sind nicht effizient genug und dürfen nicht verwendet werden. Software-basierte oder virtualisierte Lösungen, die auf regulären Servern laufen, können verwendet werden, müssen aber inline sein, d. h. sie müssen verhindern, dass bösartiger DDoS-Verkehr zusätzliche Last auf Rechenknoten verursacht.

Das für die Cloud-Umgebung verwendete DDoS-System sollte mit anderen Systemen in den Netzen der DTAG zusammenarbeiten, um ein optimales Schutzniveau zu gewährleisten.

Motivation: Eine ordnungsgemäße Implementierung des DDoS-Schutzes hilft den in der Cloud betriebenen Diensten, DDoS-Angriffen mit minimalen Auswirkungen auf ihre Verfügbarkeit standzuhalten, und verhindert auch Auswirkungen auf andere in der Cloud betriebene Dienste aufgrund von Ressourcenmangel, der durch angegriffene Dienste verursacht wird.

Umsetzungsbeispiel: Wenn die Cloud-Infrastruktur beispielsweise mit AS3320 verbunden ist, kann die bestehende Arbor-Lösung verwendet werden, und es müssen entsprechende Router für die DDoS-Überwachung hinzugefügt werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

- Verfügbarkeit

Req 59	Die Cloud-Plattform muss einen SDN-Controller verwenden, der Overlay-Netze für die Übertragung aller Mandantenverkehre erstellt.
--------	--

Der gesamte Mandantenverkehr in der Cloud muss über das Overlay-Netz abgewickelt werden, mit Ausnahme der Cloud-API-Endpunkte, die auf andere Weise (durch WAF/Proxy) zugänglich sind.

Motivation: Die Übertragung des Netzwerkverkehrs der Mandanten in einem Overlay verhindert, dass die Mandanten jemals das Cloud-Infrastrukturnetzwerk erreichen.

Umsetzungsbeispiel: Die für die Erstellung des Overlay verwendete Technologie kann VLAN, VXLAN, MPLS über UDP, GRE-Tunnel oder eine andere sein, die eine ausreichende Trennung des Datenverkehrs bietet. Bestimmte Technologien wie VLAN sind zwar einfach zu implementieren, schränken aber die Anzahl der möglichen Tenant-Netze stark ein.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-59/1.0

7.1. Allgemeine Anforderungen an das Overlay-Netz

Req 60	Die Mandanten müssen in der Lage sein, ihre Netze von anderen zu trennen.
--------	---

Der SDN-Controller muss es jedem Mandanten ermöglichen, private Netze zu schaffen, die nur für den Mandanten selbst sichtbar und erreichbar sind. Der SDN-Controller muss außerdem jedem Mandanten die Möglichkeit bieten, bestimmte Teile seiner Netze von anderen Netzen desselben Mandanten zu isolieren.

Motivation: Dies ermöglicht es Mandanten, n-Tier-Anwendungen zu erstellen.

Umsetzungsbeispiel: OpenStack mit regulärem Neutron-Netzwerk (Standardbeispiel mit Open vSwitch) erfüllt diese Anforderung.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-60/1.0

Req 61	Der SDN-Controller muss den Mandanten die Möglichkeit bieten, Sicherheitsgruppen (Mikrosegmentierung) für die zustandsabhängige L3/L4-Verkehrsfilerung zu definieren und die Filterung durchzusetzen. Die Mandanten müssen Sicherheitsgruppen verwenden, um ihre virtuellen Maschinen und Dienste zu schützen, insbesondere Management-Schnittstellen und innere Schichten.
--------	---

Es gibt keine herkömmliche Firewall vor den Cloud-VMs, und das SDN verteilt die von den Mandanten beschriebenen Firewall-Regeln an Rechenknoten, die den Datenverkehr filtern. Eine solche Firewall wird in OpenStack als Sicherheitsgruppen bezeichnet, während sie bei VMWare als Mikrosegmentierung bezeichnet wird. Im weiteren Verlauf des Dokuments wird hauptsächlich der Name Sicherheitsgruppen verwendet. Sicherheitsgruppen müssen die Möglich-

keit der zustandsabhängigen L3/L4-Filterung sowohl für eingehenden als auch für ausgehenden Verkehr bieten, einschließlich der Möglichkeit, Regeln für jede virtuelle Maschine separat festzulegen.

Die Mandanten müssen Sicherheitsgruppen für die Verkehrsfilterung verwenden, um den ein- und ausgehenden Verkehr wie folgt zu kontrollieren:

- Regeln müssen nur erlaubten Verkehr zulassen
- Alle anderen Verbindungen und Pakete müssen standardmäßig verworfen

Das per Standard definierte Verwerfen von ausgehenden Verkehr kann für virtuelle Maschinen weggelassen werden, die einen extrem offenen Internetzugang benötigen, der nicht einfach auf einen vernünftigen Regelsatz eingegrenzt werden kann (z. B. ausgehende E-Mail-Server).

Die Verwaltungsschnittstellen aller virtuellen Maschinen und alle Schnittstellen der virtuellen Maschinen, die zu den inneren Schichten der n-Tier-Anwendung gehören (wie Verwaltungsmaschinen und Datenbanken), können nicht direkt von außen erreicht werden. Eine Ausnahme ist in bestimmten Fällen möglich, in denen die internen Netze eines Mandanten in der Cloud über ein geeignetes VPN mit den internen Netzen anderer DTAG verbunden sind (z. B. wenn die Anwendung teilweise in der Cloud und teilweise in der Legacy-Infrastruktur läuft).

Der Mandant kann auch einen Jump-Host einsetzen, um die Angriffsfläche für wichtige Verwaltungsfunktionen zu minimieren und einen zentralen Kontrollpunkt für den Verwaltungszugang zu schaffen.

Motivation: Um Mandanten zu ermöglichen, ihre Arbeitslasten (z. B. VMs) effizienter zu nutzen und besser zu schützen, muss eine Cloud die Möglichkeit der Verkehrsfilterung bieten.

Umsetzungsbeispiel: OpenStack mit regulärem Neutron-Netzwerk (Standardbeispiel mit Open vSwitch) erfüllt diese Anforderung.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-61/1.0

8. Cloud-Nutzung

Clouds werden in der Regel eingesetzt, um die Automatisierung zu ermöglichen und die Kosten zu minimieren. Häufig wird dieselbe Cloud-Umgebung auch für die Bereitstellung von Entwicklungs-, Test-, Referenz- und Produktionssystemen/-anwendungen verwendet. Die Vermischung von Entwicklungs-, Test-, Referenz- und Produktionssystemen birgt ein zusätzliches Risiko. Bei ordnungsgemäßer Anwendung aller Sicherheitsmaßnahmen in diesem Dokument und der besten Sicherheitspraktiken im Allgemeinen ist es möglich, das Risiko auf ein akzeptables Niveau für den Betrieb von Entwicklungs-, Test-, Referenz- und Produktionssystemen in derselben Cloud zu senken.

In diesem Teil des Dokuments werden zusätzlich verbindliche Sicherheitsanforderungen beschrieben, die eine Vermischung von Entwicklungs-, Test-, Referenz- und Produktions-Cloud-Infrastrukturen sowie eine Vermischung von Entwicklungs-, Test-, Referenz- und Produktionssystemen in derselben Cloud-Infrastruktur ermöglichen.

Req 62	Die Cloud-Umgebung (Infrastruktur) muss angemessene Robustheitstests bestehen, um sicherzustellen, dass die implementierten Sicherheitsmaßnahmen wie erwartet funktionieren.
--------	--

Vor der Nutzung der Cloud-Umgebung für Produktionssysteme muss die Cloud-Infrastruktur daraufhin geprüft werden, ob die Sicherheitsmaßnahmen ordnungsgemäß umgesetzt wurden, einschließlich der Prüfung auf Robustheit, Trennung der Mandanten (Netzwerk, Speicher, Verarbeitung) und Quoten. Die Arbeitslasten dürfen sich nicht gegenseitig beeinflussen, d. h. die Arbeitslast eines Mandanten darf nicht dazu führen, dass ein anderer Mandant unter Ressourcenmangel leidet, und zwar bis zu einer Grenze, die durch Überbuchung und SLA festgelegt wurde. Bei hoher Last (durch andere Mandanten und/oder Angriffe) müssen alle Sicherheitsaspekte der Mandantenumgebung funktionsfähig bleiben.

Die Testergebnisse müssen dokumentiert werden. Jedes neue größere Upgrade erfordert wiederholte Tests, z. B. bei einem Wechsel der Hauptversion von Kernel, Hypervisor, Speichersoftware, Netzwerk-Stack usw.

Motivation: Nur eine hinreichend robuste Cloud-Umgebung kann verwendet werden, um mehrere Tenants einzubinden oder verschiedene Arten von Tenants (Entwicklung, Test, Produktion) gemeinsam zu betreiben.

Umsetzungsbeispiel: Die Methoden, die für Sicherheitstests verwendet werden können, variieren je nach Anwendungsfall, aber im Allgemeinen reichen sie von einfachen automatisierten Sicherheitsscans bis hin zu kreativeren Ansätzen für Penetrationstests.

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-62/1.0

8.1. Zweckgebundene Trennung der Cloud-Infrastruktur

Req 63	Die Entwicklungs-, Test- und Referenz-Cloud-Infrastrukturen selbst müssen auf einer von der Produktions-Cloud-Infrastruktur vollständig getrennten Hardware betrieben werden, einschließlich des Cloud-Management- und Orchestrierungssystems.
--------	--

Rechenknoten, Speicherknoten, Netzwerkgeräte und andere unterstützende Systeme, die zur Entwicklungs-, Test- oder Referenz-Cloud-Infrastruktur gehören, müssen auf einer von der Produktions-Cloud-Umgebung getrennten Hardware betrieben werden. Dies gilt auch für einen separaten DCR (Data Center Router).

Selbst wenn die Sicherheitsanforderungen für Test- und Referenzsysteme mit den Sicherheitsanforderungen für Produktionssysteme übereinstimmen, müssen auch betriebliche Aspekte berücksichtigt werden. Das Testen einer neuen Änderung oder Funktion auf gemeinsam genutzter Hardware zwischen Test- und Produktions-Cloud-Umgebungen könnte die gesamte Produktions-Cloud-Umgebung zum Absturz bringen.

Motivation: Entwicklungs-, Test- und Referenzsysteme haben nicht immer dieselben Sicherheitsanforderungen wie Produktionssysteme, und eine Vermischung dieser Systeme würde unnötige Risiken für die Cloud-Produktionsumgebung mit sich bringen.

Umsetzungsbeispiel: Separate (getrennte) Hardware (oder Software oder extern genutzte Dienste) für jede der Cloud-Infrastrukturplattformen für Entwicklung, Tests und Produktion.

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
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-63/1.0

Req 64	Entwicklungs-, Test- und Referenz-Cloud-Infrastrukturen dürfen keine Produktions-Workloads einbinden.
--------	---

Produktionssysteme dürfen nur auf einer Produktions-Cloud-Umgebung laufen. Entwicklungs-, Test- und Referenz-Cloud-Infrastrukturen können nur für die Entwicklung, Prüfung und Verifizierung der Cloud-Infrastruktur verwendet werden.

Das Onboarding von Entwicklungs-, Test- und Referenzsystemen (Workloads) auf Entwicklungs-, Test- und Referenz-Cloud-Infrastrukturen ist für umfassende Tests weiterhin zulässig, wobei die Cloud-Benutzer jedoch auf unterschiedliche SLA- und Sicherheitsmaßnahmen achten müssen.

Motivation: Für Entwicklungs-, Test- und Referenz-Cloud-Infrastrukturen gelten nicht immer dieselben Sicherheitsanforderungen wie für Produktions-Cloud-Infrastrukturen, so dass das Onboarding von Workloads auf Entwicklungs-, Test- oder Referenz-Cloud-Infrastrukturen ein unnötiges Risiko für die Workloads darstellen würde.

Umsetzungsbeispiel: Nutzung der Entwicklungs-, Test- und Referenz-Cloud-Infrastruktur nur für Entwicklungs-, Test- und Referenzzwecke und nicht für das Onboarding von Workloads.

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
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-64/1.0

8.2. Trennung von Systemen/Anwendungen, die in der Cloud laufen

Für die Vermischung von Entwicklungs-, Test-, Referenz- und Produktions-Workloads (Systeme/Anwendungen, die in der Cloud laufen) wird davon ausgegangen, dass die Produktions-Cloud-Umgebung verwendet wird (ausreichend stabile Cloud-Umgebung).

Req 65 Für Entwicklungs-, Test-, Referenz- und Produktionssysteme (Workloads) müssen getrennte Mandanten verwendet werden. Zwischen ihnen dürfen keine gemeinsame Ressourcen geteilt werden.

Die Anforderung, Entwicklungs-, Test-, Referenz- und Produktionssysteme vollständig zu trennen, gilt nach wie vor für Systeme, die in der Cloud laufen, auch wenn die logische Trennung anstelle der physischen Trennung verwendet wird.

Jeder unterschiedliche Workload-Typ (Entwicklung, Test, Referenz, Produktion) muss seinen eigenen Mandanten haben. Diese Mandanten dürfen weder Overlay-Netze noch Speicher gemeinsam nutzen (gilt sowohl für Volumes- als auch für Objektspeicher). Die Verbindung dieser verschiedenen Systemtypen ist ebenfalls nicht zulässig, wie in den geltenden Sicherheitsanforderungen festgelegt.

In Ausnahmefällen kann das verantwortliche PSM die Konnektivität oder den Datenaustausch zwischen Test- und Referenzsystemen oder zwischen Referenz- und Live-Systemen erlauben. Dies muss in streng kontrollierter Weise geschehen und sollte in Umfang und Dauer begrenzt sein. Kontrolliert bedeutet, dass folgende Punkte erfüllt sind:

- eine angemessene Firewall oder ein Proxy für die Netzwerkkonnektivität
- geeignetes System zur Datenmanipulation (z.B. Anonymisierung, Tokenisierung, ...) im Falle eines Datenaustauschs (Speicherung)

Eine Firewall oder ein Proxy muss den Schutz zwischen verschiedenen Systemtypen gewährleisten, damit ein Angreifer, der sich z. B. Zugang zum Referenzsystem verschafft hat, nicht automatisch Zugang zum Produktionssystem erhält.

Beispiel für einen ordnungsgemäßen Datenaustausch: Das Anonymisierungssystem befindet sich zwischen dem Produktions- und dem Referenzsystem und übernimmt Daten aus dem Objektspeicher der Produktion, anonymisiert die Daten und legt die anonymisierten Daten im Referenzobjektspeicher ab.

Motivation: Die Trennung von Umgebungen für Entwicklungs-, Test-, Referenz- und Produktionssysteme muss auf alle Cloud-Ressourcen angewandt werden.

Umsetzungsbeispiel: Beispiel für einen ordnungsgemäßen Datenaustausch: Das Anonymisierungssystem befindet sich zwischen dem Produktions- und dem Referenzsystem und übernimmt die Daten aus dem Objektspeicher des Produktionssystems, anonymisiert sie und legt die anonymisierten Daten im Objektspeicher des Referenzsystems ab.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-65/1.0

Req 66 Entwicklungs-, Test- und Referenzsysteme (Workloads) dürfen nicht direkt vom Internet oder von Kunden aus erreichbar sein.

Es ist nicht gestattet, Entwicklungs-, Test- und Referenzsysteme für Dritte (einschließlich Kunden) oder das Internet weithin zugänglich zu machen.

In Ausnahmefällen kann eine vorübergehende, kontrollierte, begrenzte Verbindung zu Dritten und/oder zum Internet gestattet werden, damit die Systeme für die künftige Produktion umfassend getestet werden können (es gelten jedoch weiterhin die entsprechenden Sicherheitsmaßnahmen).

Motivation: Auch wenn Entwicklungs-, Test- und Referenzsysteme in der Regel das gleiche Sicherheitsniveau haben wie Produktionssysteme, haben sie aufgrund ihrer Beschaffenheit in der Regel ein niedrigeres Sicherheitsniveau als Produktionssysteme, und ihre Öffnung für das Internet oder für Kunden könnte gefährlich sein. Außerdem können sie mit gefälschten Daten arbeiten.

Umsetzungsbeispiel: Die Erreichbarkeit von Entwicklungs-, Test- und Referenzsystemen muss auf die Parteien, die für die Entwicklung und den Test dieser Systeme Zugang haben müssen, beschränkt werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-66/1.0

Req 67	Datenschutzrelevante Kundendaten und andere sensible Daten dürfen nicht auf Entwicklungs-, Test- und Referenzsystemen verwendet werden.
--------	---

Diese Anforderung gehört zur regulären Liste der Datenschutzanforderungen (in Anlehnung an geltende Gesetze und Bestimmungen, ID: 911.43-7/6.0), dennoch lohnt es sich, die wichtigsten Punkte hier zu wiederholen.

Entwicklungs-, Test- und Referenzsysteme dürfen nicht verarbeitet werden:

- Daten von echten Kunden
- Datenschutzrelevante Daten
- interne oder geschäftskritische Daten
- andere sensible Daten

Motivation: Auch wenn Entwicklungs-, Test- und Referenzsysteme ein geringeres Sicherheitsniveau haben und leichter kompromittiert werden können, würde der Angreifer keinen Zugang zu echten Daten erhalten.

Umsetzungsbeispiel: Verwendung nur künstlich erzeugter, anonymisierter oder pseudonymisierter Daten (je nach Datentyp) für Entwicklungs-, Test- und Referenzsysteme.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-67/1.0

8.3. Mandantenspezifisch

Req 68	Die Daten des Mandanten müssen während der Übertragung oder im Ruhezustand verschlüsselt werden.
--------	--

Je nach Datenklassifizierung und Sicherheitsstufe der Cloud-Infrastruktur (und des Netzes, das die verschiedenen Cloud-Umgebungen miteinander verbindet) ist es erforderlich, dass:

- der gesamte Netzwerkverkehr zwischen virtuellen Maschinen (oder Containern, die sich in verschiedenen virtuellen Maschinen befinden) verschlüsselt wird.
- Daten, die auf Block- oder Objektspeichern gespeichert sind, verschlüsselt werden.

Die in der Cloud bereitgestellten Anwendungen können auf einem einzigen Hypervisor, innerhalb derselben Cloud-Umgebung (Rechenzentrum) oder verteilt auf verschiedene Cloud-Umgebungen (Rechenzentren) laufen. Obwohl die Konnektivität für den Mandanten transparent sein kann, müssen sich die Mandanten darüber im Klaren sein, dass die Kommunikation zwischen ihren Workloads über Netzkabel auf öffentlichem Grund erfolgt. Daher muss der gesamte Datenverkehr des Mandanten, der eine einzelne Workload-Einheit verlässt (virtuelle Maschine oder ein Container, der mit anderen Containern kommuniziert, die sich an einem anderen Ort befinden können), verschlüsselt werden. Es empfiehlt sich, den gesamten Datenverkehr zu verschlüsseln, um sicherzustellen, dass die Anwendung im Falle von Änderungen in den Cloud-Umgebungen oder der weiteren Bereitstellung der Anwendung an mehreren Standorten nicht neu archiviert werden muss. Die Verschlüsselung innerhalb des Rechenzentrums bietet auch zusätzlichen Schutz vor Hackern, die in die Cloud-Infrastruktur eingedrungen sind, oder vor unseriösen Cloud-Administratoren, so dass sie auch dann von Vorteil ist, wenn die Cloud-Umgebungen über verschlüsselte Verbindungen verbunden sind.

Motivation: Nicht alle Cloud-Umgebungen können an vollständig sicheren Standorten bereitgestellt werden (z. B. "Edge Clouds"), und trotz der von der Plattform angebotenen Festplattenverschlüsselung wären Angreifer, die sich Zugang zur Cloud-Infrastruktur verschafft haben, nicht in der Lage, die Daten leicht zu extrahieren, wenn die auf Volumes und in Objektspeicher-Buckets gespeicherten Daten verschlüsselt sind. Verschlüsselte Daten in Speicher-Buckets mit ordnungsgemäßer Verwendung verschiedener Schlüssel für verschiedene Buckets helfen auch, versehentliche Datenlecks zu verhindern, entweder für die Öffentlichkeit oder für andere Arbeitslasten (z. B. versehentliche Übertragung von der Produktion auf das Testsystem).

Umsetzungsbeispiel: Verwendung von sicheren Kommunikationsprotokollen (z. B. HTTPS, TLS und SSH) für die Kommunikation und Verwendung von Verschlüsselung für ruhende Daten - verschlüsselte Festplatten oder Objekte.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-68/1.0

Req 69	Die Daten des Mandanten müssen gesichert werden.
--------	--

Die Mandanten müssen über angemessene Sicherungsverfahren verfügen und alle erforderlichen Daten (einschließlich Konfigurationsdateien, Bilder usw.) sichern, um das System im Falle einer Ransomware-Infektion wiederherstellen zu können.

Die Datenreplikation, die in diesem Zusammenhang ebenfalls eine gängige Methode ist, ist kein Ersatz für ein Backup, denn bei der Replikation werden fehlerhafte oder durch Ransomware verschlüsselte Bits problemlos repliziert. Snapshots können auch nicht als richtige Datensicherung angesehen werden, weil:

- Snapshots gewährleisten nicht die Integrität der Daten (einige unsaubere Daten könnten sich noch im Speicher befinden und nicht auf die Festplatte gespielt werden, wie bei DBMS)
- ein Snapshot speichert Daten auf demselben Speichergerät wie die Quelldaten

Motivation: Die Anforderung ist aus betrieblichen Gründen ziemlich einfach, wird aber hier speziell wegen des Sicherheitsaspekts erwähnt. Ransomware ist für Hacker ein sehr profitabler Weg, um Geld zu verdienen.

Umsetzungsbeispiel: In Bezug auf die Cloud könnte ein Beispiel für eine ordnungsgemäße Sicherung einen schreibgeschützten Speicherbereich umfassen, in dem ein Tenant die Sicherungen speichern kann, aber nicht in der Lage ist, vorhandene Objekte zu lesen oder zu ändern. Ein anderer Tenant (oder ein Benutzer mit einer anderen Rolle) könnte die Berechtigung haben, die Sicherungen zu lesen und zu löschen, während die Änderung generell für beide verboten sein sollte.

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

Für diese Anforderung sind folgende Gewährleistungsziele relevant:

ID: 3.86-69/1.0

9. Referenzen

Einige Referenzen aus dem Dokument:

<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>

10. Glossar

Die Definitionen für öffentliche, private, gemeinschaftliche und hybride Clouds sowie die Definitionen für IaaS, PaaS und SaaS stammen vom NIST.

Public Cloud

Die Cloud-Infrastruktur wird zur offenen Nutzung durch die Allgemeinheit bereitgestellt. Sie kann im Besitz eines Unternehmens, einer akademischen oder staatlichen Organisation oder einer Kombination dieser Organisationen sein und von diesen verwaltet und betrieben werden. Sie befindet sich in den Räumlichkeiten des Cloud-Anbieters.

Private Cloud

Die Cloud-Infrastruktur wird zur ausschließlichen Nutzung durch eine einzelne Organisation mit mehreren Nutzern (z. B. Geschäftseinheiten) bereitgestellt. Sie kann sich im Besitz der Organisation, eines Dritten oder einer Kombination aus beiden befinden und von diesen verwaltet und betrieben werden, und sie kann innerhalb oder außerhalb der Räumlichkeiten existieren.

Community Cloud

Die Cloud-Infrastruktur wird für die ausschließliche Nutzung durch eine bestimmte Gemeinschaft von Nutzern aus Organisationen bereitgestellt, die gemeinsame Anliegen haben (z. B. Auftrag, Sicherheitsanforderungen, Richtlinien und Compliance-Überlegungen). Sie kann im Besitz einer oder mehrerer Organisationen in der Gemeinschaft, einer dritten Partei oder einer Kombination von ihnen sein und von diesen verwaltet und betrieben werden, und sie kann innerhalb oder außerhalb der Geschäftsräume existieren.

Hybrid Cloud

Die Cloud-Infrastruktur ist eine Zusammensetzung aus zwei oder mehr verschiedenen Cloud-Infrastrukturen (privat, gemeinschaftlich oder öffentlich), die zwar eigenständige Einheiten bleiben, aber durch standardisierte oder proprietäre Technologien miteinander verbunden sind, die die Portabilität von Daten und Anwendungen ermöglichen (z. B. Cloud-Bursting für den Lastausgleich zwischen Clouds).

IaaS

Die dem Verbraucher zur Verfügung gestellte Fähigkeit besteht in der Bereitstellung von Verarbeitungs-, Speicher-, Netz- und anderen grundlegenden Rechenressourcen, auf denen der Verbraucher beliebige Software, einschließlich Betriebssystemen und Anwendungen, einsetzen und ausführen kann. Der Kunde verwaltet oder kontrolliert die zugrunde liegende Cloud-Infrastruktur nicht, hat aber die Kontrolle über Betriebssysteme, Speicherplatz und bereitgestellte Anwendungen sowie möglicherweise eine begrenzte Kontrolle über ausgewählte Netzkomponenten (z. B. Host-Firewalls).

PaaS

Die dem Kunden zur Verfügung gestellte Fähigkeit besteht darin, in der Cloud-Infrastruktur vom Kunden erstellte oder erworbene Anwendungen einzusetzen, die mit den vom Anbieter unterstützten Programmiersprachen, Bibliotheken, Diensten und Tools erstellt wurden. Der Kunde verwaltet oder kontrolliert nicht die zugrunde liegende Cloud-Infrastruktur, einschließlich Netzwerk, Server, Betriebssysteme oder Speicher, sondern hat die Kontrolle über die bereitgestellten Anwendungen und möglicherweise die Konfigurationseinstellungen für die Anwendungshosting-Umgebung.

SaaS

Der Verbraucher hat die Möglichkeit, die Anwendungen des Anbieters zu nutzen, die in einer Cloud-Infrastruktur laufen. Der Zugriff auf die Anwendungen erfolgt von verschiedenen Client-Geräten aus entweder über eine Thin-Client-Schnittstelle, wie einen Webbrowser (z. B. webbasierte E-Mail), oder über eine Programmschnittstelle. Der Verbraucher verwaltet oder steuert die zugrunde liegende Cloud-Infrastruktur einschließlich Netzwerk, Server, Betriebssysteme, Speicher oder sogar einzelne Anwendungsfunktionen nicht, mit der möglichen Ausnahme begrenzter benutzerspezifischer Anwendungskonfigurationseinstellungen.