SYS: IT-Systeme

SYS.1.6: Container

1 Beschreibung

1.1 Einleitung

Der Begriff „Container“ bezeichnet eine Technik, bei der ein Wirtssystem mehrere Anwendungen parallel in separierten Umgebungen ausführt (Operating Stem Level Virtualization). In den meisten Fällen erfolgt die Überwachung, das Starten und Beenden und die weitere Verwaltung der Container durch eine Verwaltungssoftware, die somit die sogenannte Orchestrierung übernimmt. Die Orchestrierung erfolgt dabei zumeist in Gruppen von gemeinsam verwalteten Container-Hosts in einem oder mehreren sogenannten Clustern. Ohne die automatisierte Orchestrierung mit der Verwaltungssoftware ist ein Betrieb von Containern zwar möglich, aber der manuelle Betrieb oder der Betrieb über eigens erstellte Skripte ist in der Praxis nur selten anzutreffen.

Um Container zu betreiben und zu verwalten, haben sich mehrere Produkte etabliert, die es erlauben, auch sehr große Umgebungen zu bedienen. Hier ist zwischen der eigentlichen Container-Runtime, die die Prozesse auf den Container-Hosts betreibt, und der Orchestrierung, die die Runtimes auf mehreren Container-Hosts steuert, zu unterscheiden.

Der Betrieb von Containern benötigt eine spezialisierte Infrastruktur, zu der z. B. Cluster-Betriebssoftware, Image Registries, Automatisierungswerkzeuge, Verwaltungsserver, Speichersysteme und virtuelle Netze sowie Server gehören.

1.2 Zielsetzung

Ziel dieses Bausteins ist der Schutz von Informationen, die in Containern verarbeitet, angeboten oder darüber übertragen werden. Der Baustein behandelt, wie Container grundsätzlich abgesichert, wie sie orchestriert und wie die verwendeten Images verwaltet werden können. Dabei wird zwischen dem eigentlichen Container-Dienst und der Cluster-Betriebssoftware, also der Software, die für Betrieb und Verwaltung der Container zuständig ist, und den Anwendungsdiensten, die in den Containern ausgeführt werden, unterschieden.

1.3 Abgrenzung und Modellierung

Der Baustein SYS.1.6 *Container* ist immer anzuwenden, wenn Serverdienste und -anwendungen in Containern betrieben werden.

Dieser Baustein betrachtet Container und ihre Orchestrierung unabhängig vom verwendeten Produkt, die Anforderungen orientieren sich aber an den Fähigkeiten derzeit im Markt befindlicher Produkte.

Der Baustein enthält grundsätzliche Anforderungen zur Einrichtung, zum Betrieb und zur Orchestrierung von Containern sowie zur Image Registry, dem Infrastrukturdienst für die Verwaltung

und Bereitstellung von Container-Images. Die weiteren im Container-Umfeld üblichen Dienste, wie z. B. Automatisierung für CI/CD-Pipelines und Codeverwaltung in GIT, behandelt dieser Baustein nicht in der Tiefe.

Er konkretisiert und ergänzt die Aspekte, die in den Bausteinen SYS.1.1 *Allgemeiner Server* und SYS.1.3 *Server unter Unix* sowie SYS.1.2.2 *Windows Server 2012* behandelt werden, um Spezifika von Containern. Die Anforderungen dieser Bausteine sollten von den Container-Wirten (Hosts) erfüllt werden, unabhängig davon, ob diese selbst auf physischen Servern ausgeführt werden oder virtualisiert sind.

Container werden unabhängig vom Einsatzzweck der darin betriebenen Dienste bzw. Anwendungen betrachtet. Sicherheitsanforderungen möglicher Dienste, wie z. B. Webserver (APP.3.2 *Webserver*) oder Server für Groupware (siehe APP.5.1 *Groupware*), sind Gegenstand eigener Bausteine. Das Thema Virtualisierung wird im Baustein SYS.1.5 *Server-Virtualisierung* beleuchtet.

Der Schwerpunkt des Bausteins liegt auf dem Betrieb von Serverdiensten und -anwendungen. Die Isolation von Anwendungen, wie Browsern auf Clients, wird nicht betrachtet.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind im Bereich Container von besonderer Bedeutung:

2.1 Schwachstellen in Images

Container werden auf Basis von vorgefertigten Images erstellt, die häufig aus dem Internet bezogen oder selbst erstellt werden. In diesen Images ist die Software enthalten, aus denen der IT-Betrieb eigene Images erstellt oder die er um die zu betreibende Software ergänzt.

Die in den Images enthaltene Software könnte verwundbar und die aus dem Image erstellten Serverdienste könnten somit angreifbar sein. Solche Schwachstellen sind oft dem IT-Betrieb nicht bekannt, da die in den Images enthaltene Software nicht in der eigenen Software-Verwaltung erfasst ist.

Sind neue Schwachstellen in der enthaltenen Software vorhanden, ist es nur mit zusätzlichen Werkzeugen möglich, diese zu erkennen und in das Schwachstellenmanagement der Institution aufzunehmen.

2.2 Administrative Zugänge ohne Absicherung

Um Container-Dienste zu verwalten, benötigen die Administratoren und die toolgestützte Orchestrierung administrative Zugänge. Diese Zugänge sind entweder als Sockets oder Ports für Netzzugänge ausgeführt. Mechanismen zur Authentisierung und Verschlüsselung der administrativen Zugänge sind häufig vorhanden, aber nicht bei allen Produkten standardmäßig aktiviert.

Wenn Unbefugte auf das Datennetz oder auf die Container-Hosts zugreifen, können sie über ungeschützte administrativen Zugänge Befehle ausführen, die der Verfügbarkeit, Vertraulichkeit und Integrität der verarbeiteten Daten schaden.

2.3 Tool-basierte Orchestrierung ohne Absicherung

Sofern eine größere Anzahl von Containern in Betrieb ist, wird zumeist eine Software zur Orchestrierung zur Verwaltung der Container eingesetzt. Diese Software kann selbst über Schwachstellen verfügen oder nicht ausreichend gegen unbefugte Nutzung abgesichert sein.

Auf diese Weise kann ein Angreifer Befehle auf den Container-Hosts mit administrativen Berechtigungen ausführen. Dienste können abgeschaltet, Daten gelöscht oder eingesehen werden.

2.4 Ausbruch aus dem Container

Sollte ein Angreifer in der Lage sein, im Container eigenen Code auszuführen, kann er möglicherweise aus dem Container ausbrechen und auf den Container-Host zugreifen. Dieser Angriff kann z. B. über

Schwachstellen in Prozessoren, im Betriebssystem-Kernel oder in lokal angebotenen Infrastruktur-Diensten wie z. B. DNS oder SSH erfolgen.

In der Folge könnte ein Angreifer die Kontrolle über den Container-Host oder andere Server aus der Infrastruktur übernehmen und so unbefugt Daten einsehen, verändern und löschen oder andere Container, Hosts oder Infrastrukturdienste angreifen.

2.5 Datenverluste durch fehlende Persistenz

Container sind von ihrem Aufbau her dafür gedacht, nur eine bestimmte Zeit lang ausgeführt zu werden, und die Verwaltungssoftware kann sie jederzeit abschalten. Wird dies nicht beachtet, könnten Anwendungen in Containern Daten speichern, die sich ausschließlich im Container befinden. Wird eine neue Instanz des Containers gestartet, beispielsweise bei einem Update des Images oder der betriebenen Anwendung, sind alle diese Daten verloren.

Nutzdaten der Anwendung werden in der Regel geeignet gesichert. Bei dateibasierten Protokolldaten oder Zwischenergebnissen der Verarbeitung fällt eine fehlende Datensicherung nur dann auf, wenn ein Container beendet und entfernt ist und die enthaltenen Daten unwiderruflich verloren sind. Sind die Protokolldaten oder Zwischenergebnisse verloren, kann die Verarbeitung nicht lückenlos dokumentiert und deren Ergebnisse können unter Umständen nicht mehr nachvollzogen werden.

2.6 Vertraulichkeitsverlust von Zugangsdaten

Aufbau und Erstellung von Images für Container machen es oft notwendig, dass Zugangsdaten im Container verfügbar sind, z. B. für Datenbanken. Oft liegen sie dann ungeschützt im Image. Über die Images selbst, die Skripte zur Erstellung der Images oder die Versionskontrolle der Skripte könnten diese Zugangsdaten in unbefugte Hände gelangen.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.1.6 *Container* aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	-

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein *SYS.1.6 Container* vorrangig erfüllt werden.

SYS.1.6.A1 Planung des Container-Einsatzes (B)

Bevor Container eingesetzt werden, MÜSSEN alle sicherheitsrelevanten Aspekte der Installation, des Betriebs und der Außerbetriebnahme geplant werden. Diese Planung SOLLTE angemessen dokumentiert werden.

SYS.1.6.A2 Planung der Separierung der Anwendungen in Containern (B)

Vor der Inbetriebnahme MUSS geplant werden, wie die in Containern betriebenen Anwendungen und deren unterschiedlichen Test- und Produktions-Betriebsumgebungen separiert werden. Auf Basis des Schutzbedarfs der Anwendungen, des Netzzonenkonzepts und einer Risikobetrachtung MUSS die Planung festlegen, welche Architektur angemessen auf die Risiken eingeht.

SYS.1.6.A3 Planung der Verwaltung und Orchestrierung (B)

Die Verwaltung und Orchestrierung der Container DARF NUR nach einer geeigneten Planung erfolgen. Die Planung MUSS den gesamten Lebenszyklus von Inbetrieb- bis Außerbetriebnahme inklusive Betrieb und Updates umfassen. Die Orchestrierung MUSS die Container überwachen, starten, stoppen und nach festgelegten Regeln verschieben, um so die Verfügbarkeit der Dienste auch bei Ausfall eines Container-Hosts zu gewährleisten. Sie SOLLTE Schnittstellen für Automatisierungs-Software (CI/CD) anbieten.

SYS.1.6.A4 Härtung des Host-Systems (B)

Es DÜRFEN NUR für den Einsatz als Container-Host benötigte Dienste und Anwendungen auf dem Host-System installiert sein. Die Konfiguration des Host-Systems MUSS angemessen gehärtet werden.

Server für den Betrieb als Container-Host DÜRFEN KEINE Dienste betreiben, die nicht für den Betrieb der Container notwendig sind.

SYS.1.6.A5 Separierung der Container (B)

Der Betriebssystem-Kernel MUSS über Namespaces (wie Linux cgroups) oder andere geeignete Mechanismen die Container voneinander und von anderen Prozessen auf dem Container-Host trennen. Die Trennung MUSS dabei mindestens Prozess-IDs, Inter-Process-Kommunikation, Benutzer-IDs, Dateisystem und Netz inklusive Hostname umfassen.

Wenn der Container-Dienst oder die Cluster-Betriebssoftware mehrere Container miteinander in einer Einheit betreibt, dürfen diese Einheiten sich einen Namespace teilen.

SYS.1.6.A6 Verwendung sicherer Images (B)

Es MUSS sichergestellt sein, dass Images nur aus vertrauenswürdigen Verzeichnissen (Registries) stammen. Sie MÜSSEN unverändert und frei von bekannten Schwachstellen sind.

Signaturen MÜSSEN jedes Image gegen Veränderung und falsche Herausgeber absichern. Die Quelle MUSS danach ausgewählt werden, dass der Anbieter die enthaltene Software regelmäßig auf Sicherheitsprobleme prüft, diese behebt und dies seinen Kunden zusichert.

Die verwendete Version von Basis-Images DARF NICHT abgekündigt („deprecated“) sein. Es MÜSSEN Versionsnummern angegeben sein. Um Updates nicht zu behindern, SOLLTE die Versionsangabe NICHT die Minor-Version enthalten.

SYS.1.6.A7 Härtung der Software im Container (B)

Alle nicht benötigten Bestandteile der Anwendung bzw. des Dienstes, die bzw. der im Container ausgeführt wird, MÜSSEN deinstalliert werden. Die Konfiguration der Anwendung bzw. des Dienstes MUSS angemessen gehärtet werden.

SYS.1.6.A8 Persistenz von Protokollierungsdaten (B)

Die Protokollierung MUSS den Betrieb der Container-Hosts, der Containern und der Orchestrierung vollständig erfassen. Notwendige Protokollierungsdaten MÜSSEN persistent außerhalb der Container gespeichert werden.

SYS.1.6.A9 Persistenz von Nutzdaten (B)

Nutzdaten, auf die durch Anwendungen bzw. Dienste im Container zugegriffen wird oder die sie dauerhaft abspeichern, MÜSSEN persistent außerhalb des Containers gespeichert werden.

SYS.1.6.A10 Speicherung von Zugangsdaten (B)

Zugangsdaten MÜSSEN so gespeichert und verwaltet werden, dass nur berechtigte Personen und Container hierauf zugreifen können. Insbesondere MUSS sichergestellt sein, dass Zugangsdaten nur an zugangsgeschützten Orten und nicht in den Images liegen. Die von der Verwaltungssoftware bereitgestellten Verwaltungsmechanismen für Zugangsdaten SOLLTEN eingesetzt werden.

Folgende Zugangsdaten MÜSSEN mindestens berücksichtigt werden:

- Passwörter jeglicher Accounts,

- API-Keys für von der Anwendung genutzte Dienste sowie
- Private Schlüssel bei Public-Key Authentisierung.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein SYS.1.6 *Container*. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.1.6.A11 Richtlinie für Betrieb und Images (S)

Es SOLLTE eine Richtlinie existieren, die die Anforderungen an den Betrieb der Container, der Cluster-Betriebssoftware und die Container-Images festlegt. Die Richtlinie SOLLTE auch Anforderungen an die Automatisierung der Verwaltung, der Bereitstellung der Images und des Betriebs enthalten.

SYS.1.6.A12 Nur eine Anwendung bzw. ein Dienst pro Container (S)

Jeder Container SOLLTE jeweils nur eine Anwendung bzw. einen Dienst bereitstellen. Eine Gruppierung von mehreren Anwendungen bzw. Diensten in eine funktionale Einheit SOLLTE erfolgen, indem die Orchestrierung die Container als eine Gruppe betreibt.

SYS.1.6.A13 Freigabe von Images und Konfigurationen (S)

Alle Images für den produktiven Betrieb SOLLTEN einen geeigneten Freigabeprozess durchlaufen. Änderungen an den Konfigurationsdateien, die Betrieb, Architektur, Images und Datennetze definieren, SOLLTEN ebenfalls in den Freigabeprozess integriert werden.

SYS.1.6.A14 Updates von Containern (S)

Wenn sicherheitsrelevante Updates der zugrundeliegenden Images oder der betriebenen Software bzw. des betriebenen Dienstes erscheinen, SOLLTEN die Images für die Container neu erstellt und daraus neue Container instanziiert werden. Container auf Basis veralteter Images SOLLTEN dann beendet werden.

Beim Start eines Containers SOLLTE der Container-Dienst immer auf die aktuell verfügbare Version des Images prüfen und eine vorhandene neue Version herunterladen. Auf dem Container-Host zwischengespeicherte alte Versionen DÜRFEN dann NICHT gestartet werden.

SYS.1.6.A15 Unveränderlichkeit der Container (S)

Die Container SOLLTEN ihr Dateisystem während der Laufzeit nicht verändern können.

SYS.1.6.A16 Limitierung der Ressourcen pro Container (S)

Für jeden Container SOLLTEN Ressourcen auf dem Host-System, wie CPU sowie flüchtiger und persistenter Speicher, angemessen limitiert werden.

SYS.1.6.A17 Einbinden von Massenspeichern in Container (S)

Die Container SOLLTEN NUR auf die für den Betrieb notwendigen Massenspeicher und Verzeichnisse zugreifen können. Wenn Schreibrechte nicht benötigt werden, SOLLTEN diese entfernt werden. Sofern Container lokale Speicher einbinden, SOLLTEN die Zugriffsrechte im Dateisystem auf den Service-Account des Containers eingeschränkt sein. Bei Netzspeicher SOLLTE diese Berechtigung auf dem Netzspeicher gesetzt sein.

SYS.1.6.A18 Absicherung der Wirk- und Administrations-Netze (S)

Die Netze für die Administration der Hosts, die Administration des Container-Dienstes und die einzelnen Netze der Anwendungsdienste SOLLTEN separiert werden.

Es SOLLTEN NUR die für den Betrieb notwendigen Netzports der Container in die dafür vorgesehenen Produktivnetze freigegeben werden.

Die zur Administration der Container-Hosts, der Container-Dienste und der Cluster-Betriebssoftware notwendigen Netzports SOLLTEN NUR aus dem Administrationsnetz erreichbar sein, Ausnahme sind hier die Container der Cluster-Betriebssoftware inklusive der Container des Netz-Managements („CNI“), die per SSH, mit lokalen Agenten der Cluster-Betriebssoftware und der Datenhaltung der

Cluster-Betriebssoftware oder dem Container-Host kommunizieren.

SYS.1.6.A19 Verwendung vorgelagerter Ein- und Ausgangssysteme (S)
Sofern mehrere Container-Hosts in einem Verbund arbeiten („Cluster"), SOLLTEN dedizierte Container-Hosts die Ein- und Ausgabe zu anderen Netzen übernehmen. Die anderen Container-Hosts SOLLTEN NICHT aus anderen Netzen außer dem Administrationsnetz erreichbar sein.

SYS.1.6.A20 Absicherung von Konfigurationsdaten und Automatisierung (S)
Die Beschreibung der Container-Konfigurationsdaten SOLLTE versioniert und annotiert erfolgen. Zugangsrechte auf die Verwaltungssoftware der Konfigurationen SOLLTEN minimal vergeben werden. Nur der notwendige Kreis von Personen SOLLTE die Berechtigung haben, Prozesse der Automatisierung auszulösen.

SYS.1.6.A21 Container-Ausführung ohne Privilegien (S)
Alle Anwendungsdienste in Containern SOLLTEN nur unter einem nicht privilegierten Account gestartet werden. Sie SOLLTEN NICHT über erweiterte Privilegien für die Container-Dienste oder die Cluster-Betriebssoftware verfügen.

SYS.1.6.A22 Absicherung von Hilfsprozessen der Automatisierung (S)
Alle Prozesse der Automatisierungssoftware SOLLTEN nur mit minimalen Rechten arbeiten. Wenn unterschiedliche Benutzergruppen über die Automatisierungssoftware die Konfiguration verändern können, SOLLTE dies für jede Gruppe durch eigene Prozesse durchgeführt werden, die nur die für die jeweilige Benutzergruppe notwendigen Rechte besitzen.

SYS.1.6.A23 Administrativer Fernzugriff auf Container (S)
Es SOLLTE sichergestellt sein, dass der administrative Fernzugriff nur auf die Cluster-Betriebssoftware oder den Container-Host und nur über diese auf die Container selbst erfolgen kann. Container SOLLTEN selbst keine Dienste für administrativen Fernzugriff enthalten.

SYS.1.6.A24 Identitäts- und Berechtigungsmanagement für die Container-Verwaltung (S)
Die Verwaltungssoftware SOLLTE jede Aktion eines Benutzers oder im automatisierten Betrieb einer entsprechenden Software authentifizieren und autorisieren, unabhängig davon, ob die Aktionen über eine Weboberfläche oder über eine API erfolgt. Aktionen SOLLTEN NICHT anonym erfolgen.

SYS.1.6.A25 Service-Accounts für Container (S)
Container SOLLTEN jeweils eigene Service-Accounts nutzen, um miteinander und mit den Diensten der Cluster-Betriebssoftware authentifiziert zu kommunizieren, Gruppen von Containern können, wenn sie gleiche Aufgaben haben, einen gemeinsamen Service-Account nutzen. Berechtigungen für die Service-Accounts SOLLTEN nur minimal vergeben sein.

Jeder Dienst, der einen Service-Account nutzt, SOLLTE ein eigenes Token erhalten.

SYS.1.6.A26 Accounts der Anwendungsdienste in Containern (S)
Die Accounts der Prozesse in den Containern SOLLTEN keine Berechtigungen auf dem Container-Host haben. Wenn dies dennoch notwendig ist, SOLLTEN diese Berechtigungen nur für unbedingt notwendigen Daten gelten.

SYS.1.6.A27 Überwachung der Container (S)
Jedes Image SOLLTE einen Health-Check für den Start und den Betrieb („readiness" und „liveness") definieren. Diese Checks SOLLTEN Auskunft über die Verfügbarkeit der Anwendung im Container geben. Sie SOLLTEN fehlschlagen, wenn die Anwendung nicht in der Lage ist, ihre Aufgaben ordnungsgemäß wahrzunehmen.

Der Container-Dienst oder die Cluster-Betriebssoftware SOLLTEN diese Checks überwachen und Container, bei denen die Checks fehlschlagen, beenden und durch neue Instanzen ersetzen.

SYS.1.6.A28 Absicherung der Registry für Images (S)
Sofern eine eigene Registry für Images eingesetzt wird, SOLLTE diese ausreichend abgesichert sein.

Dabei SOLLTEN beachtet werden:

- Verwendung von personenbezogenen und Service-Accounts für den Zugang,
- minimale Vergabe der Berechtigungen,
- Anbindung der Software für die Überwachung der Images auf Verwundbarkeiten,
- Protokollierung der Veränderungen der Images und
- die Datensicherung.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein SYS.1.6 *Container* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

SYS.1.6.A29 Automatisierte Auditierung von Containern (H)

Die gesamte Software in den Images SOLLTE automatisiert katalogisiert werden. Sie SOLLTE mindestens täglich mit aktualisierten Datenbanken über bekannte Verwundbarkeiten abgeglichen werden. Auch die Einstellungen des Containers selbst sowie die des betriebenen Anwendungsdienstes SOLLTEN automatisiert mit einer Liste der erlaubten Einstellungen abgeglichen werden. Nur Container, die geeignet überprüft wurden, SOLLTEN für den Einsatz im Produktivbetrieb freigegeben werden. Die Orchestrierung SOLLTE diese Prozesse automatisieren.

SYS.1.6.A30 Eigene Trusted Registry für Container (H)

Images SOLLTEN nur in einem eigenen Verzeichnis (Registry) bereitgestellt werden. Es SOLLTE durch technische Maßnahmen sichergestellt sein, dass nur Images aus dieser Registry eingesetzt werden.

SYS.1.6.A31 Erstellung erweiterter Richtlinien für Container (H)

Erweiterte Richtlinien SOLLTEN die Berechtigungen der Container und der betriebenen Anwendungsdienste einschränken. Die Richtlinien SOLLTEN folgende Zugriffe einschränken:

- Netzverbindungen,
- Dateisystem-Zugriffe und
- Kernel-Anfragen (Syscalls).

SYS.1.6.A32 Host Based Intrusion Detection für Container (H)

Die Container und die betriebenen Anwendungsdienste SOLLTEN überwacht werden. Abweichungen vom normalen Verhalten SOLLTEN erkannt und gemeldet werden. Verdächtige Container SOLLTEN automatisch beendet und neu gestartet werden.

Das zu überwachende Verhalten SOLLTE umfassen:

- Netzverbindungen,
- Dateisystem-Zugriffe und
- Kernel-Anfragen (Syscalls).

SYS.1.6.A33 Mikro-Segmentierung von Containern (H)

Die Container SOLLTEN nur über die notwendigen Netzports miteinander kommunizieren können. Es SOLLTEN innerhalb der virtuellen Netze Regeln existieren, die alle bis auf die für den Betrieb notwendigen Netzverbindungen unterbinden. Die Regeln SOLLTEN Quelle und Ziel der Verbindungen genau definieren und dafür mindestens die Service-Namen, Meta-Daten („Labels“) oder die Service-Accounts verwenden. Sofern möglich SOLLTEN die Regeln eine zertifikatsbasierte Authentifizierung vorschreiben und nur die in den Zertifikaten hinterlegten Identitäten für die Definition der erlaubten Verbindungen nutzen.

Alle Kriterien, die als Bezeichnung für diese Verbindung dienen, SOLLTEN so abgesichert sein, dass nur

berechtige Personen und Verwaltungs-Dienste diese Kriterien setzen dürfen.

SYS.1.6.A34 Hochverfügbarkeit von Containern (H)
Der Containerbetrieb SOLLTE so aufgebaut sein, dass bei Ausfall eines Rechenzentrums die Anwendungen in den Containern in kurzer Zeit an einem anderen Standort neu anlaufen können. Dafür SOLLTEN alle notwendigen Konfigurationsdateien, Images, Nutzdaten, Netzverbindungen und sonstige für den Betrieb benötigten Ressourcen inklusive der zum Betrieb nötigen Hardware an diesem Standort verfügbar sein.

SYS.1.6.A35 Verschlüsselte Datenhaltung bei Containern (H)
Die Dateisysteme mit den persistenten Daten der Anwendungsdienste SOLLTEN verschlüsselt sein.

SYS.1.6.A36 Verschlüsselung der Netzkommunikation zwischen Containern (H)
Daten, die über virtuelle oder physische Netze zwischen den Containern übertragen werden, SOLLTEN verschlüsselt werden. Die Verbindungen SOLLTEN mit Zertifikaten authentifiziert werden.

4 Weiterführende Informationen

4.1 Wissenswertes

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen im Bereich Container finden sich unter anderem in folgenden Veröffentlichungen:

- NIST 800-190
  https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-190.pdf
- CIS Benchmark Docker
  https://www.cisecurity.org/benchmark/docker/
- CIS Benchmark Kubernetes
  https://www.cisecurity.org/benchmark/kubernetes/
- OCI – Open Container Initiative
  https://www.opencontainers.org/
- CNCF – Cloud Native Computing Foundation
  https://www.cncf.io/

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die Kreuzreferenztabelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tabelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden.

Die folgenden elementaren Gefährdungen sind für Container von Bedeutung.

G 0.14 Ausspähen von Informationen / Spionage

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.28 Software-Schwachstellen oder -Fehler

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.37 Abstreiten von Handlungen

G 0.39 Schadprogramme

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdugen Anforderungen	CIA	G 0.14	G 0.19	G 0.20	G 0.21	G 0.23	G 0.25	G 0.27	G 0.28	G 0.30	G 0.37	G 0.39	G 0.45	G 0.46
SYS.1.6.A1		X	X	X	X	X		X	X	X	X	X	X	X
SYS.1.6.A2		X			X			X				X		X
SYS.1.6.A3				X	X					X				
SYS.1.6.A4		X			X	X				X		X		
SYS.1.6.A5		X				X						X		X
SYS.1.6.A6				X	X				X					
SYS.1.6.A7		X			X	X			X			X		
SYS.1.6.A8									X		X			
SYS.1.6.A9													X	X
SYS.1.6.A10		X				X				X				
SYS.1.6.A11		X	X	X	X	X		X		X	X	X	X	X
SYS.1.6.A12			X											
SYS.1.6.A13				X	X	X		X				X	X	X
SYS.1.6.A14		X				X			X			X		
SYS.1.6.A15		X				X						X		
SYS.1.6.A16								X						
SYS.1.6.A17			X										X	
SYS.1.6.A18		X	X			X				X				
SYS.1.6.A19		X			X	X				X			X	X
SYS.1.6.A20				X	X			X		X			X	X
SYS.1.6.A21						X			X				X	X
SYS.1.6.A22		X				X				X				
SYS.1.6.A23		X				X				X				
SYS.1.6.A24						X				X	X			
SYS.1.6.A25		X			X	X				X				
SYS.1.6.A26		X			X	X				X				
SYS.1.6.A27								X					X	X
SYS.1.6.A28				X		X				X	X			
SYS.1.6.A29	CIA	X		X		X		X	X	X		X	X	X
SYS.1.6.A30	CIA			X					X			X		
SYS.1.6.A31	CIA	X	X			X							X	X
SYS.1.6.A32	CIA	X	X			X			X	X				
SYS.1.6.A33	CI	X	X			X			X					
SYS.1.6.A34	A						X							
SYS.1.6.A35	C	X	X											X
SYS.1.6.A36	C	X	X											X