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 System Level Virtualization). Derzeit im Markt befindliche Produkte für Container integrieren eine Systemmanagement-Software, durch die die separierte Umgebung detailliert beschrieben werden kann und die das Erstellen von identischen Umgebungen unterstützt. Um Container zu verwalten, haben sich mehrere Produkte etabliert, die es erlauben, auch sehr große Umgebungen zu bedienen. Aktuelle Container-Lösungen sind z. B. Docker, Kubernetes, LXC oder rkt.

Dieser Baustein betrachtet Container unabhängig vom verwendeten Container-Produkt.

1.2 Zielsetzung

Ziel dieses Bausteins ist der Schutz von Informationen, die in Containern verarbeitet, angeboten oder darüber übertragen werden. Der Baustein behandelt daher, wie Container grundsätzlich abgesichert, wie sie orchestriert und wie die verwendeten Images mit bordeigenen Mitteln verwaltet werden können, unabhängig vom Einsatzzweck des im Container betriebenen Dienstes bzw. der Anwendung. Dabei wird zwischen dem eigentlichen Container-Dienst, 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

Der Baustein enthält grundsätzliche Anforderungen zur Einrichtung und zum Betrieb von Containern. 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.

Sicherheitsanforderungen möglicher Server-Funktionen wie 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 oft auf Basis von Images erstellt, die aus dem Internet bezogen 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. Diese 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 schwer 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 oder die tool-gestützte 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 standardmäßig aktiviert.

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

2.3 Tool-basierte Orchestrierung ohne Absicherung

Sofern eine große Anzahl von Containern betrieben wird, wird zumeist eine Software zur Orchestrierung, also 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 Datenverluste durch fehlende Persistenz

Container sind von ihrem Aufbau her dafür gedacht, nur eine bestimmte Zeit ausgeführt zu werden, und sie können sich jederzeit auch abschalten. Wird dies nicht beachtet, könnten in manchen Containern Daten gespeichert werden, die sich ausschließlich im Container befinden. Wird eine neue Version des zugrundeliegenden Images verwendet, beispielsweise bei einem Update des Images oder der betriebenen Anwendung, beenden sich die Container und es werden neue Daten auf Basis des neuen Images erstellt. Alle im vorherigen Container enthaltenen Daten sind dann 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 somit deren Ergebnisse nicht mehr nachvollzogen werden.

2.5 Vertraulichkeitsverlust von Zugangsdaten

Die Art und Weise des Aufbaus und der Erstellung von Images für Container macht es oft notwendig, dass Zugangsdaten im Container hinterlegt sind, z. B. für Datenbanken. 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 spezifische Anforderungen für den Bereich Container aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden.

Bausteinverantwortlicher	IT-Betrieb
Weitere Verantwortliche	Leiter IT

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein Container vorrangig umgesetzt werden:

SYS.1.6.A1 Planung des Container-Einsatzes [Leiter IT]

Bevor Container eingesetzt werden, MUSS geplant werden, wie alle relevanten Aspekte der Installation, des Betriebs und der Sicherheit berücksichtigt werden. Diese Planung SOLLTE angemessen dokumentiert werden.

SYS.1.6.A2 Planung der Separierung

Vor der Inbetriebnahme MUSS geplant werden, wie die in Containern betriebenen Anwendungen voneinander separiert werden. Auf Basis des Schutzbedarfs der Anwendungen, des Netzzonenkonzepts und einer Risikobetrachtung SOLLTE entschieden werden, welches dieser Modelle eingesetzt wird:

- Separierung der Anwendungen in Containern auf dem gleichen Wirt,
- Separierung der Container in virtualisierte Wirte auf einem physischen Wirt oder
- Separierung der physischen Wirte (mit oder ohne virtualisierte Wirte) auf separaten physischen Wirten.

SYS.1.6.A3 Härtung des Host-Systems

Alle im Host-System nicht benötigten Dienste und Anwendungen MÜSSEN deinstalliert werden. Die Konfiguration des Host-Systems MUSS angemessen gehärtet werden.

SYS.1.6.A4 Härtung der Software im Container

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

SYS.1.6.A5 Persistenz von Protokollierungsdaten

Die Protokollierungsdaten der im Container ausgeführten Anwendungen MÜSSEN persistent außerhalb des Containers gespeichert werden.

SYS.1.6.A6 Persistenz von Nutzdaten

Die Nutzdaten, auf die die Anwendungen im Container zugreifen, MÜSSEN persistent außerhalb des Containers gespeichert werden.

SYS.1.6.A7 Verwendung sicherer Images

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

Sollten Images aus öffentlichen Quellen eingesetzt werden, so MUSS jedes Image geprüft werden, ob es auf dem Transportweg verändert wurde. Images DÜRFEN NUR aus vertrauenswürdigen Quellen stammen. Die Quelle SOLLTE danach ausgewählt werden, dass der Anbieter die enthaltene Software regelmäßig auf Sicherheitsprobleme prüft, diese behebt und dies seinen Kunden zusichert.

SYS.1.6.A8 Speicherung von Zugangsdaten

Zugangsdaten MÜSSEN so gespeichert und verwaltet werden, dass nur berechtigte Personen hierauf zugreifen können. Insbesondere MUSS bei der Verwaltung der Images und der in den Images betriebenen Anwendungen darauf geachtet werden, dass die Zugangsdaten nur an zugangsgeschützten Orten gespeichert werden. Die von der Container-Software 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

SYS.1.6.A9 Separierung der Netze

Die Netze für die Administration des Hosts, die Administration des Container-Dienstes und die einzelnen Netze der Anwendungsdienste MÜSSEN separiert werden, zumindest wenn unsichere Protokolle verwendet werden.

Es DÜRFEN NUR die für den Betrieb notwendigen Netz-Ports der Container in die dafür vorgesehenen Netze freigegeben werden.

SYS.1.6.A10 Einbinden von Volumes

Die Container DÜRFEN NUR auf die für den Betrieb notwendigen Volumes und Verzeichnisse zugreifen können. Wenn Schreibrechte nicht benötigt werden, MÜSSEN diese eingeschränkt werden. Der private Modus von Volumes MUSS genutzt werden, sofern es keine Notwendigkeit für den Shared-Modus gibt.

SYS.1.6.A11 Administrativer Fernzugriff auf Container

Es MUSS sichergestellt sein, dass der administrative Fernzugriff nur auf den Container-Host und nicht auf die Dienste innerhalb der Container erfolgen kann.

3.2 Standard-Anforderungen

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

SYS.1.6.A12 Freigabe von Images

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

SYS.1.6.A13 Updates von Containern

Wenn sicherheitsrelevante Updates der zugrundeliegenden Images oder der betriebenen Software des Anwendungsdienstes erscheinen, SOLLTEN die Images für die Container neu erstellt und daraus neue Container instantiiert werden.

Von extern bezogene Images SOLLTEN nur dann eingesetzt werden, wenn der Anbieter für diese Images auch regelmäßig und bei sicherheitsrelevanten Änderungen schnell neue Versionen bereit stellt.

SYS.1.6.A14 Verschlüsselung der Netzkommunikation

Daten, die über virtuelle oder physische Netze zwischen den Containern übertragen werden, SOLLTEN verschlüsselt werden.

SYS.1.6.A15 Identitätsmanagement der Administratoren

Alle administrativen Zugänge zum Container-Dienst SOLLTEN durch personenbezogene Accounts und starke Authentisierung geschützt werden. Zugänge, die von der Verwaltungssoftware genutzt werden, SOLLTEN ebenfalls durch separate Accounts und starke Authentisierung geschützt werden.

SYS.1.6.A16 Accounts der Anwendungsdienste

Die Accounts innerhalb der Container 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.A17 Container-Ausführung ohne privilegierten Account

Alle Anwendungsdienste in Containern SOLLTEN nur unter einem nicht privilegierten Account ausgeführt werden.

SYS.1.6.A18 Nur ein Dienst pro Container

Jeder Container SOLLTE jeweils nur einen Dienst ausführen bzw. bereitstellen.

SYS.1.6.A19 Planung der Verwaltung und Orchestrierung

Die Verwaltung und Orchestrierung der Container SOLLTE erst nach einer geeigneten Planung erfolgen. Die Planung SOLLTE mindestens diese Punkte umfassen:

- Festlegung auf eine Verwaltungssoftware,
- Benutzermanagement der Verwaltungssoftware,
- Authentifizierung von Container-Diensten gegenüber der Verwaltungssoftware,
- Betrachtung der Anforderungen von Continous Integration und Deployment,
- Schnittstellen zu automatisierten Methoden des Schwachstellenmanagements,
- Anforderungen der Protokollierung und der Überwachung sowie
- Rollout und Rollback.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein 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. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

SYS.1.6.A20 Limitierung der Ressourcen pro Container (A)

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

SYS.1.6.A21 Automatisierte Auditierung (CIA)

Die gesamte Software in den Images SOLLTE automatisiert katalogisiert und mit 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 Wirkbetrieb freigegeben werden.

SYS.1.6.A22 Eigene Trusted Registry (CIA)

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.A23 Reduzierte Rechte (CIA)

Container SOLLTEN nur mit reduzierten Rechten gestartet werden, insbesondere wenn der Anwendungsdienst unter einem privilegierten Account läuft.

SYS.1.6.A24 Erstellung erweiterter Richtlinien für Container (CIA)

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.A25 Host Based Intrusion Detection (CIA)

Die Container und die betriebenen Anwendungsdienste SOLLTEN überwacht werden. Abweichungen des normalen Verhaltens SOLLTEN bemerkt und gemeldet werden.

Das zu überwachende Verhalten sollte umfassen:

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

SYS.1.6.A26 Hochverfügbarkeit (A)

Die Management-Software SOLLTE alle Container mit hohen oder sehr hohen Anforderungen an die Verfügbarkeit bei Ausfall von einem oder mehrere Knoten automatisch auf noch verfügbaren Knoten neu starten.

SYS.1.6.A27 Verschlüsselte Datenhaltung (C)

Die Dateisysteme mit den persistenten Daten der Anwendungsdienste SOLLTEN verschlüsselt sein.

4 Weiterführende Informationen

4.1 Literatur

- [Docksec] Docker security
  Docker, https://docs.docker.com/engine/security/security, zuletzt abgerufen am 15.05.2018

- [DSDG] Docker-Secure-Deployment-Guidelinies
  https://github.com/GDSSecurity/Docker-Secure-Deployment-Guidelines, zuletzt abgerufen am 15.05.2018

- [InSpec] InSpec Profil
  https://github.com/dev-sec/cis-docker-benchmark, zuletzt abgerufen am 15.05.2018

- [Oslv] Operation-system-level virtualization
  Wikipedia,
  https://en.wikipedia.org/wiki/Operating_system-level_virtualization_implementations, zuletzt abgerufen am 15.05.2018

- [SANS] A Checklist for Audit of Docker Containers
  SANS Institute, November 2016,
  https://sans.org/reading-room/whitepapers/auditing/checklist-audit-docker-containers-37437,
  zuletzt abgerufen am 15.05.2018

- [securdocker] A step-by-step checklist so secure Docker
  Center for Internet Security, https://cisecurity.org/benchmark/docker/, zuletzt abgerufen am 15.05.2018

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den Baustein 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 0.24 Zerstörung von Geräten oder Datenträgern
- 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 Gefährdungen / Anforderungen	G 0.14	G 0.19	G 0.20	G 0.21	G 0.23	G 0.24	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	x	x
SYS.1.6.A2	x	x		x	x					x				x
SYS.1.6.A3	x	x			x					x				x
SYS.1.6.A4	x	x			x					x				x
SYS.1.6.A5				x							x			
SYS.1.6.A6													x	
SYS.1.6.A7			x	x					x					
SYS.1.6.A8	x				x					x	x			
SYS.1.6.A9	x				x									
SYS.1.6.A10												x		
SYS.1.6.A11	x				x					x				
SYS.1.6.A12		x		x					x			x		
SYS.1.6.A13									x			x		
SYS.1.6.A14	x	x			x									
SYS.1.6.A15	x	x		x	x					x				
SYS.1.6.A16	x				x									x
SYS.1.6.A17	x				x									x
SYS.1.6.A18	x				x									x
SYS.1.6.A19							x						x	x
SYS.1.6.A20							x						x	x
SYS.1.6.A21					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		
SYS.1.6.A26						x							x	x
SYS.1.6.A27	x													x