IG Betrieb von Containern

Inhaltsverzeichnis

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

Bevor Container eingesetzt werden, MUSS zunächst das Ziel des Container-Einsatzes (z.B. Skalierung, Verfügbarkeit, Wegwerf-Container zur Sicherheit oder CI/CD) festgelegt werden, damit alle sicherheitsrelevanten Aspekte der Installation, des Betriebs und der Außerbetriebnahme geplant werden können. Bei der Planung SOLLTE auch der zukünftige zusätzliche Betriebsaufwand berücksichtigt werden, der durch Container-Einsatz oder Mischbetrieb entsteht. Die Planung MUSS angemessen dokumentiert werden.

Archiv: SYS.1.6.A1 (Alt) 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.

Rolle	Prio	Anforderung	Anmerkungen	CI/CD	Whitepaper SWL	per Policy prüfbar
Softwarebertreiber	muss	das Ziel des Container-Einsatzes (z.B. Skalierung, Verfügbarkeit, Lebenszeit, CI/CD) festlegen und die Sicherheitsaspekte für den gesamten Lebenszyklus eines Containers (z.B. Installation, Betrieb und Außerbetriebnahme) planen und dem Plattformbetreiber und Softwarelieferanten in einer angemessenen Dokumentation zur Verfügung stellen.				---
Softwarebetreiber	muss	die vom Softwarelieferanten und Plattformbetreiber zurückgelieferten Ergebnisse auf Erfüllung der Anforderungen prüfen und über die Aufnahme des Betriebes auch unter Berücksichtigung der entsehenden Betriebsaufwände entscheiden. Das Ergebnis der Prüfung und der Entscheidungsfindung ist angemssen zu dokumentieren.				
Softwarebetreiber	muss	definieren, wie viele Ressourcen für den Betrieb seiner Software benötigt werden.	Beispiele für Ressourcen sind: CPU, RAM, Festplatte, IO-Leistung, Netzanbindung Der Softwarebetreiber soll mit dem Softwarelieferanten abstimmen, welche Ressourcen benötigt werden. Er stellt sicher, dass die Anforderungen bzgl. SLA usw. umgesetzt werden.			
Softwarelieferant	muss	die vom Softwarebetreiber geplanten Anforderungen auf Erfüllung der geforderten Aspekte prüfen und das Ergebnis dem Softwarebetreiber in einer angemessenen Dokumentation zur Verfügung stellen.				
Plattformbetreiber	muss	die vom Softwarebetreiber geplanten Anforderungen auf Erfüllung der geforderten Aspekte prüfen und das Ergebnis dem Softwarebetreiber in einer angemessenen Dokumentation zur Verfügung stellen.				

SYS.1.6.A2 Planung der Verwaltung von Containern (B)

Die Verwaltung der Container DARF NUR nach einer geeigneten Planung erfolgen. Diese Planung MUSS den gesamten Lebenszyklus von Inbetrieb- bis Außerbetriebnahme inklusive Betrieb und Updates umfassen. Bei der Planung der Verwaltung MUSS berücksichtigt werden, dass der Ersteller eines Containers aufgrund der Auswirkungen auf den Betrieb in Teilen wie ein Administrator zu betrachten ist.

Start, Stopp und Überwachung der Container MUSS über die eingesetzte Verwaltungssoftware erfolgen.

Archiv: SYS.1.6.A3 Planung der Verwaltung und Orchestrierung (B) Anmerkung: Der Orchestrierungsanteil ist in den APP.4.4 verschoben worden.

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.

Rolle	Prio	Anforderung	Anmerkungen	CI/CD	Whitepaper SWL	per Policy prüfbar
Plattformbetreiber	muss	die Anforderungen an die Verwaltung der Container erfassen, definieren und dokumentieren. Hierbei finden die Anforderungen des Plattform- und Softwarebetreibers Berücksichtigung.	(aus IG BvC zu SYS.1.6.A3 alt). Für den Plattformbetreiber sind die Systemanforderungen (Affinity, Redundanz, Skalierbarkeit etc.) relevant.			---
Plattformbetreiber	muss	auf Basis der aufgenommenen Anforderungen eine Planung für die Verwaltung von Containern vornehmen, die den gesamten Lebenszyklus der Verwaltungslösung umfasst (z.B. Inbetriebnahme, Betrieb und Updates, Außerbetriebnahme).				
Plattformbetreiber	muss	sicherstellen, dass das Starten und Stoppen sowie die Überwachung von Containern durch die eingesetzte Verwaltungslösung (Kubernetes) erfolgt.				
Plattformbetreiber	muss	berücksichtigen, dass der Ersteller eines Containers (z.B. Softwarebetreiber) wie ein Administrator in seinem Arbeitsbereich (z.B. Project, Namespace etc.) zu betrachten ist (z.B. Installation von Software im Container).	Diese Forderung ist aus Sicht des Softwarebetreibers immer erfüllt, weil Änderungen im Container grundsätzlich nur durch die Bereitstellung und Nutzung von neu erstellten Images im produktiven Umfeld vorgesehen sind.			
Softwarebetreiber	muss	sicherstellen, dass eine Administration bzw. Konfigurationsänderung der Container ausschließlich an der Quelle (z.B. CI/CD-Pipeline) erfolgt.		X		
Softwarebetreiber	muss	seine Anforderungen an die Verwaltung der Container erfassen, definieren und in angemessener Dokumentation an den Plattformbetreiber übermitteln.	(aus IG BvC zu SYS.1.6.A3 alt)			
Softwarelieferant	sollte	das automatische Management seines Fachverfahrens durch die Bereitstellung von geeigneten Administrationswerkzeugen unterstützen.	Werkzeuge können Deployment-Scripte, Pipeline-Scripte für CI/CD, Kubernetes Operatoren sein (aus IG BvC zu SYS.1.6.A3 alt)	X	X	

SYS.1.6.A3 Sicherer Einsatz containerisierter IT-Systeme (B)

Bei containerisierten IT-Systemen MUSS berücksichtigt werden, wie sich eine Containerisierung auf die betriebenen IT-Systeme und Anwendungen auswirkt, dies betrifft insbesondere die Verwaltung und Eignung der Anwendungen.

Es MUSS anhand des Schutzbedarfs der Anwendungen geprüft werden, ob die Anforderungen an die Isolation und Kapselung der containerisierten IT-Systeme und der virtuellen Netze sowie der betriebenen Anwendungen hinreichend erfüllt sind. In diese Prüfung SOLLTEN die Betriebssystem-eigenen Mechanismen mit einbezogen werden. Für die virtuellen Netze nimmt der Host die Funktion einer Netzkomponente wahr, die Bausteine der Teilschichten NET.1 Netze und NET.3 Netzkomponenten MÜSSEN entsprechend berücksichtigt werden. Logische und Overlay-Netze MÜSSEN ebenfalls betrachtet und modelliert werden. Weiterhin MÜSSEN die eingesetzten containerisierten IT-Systeme den Anforderungen an die Verfügbarkeit und den Datendurchsatz genügen.

Im laufenden Betrieb MUSS SOLLTEN die Performance und der Zustand der containerisierten IT-Systeme überwacht werden (sogenannte Health Checks).

Anmerkung: Neue Maßnahme, teilweise Anforderungen übernommen aus BSI SYS.1.6.A4 Härtung des Host-Systems (B), korrespondiert mit der Maßnahme SYS.1.6.A9 Eignung für Container-Betrieb (S) (neu)!

Rolle	Prio	Anforderung	Anmerkungen	CI/CD	Whitepaper SWL	per Policy prüfbar
Softwarelieferant	sollte	die Anwendung so bereitstellen, dass die lt. Schutzbedarf erforderliche Anwendung von technischen Schutzmaßnahmen wie z.B. die Verwendung von Betriebssystem-Mechanismen, die Isolation und Kapselung der Anwendung und auch die Netzwerktrennung durch die Software-Architektur unterstützt und nicht verhindert wird.		X	X	(P) Klassifizierung der Policies ist vorzunehmen (Muss/Soll/Information)
Softwarebetreiber	muss	anhand des Schutzbedarfs der Anwendung prüfen, ob die Anforderungen an die technischen Schutzmaßnahmen wie z.B. die Isolation und Kapselung sowie die Netzwerktrennung mit den vom Plattformbetreiber bereitgestellten Mechanismen eingehalten werden können. Dabei sind auch Betriebssystem-eigene Mechanismen zu betrachten.				
Softwarebetreiber	muss	die vom Plattformbetreiber angebotenen technischen Schutzmaßnahmen (Betriebssystem-Mechanismen, Isolation und Kapselung der Anwendung sowie Netzwerktrennung) für eine Isolation und Kapselung containerisierter IT-Systeme sowie die Trennung der IT-Systeme in unterschiedliche virtuelle Netze in Abhängigkeit vom Schutzbedarf der Anwendung umsetzen.		X		
Softwarebetreiber	muss	die Anforderungen an die Verfügbarkeit und den Datendurchsatz der bereitgestellten Anwendung einhalten und die Performance des IT-Systems entsprechend der Anforderungen überwachen. Dazu muss der Softwarebetreiber seine Anforderungen mit dem Plattformbetreiber abstimmen.				
Plattformbetreiber	muss	technische Maßnahmen anbieten, die eine Isolation und Kapselung containerisierter IT-Systeme sowie die Trennung dieser IT-Systeme in unterschiedliche virtuelle Netze ermöglichen. Dabei muss die Netzwerkarchitektur (physische, virtuelle und Overlay-Netze) so gestaltet werden, dass die Anforderungen an einen sicheren Netzwerkbetrieb lt. BSI-Grundschutz NET.1 und NET.3 erfüllt sind.			X	

SYS.1.6.A4 Planung der Bereitstellung und Verteilung von Images (B)

Der Prozess zur Bereitstellung und Verteilung von Images MUSS geplant und angemessen dokumentiert werden.

Anmerkung: Neue Maßnahme.. Mapping zum Teil möglich auf: SYS.1.6.A11Richtlinie für Betrieb und Images (S) und SYS.1.6.A13 Freigabe von Images und Konfigurationen (S)

Rolle	Prio	Anforderung	Anmerkungen	CI/CD	Whitepaper SWL	per Policy prüfbar
Softwarebetreiber	muss	den Prozess zur Bereitstellung und Verteilung von Images inklusive Freigabebedingungen definieren, dokumentieren und die Vorgaben des Plattformbetreibers umsetzen.	aus SYS.A.13 alt	X		---
Softwarebetreiber	sollte	bei der Definition des Prozess zur Bereitstellung und Verteilung von Images folgendes berücksichtigen: • eine Microservice-Architektur der Anwendung anstreben • Auflistung erforderlicher Lizenzen • Bereitstellung von Deployment-Artefakten und Build-Spezifikationen • Prüfung auf Schwachstellen (statische und dynamsiche Tests), Schadsoftware, veraltete Komponenten, Build-Dependencies • Prüfsummen, Signaturen und Herkunft • Lifecycle und Patchmanagement von Images • Bereitstellung über eine vertrauenswürdige Registry				
Softwarebetreiber	muss	die Informationen zum Prozess der Bereitstellung und Verteilung von Images an den Softwarelieferanten und den Plattformbetreiber übergeben und sich mit diesen abstimmen.	aus SYS.A.13 alt	X	X	
Softwarelieferant	muss	die vom Softwarebetreiber erhaltenen Informationen zum Prozess über die Bereitstellung und Verteilung von Images prüfen, umsetzen und sich mit dem Softwarebetreiber fortlaufend abstimmen.	aus SYS.A.13 alt Governikus: Hier ist eine Standardisierung der Bereitstellung wünschenswert. Es ist sonst zu befürchten, dass für jeden Softwarebetreiber ein eigener Bereitstellungsprozess umgesetzt werden muss.	X	X	
Plattformbetreiber	muss	die vom Softwarebetreiber erhaltenen Informationen zum Prozess über die Bereitstellung und Verteilung von Images prüfen und sich mit dem Softwarebetreiber abstimmen.	aus SYS.A.13 alt	X		
Plattformbetreiber	muss	für den Softwarebetreiber konkrete Vorgaben für den Prozess zur Bereitstellung und Verteilung von Images definieren.	Folgende Punkte sollten mindestens betrachtet werden: - Umgang mit Schwachstellen - Lizenzvorgaben / Vorgaben zur Lizenzprüfung - Anforderungen zur Sicherstellung der Vertrauenswürdigkeit von Images	X	X	

SYS.1.6.A5 Separierung der Administrations- und Zugangsnetze bei Containern (B)

Die Netze für die Administration des Hosts, die Administration der Container und deren Zugangsnetze MÜSSEN dem Schutzbedarf angemessen separiert werden. Grundsätzlich SOLLTE mindestens die Administration des Hosts nur aus dem Administrationsnetz möglich sein.

Es SOLLTEN nur die für den Betrieb notwendigen Kommunikationsbeziehungen erlaubt werden.

Archiv: SYS.1.6.A18 Absicherung der Wirk- und Administrations-Netze (S) --> siehe auch APP.4.4.A7 Separierung der Netze bei Kubernetes (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.

Anmerkung: Maßnahme sinngemäß vereinfacht. Neu ist der Bezug zum Schutzbedarf . Frage : Definition Zugangsnetze. Ist hier das Administrationsnetz oder auch die einzelnen Netze der Anwendungsdienste mit gemeint?

Anmerkung:
Der Begriff "Zugangsnetze" wird durch die IG BvC so interpretiert, dass auch der Zugang zu den betriebenen Verfahren (inkl. Nutzdaten) enthalten ist. (Formulierungsvorschläge gewünscht)

Rolle	Prio	Anforderung	Anmerkungen	CICD	Whitepaper SWL	per Policy prüfbar
Softwarelieferant	muss	alle erforderlichen Kommunikationsverbindungen inklusive Zielhosts, Kommunikationsprotokolle und Ports beschreiben, die für Inbetriebnahme und Betrieb erforderlich sind.	aus SYS.1.6.A18 alt	x	x	---
Softwarelieferant	kann	in Abstimmung mit dem Softwarebetreiber die Kommunikationsbeziehungen zusätzlich in einer technisch formalen Form darstellen.	aus SYS.1.6.A18 alt siehe https://kubernetes.io/docs/concepts/services-networking/network-policies/		x	
Softwarelieferant	muss	die Vorgaben und Rahmenbedingungen des Software- und des Plattformbetreibers für die Kommunikationsbeziehungen berücksichtigen und seine Implementierung entsprechend auslegen.	Bei Anbietern für Standardsoftware solle der Plattformbetreiber prüfen, ob seine Anforderungen dem Marktangebot gerecht werden.		x	
Softwarebetreiber	muss	die Planung für die Konfiguration und den Betrieb der Netze nach dem Schutzbedarf seiner Anwendung ausrichten.	Der Softwarebetreiber ist für die Planung entsprechend der Anforderungen verantwortlich und beauftragt einen Plattformbetreiber, der diese Anforderungen umsetzt.			
Softwarebetreiber	muss	alle erforderlichen Kommunikationsverbindungen planen, dokumentieren und mit Softwarelieferanten und Plattformbetreiber abstimmen.	aus SYS.1.6.A18 alt			
Softwarebetreiber	muss	die Kommunikation auf die erforderlichen Kommunikationsverbindungen inklusive Zielhosts, Kommunikationsprotokolle und Ports einschränken, die für Inbetriebnahme und Betrieb erforderlich sind.	aus SYS.1.6.A18 alt z.B. Nutzung von Network-Namespaces, Netzwerk-Funktion mit hinreichender Isolations- und Filterwirkung bis mindestens OSI Layer 4 (z.B. Calico, openvSwitch, ACI, NSX-T)			o
Softwarebetreiber	kann	zur Beschreibung der Kommunikationsverbindungen Labels nutzen.				
Softwarebetreiber	sollte	für jeden nach außen exponierten Service oder Anwendung eine eigene IP-Adresse nutzen.	Verschiedene, nach außen exponierte Services sollten sich über die IP-Adressierung unterscheiden lassen, um Schutzmaßnahmen außerhalb der Kubernetes-Umgebung zu vereinfachen.			o
Plattformbetreiber	muss	Netze für die Administration der Hosts, des Container-Dienstes und den Anwendungsnetzen logisch trennen, z. B: auf Basis VLANs.	Anforderung ist Bestandteil "Planung der Plattform". Diese Anforderung hat einen Bezug zu BSI IT-GS NET.1.1 Netzarchitektur und Design.			
Plattformbetreiber	muss	die Kommunikation auf die erforderlichen Kommunikationsverbindungen inklusive Nodes, Kommunikationsprotokolle und Ports einschränken, die für Inbetriebnahme und Betrieb des Clusters und seiner Nodes erforderlich sind.				
Plattformbetreiber	sollte	für jeden direkt nach außen exponierten Service (oder direkt nach außen exponierte Anwendung) eine eigene IP-Adresse bereitstellen.	Verschiedene, nach außen exponierte Services sollten sich über die IP-Adressierung unterscheiden lassen, um Schutzmaßnahmen außerhalb der Kubernetes-Umgebung zu vereinfachen (bspw. Filterung auf OSI-Layer 3 ermöglichen).			
Plattformbetreiber	muss	für die Kommunikation zwischen den Nodes des Kubernetes-Clusters sichere Tunnelprotokolle nutzen.	Der zwischen den Cluster-Nodes bestehende Netzwerkverkehr muss geeignet voneinander isoliert und ggf. auch verschlüsselt werden (z.B. VXLAN, NVGRE, GENEVE).			

SYS.1.6.A6 Verwendung sicherer Images (B)

Es MUSS sichergestellt sein, dass sämtliche verwendeten Images nur aus vertrauenswürdigen Quellen stammen. ~~Digitale Signaturen MÜSSEN jedes Image gegen Veränderung absichern und~~ Der Ersteller MUSS eindeutig identifizierbar sein. Die Quelle MUSS danach ausgewählt werden, dass der Ersteller des Images die enthaltene Software regelmäßig auf Sicherheitsprobleme prüft, diese behebt und dokumentiert sowie dies seinen Kunden zusichert.

Die verwendete Version von Basis-Images DARF NICHT abgekündigt ("deprecated") sein. Es MÜSSEN eindeutige Versionsnummern angegeben sein. Wenn ein Image mit einer neueren Versionsnummer verfügbar ist, MUSS im Rahmen des Patch- und Änderungsmanagement geprüft werden, ob und wie dieses ausgerollt werden kann.

Archiv: BSI 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 sein. 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.

Rolle	Prio	Anforderung	Anmerkungen	CI/CD	Whitepaper SWL	per Policy prüfbar
Softwarelieferant	MUSS	vom Plattformbetreiber freigegebene, richtlinienkonforme Standard-Images verwenden	Governikus: Wünschenswert sind standardisierte Vorgaben. Es sollte eine Liste der mindestens zu unterstützenden Base-Images durch die IG BvC standardisiert werden, die die Bedarfe aller Plattformbetreiber abdeckt. Diese kann ein Plattformbetreiber weiter einschränken.		x	P
Softwarebetreiber	MUSS	Vorgaben für möglichst minimale Images festlegen und veröffentlichen.	ein Service pro Image		x	
Softwarelieferant	MUSS	dem Softwarebetreiber vollständige Artefakte bereitstellen.	ein Nachladen von Modulen aus fremden Quellen ist nicht erlaubt			
Softwarebetreiber	MUSS	dem Softwarelieferant für die Anlieferung eine vertrauenswürdige Registry bereitstellen				
Plattformbetreiber	SOLL	die Vertrauenswürdigkeit des Softwarelieferanten überprüfen				
Plattformbetreiber	MUSS	die Vertrauenswürdigkeit und die Integrität der angelieferten Artefakte überprüfen				
Plattformbetreiber	MUSS	Richtlinien für die Bereitstellung von Images den Softwarelieferant zur Verfügung stellen	- Zulässigkeit beim Überschreiten eines CVSS Wertes, etc.		x	
Plattformbetreiber	MUSS	dem Softwarebetreiber ein vertrauenswürdiges Repository zur Anlieferung der Images und Build-Spezifikationen bereitstellen.				
Plattformbetreiber	MUSS	Images unmittelbar bei der Bereitstellung in geeigneter Weise auf Schadcode und Schwachstellen prüfen.	Die Registry muss mit geeigneten Werkzeugen zur Schadcode und Schwachstellenanalyse ausgestattet sein.		x	
Softwarelieferant	MUSS	Images vor deren Bereitstellung in geeigneter Weise auf Schadcode und Schwachstellen prüfen.	Die Registry sollte mit geeigneten Werkzeugen zur Schadcode und Schwachstellenanalyse ausgestattet sein.		x	
Plattformbetreiber	SOLL	automatisierte Policies implementieren, die die Herkunft, Vertrauenswürdigkeit und Integrität der Images prüfen und durchsetzen.	Auf der Containerplattform dürfen keine Images betrieben werden, welche aus nicht zugelassenen Quellen stammen.		x	

SYS.1.6.A7 Persistenz von Protokollierungsdaten der Container (B)

Die Speicherung der Protokollierungsdaten der Container MUSS außerhalb des Containers, mindestens auf dem Container-Host, erfolgen.

Archiv: BSI SYS.1.6.A8 Persistenz der Protokollierungsdaten (B)

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

Rolle	Prio	Anforderung	Anmerkungen	CI/CD	Whitepaper SWL	per Policy prüfbar
Softwarelieferant	muss	alle Protokolldaten der Anwendung im Container über die Standardausgabe ausgeben.	Log-Daten MÜSSEN über STDOUT / STDERR ausgegeben werden.		x	---
Softwarelieferant	muss	Konfigurationsoptionen für die Protokollierung beschreiben.	Der Softwarebetreiber soll in die Lage versetzt werden, die Protokollierung , bspw. Log-Level, -Format oder -Kategorien, einzurichten.		x	
Softwarebetreiber	*muss*	*sicherstellen, dass Protokollierungsdaten außerhalb des Containers gespeichert werden*	*zusammen mit Plattformbetreiber sicherstellen, dass Cluster Protokollierungsdaten aggregiert und an einen zentralen Protokollierungsspeicher weitergegeben werden*			
Softwarebetreiber	muss	das vom Plattformbetreiber bereitgestellte System zum Aufzeichnen der Protokolldaten nutzen				
Plattformbetreiber	muss	den Zugang zu einem System zum Aufzeichnen der Protokolldaten bereitstellen.				
Plattformbetreiber	kann	die Log-Daten der Plattform und der Anwendungen getrennt speichern.				

SYS.1.6.A8 Sichere Speicherung von Zugangsdaten bei Containern (B)

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

Mindestens die folgenden Zugangsdaten MÜSSEN sicher gespeichert werden:

· Passwörter jeglicher Accounts,

· API-Keys für von der Anwendung genutzte Dienste,

· Schlüssel für symmetrische Verschlüsselungen sowie

· private Schlüssel bei Public-Key-Authentisierung.

Archiv: BSI 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*

Rolle	Prio	Anforderung	Anmerkungen	CI/CD	Whitepaper SWL	per Policy prüfbar
Softwarelieferant	MUSS	sicherstellen, dass keine Zugangsdaten (z.B. Passworte, geheime/private Schlüssel, API-Keys, Schlüssel für symmetrische Verschlüsselungen) in Container-Images gespeichert werden.		X	X	P
Softwarebetreiber	MUSS	Zugangsdaten (z.B. Passworte, geheime/private Schlüssel, API-Keys, Schlüssel für symmetrische Verschlüsselungen) in geschützten Bereichen hinterlegen. Dafür sind Kubernetes Secrets oder gleichwertige Systeme zu benutzen.		X		o
Softwarebetreiber	MUSS	die Einschränkung des Zugriffs auf Zugangsdaten durch ein Rollen- und Rechtekonzept umsetzen.				
Plattformbetreiber	MUSS	eine verschlüsselte Ablage von Zugangsdaten (z.B. Passworte, geheime/private Schlüssel, API-Keys; Schlüssel für symmetrische Verschlüsselungen) bereitstellen.	Es ist zu beachten, dass die etcd verschlüsselt gespeichert wird. Vault kann als System zur Speicherung und Verwaltung von Zugangsdaten genutzt werden. (https://github.com/hashicorp/vault)			
Plattformbetreiber	MUSS	ein System zur Umsetzung von Rollen- und Rechtekonzepten bereitstellen.	z.B LDAP, Active Directory oder Identity-Management	X		
Plattformbetreiber	MUSS	das Rollen- und Rechtekonzept vom Softwarebetreiber unterstützen.		X		

SYS.1.6.A9 Eignung für Container-Betrieb (S)

Die Anwendung bzw. der Dienst, der im Container betrieben werden soll, SOLLTE für den Container-Betrieb geeignet sein. Dabei SOLLTE berücksichtigt werden, dass Container häufiger für die darin ausgeführte Anwendung unvorhergesehen beendet werden können. Die Ergebnisse der Prüfung nach SYS.1.6.A3 *Sicherer Einsatz containerisierter IT-Systeme* SOLLTE nachvollziehbar dokumentiert werden.

Querbeziehungen zu folgenden Anforderungen:

SYS.1.6.A1 Planung des Container-Einsatzes (B), SYS.1.6.A11 Nur ein Dienst pro Container (S), BSI SYS.1.6.A15 Unveränderlichkeit der Container (S), SYS.1.6.A17 Ausführung von Containern ohne Privilegien (S), SYS.1.6.A18 Accounts der Anwendungsdienste (S).

Anmerkung: Neue Maßnahme, keine entsprechenden Inhalte im Archiv

Rolle	Prio	Anforderung	Anmerkungen	CI/CD	Whitepaper SWL	per Policy prüfbar
Softwarelieferant	sollte	Deployment Manifeste zur Installation bereitstellen.		x	x	---
Softwarelieferant	sollte	Container stateless gestalten und eine transaktionsoriente Funktionsweise der Anwendung sicherstellen.	Die transaktionsorientierte Funktionsweise soll sicherstellen, dass alle Verarbeitungen korrekt abgeschlossen werden können und keine inkonsistenten Zustände entstehen, selbst wenn Container neu deployed werden.		x	
Softwarelieferant	muss	bei der Nutzung von CRON-Jobs die unterstützten Mechanismen der Containerplattform zur Ausführung nutzen.	Beispielsweise müssen CronJobs in Kubernets oder als Implementierung in der Anwendung umgesetzt werden.		x	
Softwarelieferant	sollte	die Container so auslegen, dass eine horizontale Skalierung möglich ist.			x	
Softwarelieferant	sollte	Init Container für Konfigurationsanpassungen nutzen.		x	x	
Softwarelieferant	muss	Konfigurationsanpassungen so ausführen, dass keine manuellen Anpassungen in laufenden Containern erfolgen.		x	x	
Softwarelieferant	muss	die Nutzung von temporären Speicher so vorsehen, dass ein Restart des Containers und ein Wechsel des Hosts zur Laufzeit möglich ist.			x	
Softwarelieferant	sollte	Schnittstellen zur Überwachung des Betriebszustands der Container vorsehen, damit ein automatischer Restart ermöglicht werden kann.	siehe auch Anforderung APP.4.4.A11, Healtcheck für Container		x	
Softwarelieferant	muss	für die genutzten Anwendungen, Bibliotheken, Werkzeuge usw. auf ein für den Containerbetrieb und die genutzte Plattform geeignetes Lizenzmodell achten.			x	
Softwarebetreiber	muss	geeignete Anforderungen an den Softwarelieferanten stellen	Generisch. Es gibt viele Einsatz-Szenarien die man auf Meta-Ebene beschreiben muss. So erhält man z. B. eine Checkliste, auf was zu achten ist. Besonders auch hinsichtlich Trennung von Verantwortlichkeiten wichtig.			
Softwarebetreiber	muss	ein geeignetes Patchmanagement sicherstellen.		x		
Softwarebetreiber	sollte	ein automatisches Deployment umsetzen.		x		
Softwarebetreiber	muss	mit dem Softwarelieferanten die Basis für gelieferte Images abstimmen.	z. B. Abstimmung hinsichtlich Standard-Images oder auch Lizenztechnische Belange	x	x	
Softwarebetreiber	muss	die Restartfähigkeit der Container sicherstellen.	auch hinsichtlich vertraglicher Vereinbarungen mit den Stakeholdern	x		
Softwarebetreiber	muss	sicherstellen, dass die Prüfung der Eignung durchgeführt und angemessen dokumentiert wird.	Den Verweis auf SYS.1.6.A3 *Sicherer Einsatz containerisierter IT-Systeme* beachten.	x		
Plattformbetreiber	muss	geeignete Werkzeuge zur Überwachung der betriebenen Lösung bereitstellen.		x		
Plattformbetreiber	muss	geeignete Werkzeuge zum automatischen Deployment und Restart der Container bereitstellen.		x		

SYS.1.6.A10 Richtlinie für Images und Container-Betrieb (S)

Es SOLLTE eine Richtlinie erstellt und angewendet werden, die die Anforderungen an den Betrieb der Container und die erlaubten Images festlegt. Die Richtlinie SOLLTE auch Anforderungen an den Betrieb und die Bereitstellun

Archiv: BSI 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 V Images und des Betriebs enthalten.

Rolle	Prio	Anforderung	Anmerkungen	CICD	Whitepa SWL
Softwarelieferant	SOLLTE	die übermittelten Richtlinien des Softwarebetreibers umsetzen.	Hinweis: Das Whitepaper für Softwarelieferanten soll als Grundlage genutzt werden. Softwarelieferanten werden eine Vielzahl verschiedener Anforderungen nicht umsetzen können.	x	x
Softwarelieferant	MUSS	sicherstellen, dass gelieferte Artefakte, insb. Images, dem IT-Grundschutz entsprechen.		x	x
Softwarelieferant	MUSS	ein Patchmanagement gewährleisten.			x
Softwarebetreiber	MUSS	die Richtlinien und Vorgaben zum sicheren Betrieb dem Softwarelieferanten bereitstellen.			x
Softwarebetreiber	SOLLTE	die Umsetzung der Richtlinien und Vorgaben mit dem Softwarelieferanten vertraglich festhalten.	Insbesondere bei der Lieferung von Images, da hier die Fähigkeit der Anpassung der Images beschränkt wird.		x
Softwarebetreiber	MUSS	sicherstellen, dass die Richtlinie für den Betrieb der Container umgesetzt wird.		x	
Softwarebetreiber	SOLLTE	dem Softwarelieferanten erkannte Schwachstellen mitteilen.		x	
Softwarebetreiber	SOLLTE	die Richtlinie des Plattformbetreibers mit seinen anwendungsspezifischen Anforderungen erweitern.	Es dürfen keine Widersprüche oder Abschwächungen der Vorgaben des Plattformbetreibers entstehen. Es wird eine Konkretisierung der Prozesse und Übergabepunkte auf Basis generischer Definitionen angestrebt.	x	
Plattformbetreiber	MUSS	eine Richtlinie für die Nutzung der Plattform für den Softwarebetreiber bereitstellen.			
Plattformbetreiber	SOLLTE	die Einhaltung der Richtline für den Betrieb der Container über geeignete technische Maßnahmen automatisiert und regelmäßig prüfen.		x	
Plattformbetreiber	MUSS	in seiner Richtlinie die BSI Bausteine, insb. APP.4.4 betrachten.	Die IG Betrieb von Containern betrachtet den Betrieb von Kubernetes-Clustern. Es soll sichergestellt werden, dass auch der Baustein APP.4.4 Berücksichigung findet.		
Plattformbetreiber	MUSS	die Richtlinie in seine vorhandenen Lifecylcle-Prozesse integrieren und damit ein regelmäßiges Review und ggf. die Fortschreibung sicherstellen.			

SYS.1.6.A11 Nur ein Dienst pro Container (S)

Jeder Container SOLLTE jeweils nur einen Dienst bereitstellen.

Rolle	Prio	Anforderung	Anmerkungen	CICD	Whitepaper SWL	per Policy prüfbar
Softwarelieferant	sollte	die Software so gestalten, dass jeder Container nur einen Dienst bereitstellt. Der Softwarelieferant sollte dann sicherstellen, dass zusammenhängende Dienste durch das Deployment bzw. die Orchestrierung als Verwaltungseinheiten bereitgestellt werden können und z.B. geeignete Deployment-Artefakte (Manifeste) liefern.	Die Einstufung mit "soll" ist nur aufgrund der Übergangsphase aus der "klassischen" in die Containerwelt vorgenommen worden. Es wird ein "muss" angestrebt. Definition Dienst im Kontext dieser Anforderung erforderlich: Singuläre fachliche Funktion ? Fachliche bzw. funktionale Zerlegung von Applikationen in einzelne Komponenten ? Verwaltungseinheiten können beispielsweise Kubernetes-Pods sein. siehe auch "Extending applications on Kubernetes with multi-container-pods" (https://learnk8s.io/sidecar-containers-patterns)		X	---
Softwarelieferant	muss	bei Neuentwicklungen die Software so gestalten, dass jeder Container nur einen Dienst bereitstellt.			X	
Softwarelieferant	muss	für Dienste, die unterschiedlich skalieren oder auf verschiedenen Worker-Nodes betrieben werden sollen, verschiedene Deployments ermöglichen.	Ein Deployment wird nicht unbedingt durch den Softwarelieferanten geliefert.		X	
Softwarelieferant	sollte	für die durch ihn bereitgestellten Software-Artefakte automatisiert zu verarbeitende Deployment-Anweisungen bereitstellen (z.B. YAML-basierte Deployments).		X	X	
Softwarebetreiber	muss	prüfen, dass die durch den Softwarelieferanten gelieferten Software-Artefakte nur einen Dienst je Container oder Verwaltungseinheit bereitstellen und geeignete Deployment-Anweisungen verfügbar sind.		X	X	
Softwarebetreiber	sollte	die Prüfung der durch den Softwarelieferanten bereitgestellten Artefakte und Deployment-Anweisungen automatisiert vornehmen und in seine CI/CD-Prozesse integrieren.	z.B. Integration des Werkzeugs in eine CI/CD-Pipeline	X	X	
Softwarebetreiber	muss	bei Neuentwicklungen Anforderungen definieren, dass die durch den Softwarelieferanten gelieferten Software-Artefakte nur einen Dienst je Container oder Verwaltungseinheit bereitstellen.				
Softwarebetreiber	muss	für Dienste, die unterschiedlich skalieren oder auf verschiedenen Worker-Nodes betrieben werden sollen, verschiedene Deployments realisieren.				
Softwarebetreiber	muss	für die durch ihn bereitgestellten Software-Artefakte automatisiert zu verarbeitende Deployment-Anweisungen bereitstellen (z.B. YAML-basierte Deployments).		X		

Archiv: BSI 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.A12 Verteilung sicherer Images (S)

Es SOLLTE angemessen dokumentiert werden, welche Quellen für Images als vertrauenswürdig klassifiziert wurden und warum. Zusätzlich SOLLTE der Prozess angemessen dokumentiert werden, wie Images bzw. die im Image enthaltenen Softwarebestandteile aus vertrauenswürdigen Quellen bezogen und schließlich für den produktiven Betrieb bereitgestellt werden.

Die verwendeten Images SOLLTEN über Metadaten verfügen, die die Funktion und die Historie des Images nachvollziehbar machen. Digitale Signaturen SOLLTEN jedes Image gegen Veränderung absichern.

Anmerkung: Keine Entsprechung der Inhalte?

Rolle	Prio	Anforderung	Anmerkungen	CI/CD	Whitepaper SWL	per Policy prüfbar
Softwarelieferant	muss	dokumentieren, welche Quellen für Images verwendet wurden.			X	P
Softwarelieferant	muss	sich an die vom Softwarebetreiber bereitgestellte Whitelist für die Erstellung der Images halten.	Empfehlung: Die Standardimages der OpenCoDE-Plattform anwenden.		X	
Softwarelieferant	kann	dem Softwarebetreiber ein Klassifikationssystem für die Erstellung einer Whitelist für vertrauenswürdige Quellen vorschlagen.			X	o
Softwarelieferant	muss	das Image mit Metainformation versehen und signieren.	- Es muss eine Liste von Metadaten die mindestens vorhanden sein müssen exisitieren. -> Verweiß auf Arbeitsgruppe Versionierung und Tagging von Images	X	X	
Softwarebetreiber	muss	die Klassifikation von vertrauenswürdigen Quellen vornehmen und dem Softwarelieferant mitteilen.	- Definition einer Withlist mit Vertrauenswürdigen Quellen		X	
Softwarebetreiber	muss	die Klassifizierung der vertrauenswürdigen Quellen begründen.	- Es muss der Begriff Vertrauenswürdig definiert werden		X	
Softwarebetreiber	sollte	mit dem Plattformbetreiber das Klassifikationssystem seiner Quellen abstimmen.		X		
Softwarebetreiber	muss	sicherstellen das nur ordnungsgemäße signierte Images bereitgestellt werden.		X		
Softwarebetreiber	muss	den sicheren Transport der Deployment-Artefakte, insb. Images, unter Berücksichtigung des Bausteins CON.9 Informationsaustausch sicherstellen.		X	X	
Plattformbetreiber	sollte	die Infrastruktur zur Ablage von signierten Images bereitstellen.	Falls der Plattformbetreiber diese Infrastruktur nicht bereitstellt, muss der Softwarebetreiber sicherstellten, dass eine entsprechende Infrastruktur bereit steht.	X		

SYS.1.6.A13 Freigabe von Images (S)

Alle Images für den produktiven Betrieb SOLLTEN wie Softwareprodukte einen Test- und Freigabeprozess gemäß des Bausteins OPS.1.1.6 Software-Test und Freigaben durchlaufen.

Archiv: BSI 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.

Anmerkung: konkretisiert, Zusatz fällt weg

Rolle	Prio	Anforderung	Anmerkungen	CICD	Whitepaper SWL	per Policy prüfbar
Softwarelieferant	muss	eine vollständige Software Bill of Material in einem abgestimmten Format angeben.	Dokumentation der genutzten Komponenten, Ermöglichung der Prüfung von Lizenzen	x	x	---
Softwarelieferant	soll	Build-Spezifikationen (bspw. Dockerfile) für Images liefern.	statische Analyse auf Schwachstellen und Schadsoftware ermöglichen	x	x	
Softwarelieferant	soll	Freigabebedingungen für die erstellte Software sowie für Images und Konfigurationen in den Lieferantenprozessen definieren. Hierbei sind die Freigabebedingungen des Softwarebetreibers zu berücksichtigen.	z.B. Auflistung der Abhängigkeiten, statische und dynamische Tests Governikus: Wünschenswert sind standardisierte Vorgaben. Es ist sonst zu befürchten, dass jeder Softwarebetreiber eigene Bedingungen aufstellt.	x	x	
Softwarelieferant	soll	die Freigabebedingungen in einem definierten Freigabeprozess im Lieferantenkontext prüfen und alle Informationen für den weiteren Freigabeprozess an den Softwarebetreiber übergeben. Zu den übergebenen Informationen gehören auch die Ergebnisse des eigenen Freigabeprozesses.		x	x	
Softwarelieferant	kann	die zu liefernden Images bereits vor der finalen Lieferung mit dem Prüfstandard des Softwarebetreibers überprüfen.	Das ermöglicht dem Lieferanten, seine eigene Software qualitätszusichern und nicht vom Prüfergebnis des Betreibers "überrascht" zu werden. Das kann z.B. durch eine standardisierte Entwicklungsumgebung realisiert werden, die dem Lieferanten bereitgestellt wird. Umso früher, umso weniger wird man von Neuerungen überrascht	x	x	
Softwarebetreiber	soll	allen Anforderungen entsprechenden Freigabebedingungen für die Inbetriebnahme von Images und Konfigurationen definieren und für den Softwarelieferanten bereitstellen. Hierbei sind die Freigabebedingungen des Plattformbetreibers zu berücksichtigen.	z.B. Nutzung von Lizenzen, Bereitstellung Build-Spezifikation, CVE-/Schwachstellenanalyse, Schadcode-Prüfung, Image-Bereitstellung), Vollständigkeit der Abhängigkeiten	x	x	
Softwarebetreiber	muss	die Freigabebedingungen in einem Freigabeprozess gemäß des Bausteines OPS.1.1.6 Software-Test und -Freigaben definieren.		x	x	
Softwarebetreiber	muss	einen definierten Freigabeprozess für die Produktivsetzung der Anwendung / neuer Versionen etablieren.		x	x	
Softwarebetreiber	muss	sicherstellen, dass die Software den Freigabebedingungen entspricht und die Freigabe entsprechend dokumentieren.	Die Ergebnisse sollten dem Softwarelieferanten zur Verfügung gestellt werden.	x		
Plattformbetreiber	muss	seine Anforderungen entsprechend den Freigabebedingungen für die Inbetriebnahme von Images und Konfigurationen definieren und für den Softwarebetreiber bereitstellen.	z.B. Beschreibungsmittel für Konfigurationen, kernel capabilities, Begrenzung der Ressourcennutzung Die verwendbaren Basisimages sind bereits durch SYS.1.6A6 "Verwendung sicherer Images" abgedeckt.	x		

SYS.1.6.A14 Aktualisierung von Images (S)

Bei der Erstellung des Konzeptes für das Patch- und Änderungsmanagement gemäß OPS.1.1.3 Patch- und Änderungsmanagement SOLLTE entschieden werden, wann und wie die Updates der Images oder der betriebenen Software bzw. des betriebenen Dienstes ausgerollt werden. Bei persistenten Containern SOLLTE geprüft werden, ob in Ausnahmefällen ein Update des jeweiligen Containers geeigneter ist, als den Container vollständig neu zu provisionieren.

Archiv: BSI 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.

Anmerkung: komplett neue Definition

Rolle	Prio	Anforderung	Anmerkungen	CICD	Whitepaper SWL	per Policy prüfbar
Softwarelieferant	muss	sicherstellen, dass Updates von Software nicht im laufenden Container installiert werden. Bei persistenten Containern SOLLTE geprüft werden, ob in (absolut seltenen) Ausnahmefällen ein Update des jeweiligen Containers geeigneter ist, als den Container vollständig neu zu provisionieren.	Es dürfen keine Tools enthalten sein, welche nicht für den Betrieb der Applikation notwendig sind (Paketmanager, YUM, APT, APK usw.). Ausnahmefälle: NICHT EMPFOHLEN - bei vielen DVZen explizit verboten einen Container beim RUN upzudaten, da Betriebsrisiko sehr hoch! Beim BUILD an sich wäre das in Ordnung		x	P
Softwarelieferant	muss	bei sicherheitsrelevanten und featurebasierten Updates der Anwendungen oder der Standardimages neue Images erstellen und eindeutig versioniert innerhalb der vereinbarten Zeiträume / SLAs zur Verfügung stellen.		x	x	
Softwarelieferant	sollte	sicherstellen, dass die Software in der Lage ist, den Service auch während Updates entsprechend der definierten Anforderungen aufrechtzuerhalten.	d.h. Clusterfähigkeit der Software		x	
Softwarebetreiber	sollte	die benötigten SLAs zur Aktualisierung der Images mit dem Softwarelieferanten vereinbaren.			x	
Softwarebetreiber	sollte	sicherstellen, dass keine veralteten Images zum Einsatz kommen und sicher stellen, dass neue Images regelmäßig vom Softwarelieferanten in die eigene Registry übernommen werden.		x	x	
Softwarebetreiber	sollte	gemäß OPS.1.1.3 Patch- und Änderungsmanagement entscheiden, wann und wie die Updates der Images oder der betriebenen Software bzw. des betriebenen Dienstes ausgerollt werden.		x	x	
Softwarebetreiber	muss	sicherstellen, dass die Software neu angelieferter Images auf Funktionionalität und Schadcode geprüft und innerhalb der vereinbarten Zeitfenster / SLAs für den produktiven Container-Betrieb bereitgestellt werden.	z.B. Feature-basiert 30 Tage nach Veröffentlichung der Updates; 5 Tage nach Veröffentlichung kritischer sicherheitsrelevanter Updates	x	x	
Softwarebetreiber	muss	eine geeignete Update-Strategie wählen, so dass auch während der Update-Phase ein Betrieb entsprechend den definierten Anforderungen aufrecht erhalten werden kann.	z.B. Recreate- oder Rolling-Update, ...			
Softwarebetreiber	sollte	entsprechend der vereinbarten SLAs sicherstellen, dass bei auftretenden Fehlern oder reduzierter Performance nach der Verwendung neuer Images für Container ein Rollback auf einen früheren Softwarestand vorgenommen werden kann (auch automatisiert).	bei Major-Updates kann Rollback manchmal nicht funktionieren, deshalb "sollte"			
Softwarebetreiber	muss	die Verwendung von Software in den Containern mit unzureichendem Patch-Level fortlaufend prüfen und wenn erforderlich alarmieren.		x		
Softwarebetreiber	muss	einen Prozess etablieren, welcher über die Abschaltung einer Softwarelösung entscheidet, wenn das Patchmanagement nicht in ausreichender Art und Weise aufrecht erhalten werden kann.	z. B. offene kritische Schwachstellen			
Plattformbetreiber	sollte	durch geeignete Konfiguration des Clusters sicherstellen, dass Worker-Nodes nur die vorgesehenen, aktualisierten Images verwenden könnten.	im Falle eines "Rollback" entspricht das aktuelle Image einer vorherigen, noch zulässigen Version Die Zulässigkeit richtet sich nach dem Stage, in dem sich das Image befindet (z.B. neuere Version in Development-Stage). Zu berücksichtigen bei Überwachung / Logging: Nachweis, dass Image Test durchlaufen hat und von wem und auf welchem Wege das Image bereitgestellt wurde. Man muss manchmal alte Anwendungen betreiben bzw. man muss Sicherheitslücken auf Grund höherer Ziele hinnehmen oder weil man erst noch auf Patch wartet			
Plattformbetreiber	muss	geeignete Werkzeuge zum Überprüfen von Container-Images zur Verfügung stellen.	Optimal ist eine automatisierte Alarmierung des Softwarebetreibers.			

SYS.1.6.A15 Limitierung der Ressourcen pro Container (S)

Für jeden Container SOLLTEN Ressourcen auf dem Host-System, wie CPU, flüchtiger und persistenter Speicher sowie Netzbandbreite, angemessen reserviert und limitiert werden. Es SOLLTE definiert und dokumentiert sein, wie das System im Fall einer Überschreitung dieser Limitierungen reagiert.

Archiv: BSI 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.

Anmerkung: konkretisiert mit Zusatz

Rolle	Prio	Anforderung	Anmerkungen	CI/CD	Whitepaper SWL	per Policy prüfbar
Softwarelieferant	muss	Dimensionierungen (Requests) und Begrenzungen (Limits) für CPU, RAM sowie temporären Speicher für jeden Container auf den von ihm angenommenen Nutzerprofile empfehlen. Er muss ebenfalls die Dimensionierungen und die Größe des benötigten persistenten Speichers empfehlen. Die Informationen müssen dem Softwarebetreiber mitgeteilt werden.	Nach dem Prinzip pro Container einen Dienst. Deckt mit ab: will in der Lage sein, Resourcen zu begrenzen. Ggf., je nach Szenario feingranular pro Dienst (Requests und Limits gibt es nicht nur auf Container-Ebene, sondern auch auf Pod-Ebene, hier in diesem Baustein allerdings nicht Thematik) Der Softwarelieferant muss Defaultwerte für die Limits liefern, die dann ggf. vom Softwarebetreiber angepasst werden können.	x	x	P
Softwarelieferant	muss	die Möglichkeiten und Funktionsweisen zur Skalierung der Dienste beschreiben.	Z.b. kubernetes pod hpa - https://kubernetes.io/de/docs/tasks/run-application/horizontal-pod-autoscale/ Anmerkung: - Limitierung muss auch berücksichtigt werden, wenn der Dienst skaliert werden soll.		x	
Softwarelieferant	sollte	Dimensionierungen (Requests) und Begrenzungen (Limits) auf den von ihm angenommenen Nutzerprofile für das Netzwerk definieren und dem Softwarebeteiber mitteilen.	Möglichkeiten im Stack eruieren. Beispiele: Bandbreite. Einbindung von Plugins beispielweise. Bekannte (indirekte) Netzwerk-Quotierungen sind: - Quotierung der Anzahl von Pods (Auswirkung auf Subnet-Size) - Quotierung von Loadbalancern - Quotierung von Ingress - Ressourcen Connection oder Lastabhängige Limitierungen sind nicht bekannt. Fragestellung wäre auch, wie dies technisch machbar ist. Pods können ja auch innerhalb eines Nodes miteinander Kommunizieren. Hier wären Limitationen eher unerwünscht oder hätten negative Nebeneffekte. Limitierung und Angaben ggf. in Bezug auf die Anzahl der Verbindungen wären hilfreich.	x	x	
Softwarelieferant	sollte	Handlungsempfehlungen bereitstellen, für den Fall, dass ein Container an seine Ressourcengrenzen kommt.			x	
Softwarebetreiber	muss	Die Konfiguration der Anforderungen und Begrenzungen zu den Ressourcen beim Plattformbetreiber anfordern und umsetzen.	Namespaces, Requests Kapazitätsmanagement für Plattformbetreiber, Forecasting wünschenswert für zukünftige App-Deployments. Vor allem bei on-premise bzw. private cloud Betrieb. Skalierung pro Container oder IT gesamt.			
Softwarebetreiber	sollte	dem Plattformbetreiber einen Kapazitäts-Forecast mitteilen.				
Softwarebetreiber	kann	ein Resourcen Management nach außen zur Containerverwaltung exponieren, dokumentieren und klassifizieren.	Beispiel: Die Oracle Datenbank hat die Möglichkeit, über das DB-interne Resource Management die Resourcen pro ServiceName (Bestandteil des Connection Strings) zuzuteilen. Man könnte z.b. einen ServiceName für OLTP-, Batch-, oder Backup/rman- Verbindungen definieren. So könnte man steuern, daß OLTP die höchste Priorität gegenüber Batch -und Backup Services hat.			
Softwarebetreiber	muss	die angegebenen Begrenzungen der Ressourcen (Limits) durch entsprechende Konfiguration der Container umsetzen.		x	x	x
Softwarebetreiber	muss	Dokumentieren wie beim Erreichen einer Ressourcengrenze reagiert wird.	Vor allem beim Überschreiten der Quotas Normalerweise ziehen hier auch die Standard-Kubernetes-Mechanismen, allerdings auch die Eskalationswege, wenn grundsätzlich Maxima überschritten werden. Die Reaktionen könnten dann z.B. im Rahmen von Risikotabellen entsprechend definiert werden	x		
Plattformbetreiber	muss	Quotierungen auf dem Namespace setzen.	https://kubernetes.io/docs/concepts/policy/resource-quotas/			x
Plattformbetreiber	kann	Default-Limits in den Namespaces konfigurieren.	https://kubernetes.io/docs/tasks/administer-cluster/manage-resources/memory-default-namespace/ Dies ist eine Komfort-Funktion, die Defaults definiert, falls ein Pod/Containerr keine Limits oder Requests setzt. Sind diese Werte nicht gesetzt, kann ein Pod nicht starten!	x		
Plattformbetreiber	kann	ein Ressourcen Management nach außen zur Containerverwaltung exponieren.				
Plattformbetreiber	sollte	aus dem Kapazitäts-Forecast der Softwarebetreiber einen Gesamtüberblick generieren und den Softwarebetreibern mitteilen, ob und wann die angeforderte Kapazität zur Verfügung steht.				
Plattformbetreiber	muss	bekanntgeben wie seine Kuberneteslösung im Falle des Erreichens einer Ressourcengrenze reagiert.				

SYS.1.6.A16 Administrativer Fernzugriff auf Container (S)

Administrative Zugriffe von einem Container auf den Container-Host und umgekehrt SOLLTEN prinzipiell wie administrative Fernzugriffe betrachtet werden. Aus einem Container SOLLTEN KEINE administrativen Fernzugriffe auf den Container-Host erfolgen.

Applikations-Container SOLLTEN keine Fernwartungszugänge enthalten. Administrative Zugriffe auf Applikations-Container SOLLTEN immer über die Container-Runtime erfolgen.

Archiv: BSI 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.*

Anmerkung: stark verkürzt mit anderem Ansatz-Blickwinkel für Administration

Rolle	Prio	Anforderung	Anmerkungen	CICD	Whitepaper SWL	per Policy prüfbar
Softwarelieferant	muss	die Software so bereitstellen, dass kein Fernzugriff bei der Implementierung und beim Betrieb erforderlich ist.	Software zum administrativen Zugriff wie zum Beispiel ssh, telnet sollten in den Images nicht vorhanden und auch nicht erforderlich sein. (vgl. IG BvC SYS.1.6.A23 ALT)		x	P
Softwarelieferant	muss	sicherstellen, dass in der gelieferten Software (Images) keine Komponenten zur Fernwartung enthalten sind.	Applikations-Container SOLLTEN keine Fernwartungszugänge enthalten. Außgeschlossen sind dabei Infrastruktur Container (API für Datenbanken und Storage Systeme). Defintion von Infrastruktur Container noch abklären		x	
Softwarebetreiber	muss	die Software (Images vom Softwarelieferanten) daraufhin überprüfen, dass keine Software zur Fernwartung enthalten ist.	z.B. Services / Anwendungen wie SSH, Telnet, RDP, ... (vgl. IG BvC SYS.1.6.A23 ALT) Applikations-Container SOLLTEN keine Fernwartungszugänge enthalten.	x		
Plattformbetreiber	muss	ein Regelwerk (Network Policies) erstellen, welche Dienste innerhalb von Containern bei ihm erlaubt, bzw. verboten sind.	(vgl. IG BvC SYS.1.6.A23 ALT) Applikations-Container SOLLTEN keine Fernwartungszugänge enthalten. typische zu unterbindende Protokolle für die Fernwartung sind, z.B. SSH, Telnet, RDP, VNC. Der Plattformbetreiber sollte geeignete Werkzeuge zur automatischen Prüfung der Images bereitstellen, z. B. Imagescanner.	x		o
Softwarebetreiber	muss	sicherstellen, dass die Images den gesetzten Policies entsprechen.				
Softwarebetreiber	muss	sicherstellen, dass aus einem Container heraus keine administrativen Zugriffe auf den Container-Host erfolgen können.	Sicherstellung durch Image Scan & Einhaltung der Policies.			o
Softwarebetreiber	muss	sicherstellen, dass administrative Zugriffe auf Applikations-Container immer über die Container-Runtime erfolgen.	Zugriffe sollten möglichst über ein Management-Interface erfolgen.			
Softwarebetreiber	muss	sicherstellen, dass administrative Zugriffe auf Container hinreichend gesichert (z.B. durch Authentisierung, Authorisierung, Verschlüsselung, Integritätswahrung) erfolgen.				
Plattformbetreiber	muss	sicherstellen, dass administrative Zugriffe auf Container-Hosts hinreichend gesichert (z.B. durch Authentisierung, Authorisierung, Verschlüsselung, Integritätswahrung) erfolgen.	Administrative Zugriffe vom Container-Host zum Container SOLLTEN prinzipiell wie administrative Fernzugriffe betrachtet werden.			
Plattformbetreiber	sollte	die Kommunikation im Netzwerk laufender Container auf unerlaubte Protokolle und offene Kommunikationsendpunkte (Ports) überwachen.	Das Vorgehen und die Reaktion auf Ereignisse wird in den übergreifenden BSI-Anforderungen beschrieben und müssen entsprechend für das jeweilge Rechenzentrum geregelt werden. z.B. IDS und Port-Scans (vgl. IG BvC SYS.1.6.A23 ALT)			o

SYS.1.6.A17 Ausführung von Containern ohne Privilegien (S)

Die Container-Runtime und alle instanziierten Container SOLLTEN nur von einem nicht-privilegierten System-Account ausgeführt werden, der keine erweiterten Rechte für den Container-Dienst bzw. das Betriebssystem des Host-Systems verfügt oder diese Rechte erlangen kann. Die Container-Runtime SOLLTE durch zusätzliche Maßnahmen gekapselt werden, etwa durch Verwendung der Virtualisierungs-Erweiterungen von CPUs.

Sofern Container ausnahmsweise Aufgaben des Host-Systems übernehmen sollen, SOLLTEN die Privilegien auf dem Host-System auf das erforderliche Minimum begrenzt werden. Ausnahmen SOLLTEN angemessen dokumentiert werden.

Archiv: BSI 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.

Anmerkung: konkretisiert sowie stark erweitert

Rolle	Prio	Anforderung	Anmerkungen	CICD	Whitepaper SWL	per Policy prüfbar
Softwarelieferant	MUSS	die Software so gestalten, dass die Container-Runtime und alle instanziierten Container nur von einem nicht-privilegierten System-Account ausgeführt werden, der keine erweiterten Rechte für den Container-Dienst bzw. das Betriebssystem des Host-Systems benötigt oder diese Rechte erlangen kann. Ausnahmen hiervon sind Container, welche Aufgaben des Host-Systems übernehmen.	kein "privileged"-Mode für die Container-Runtime und den laufenden Containern Beispiel für Ausnahmen sind: - ingress, egress - Infrastrukturcontainer Beispiele für Aufgaben des Hostsystems sind: - ingress und egress sind Bastion-Node-Aufgaben - Bereitstellung von Speichersystemen sind Speicher-Node-Aufgaben		X	P
Softwarelieferant	MUSS	die Privilegien für Container auf das erforderliche Minimum begrenzen.			x	
Softwarebetreiber	MUSS	die Informationen zur Einschränkung der Nutzung von erweiterten Privilegien dem Softwarelieferanten zur Verfügung stellen.			X	
Softwarebetreiber	MUSS	die Konfiguration so umsetzen, dass keine erweiterten Privilegien angefordert werden. Ausnahmen hiervon sind Container, welche Aufgaben des Host-Systems übernehmen.				
Softwarebetreiber	MUSS	die Privilegien für Container auf das erforderliche Minimum begrenzen.				
Plattformbetreiber	MUSS	die Informationen zur Einschränkung der Nutzung von erweiterten Privilegien dem Softwarebetreiber zur Verfügung stellen.				
Plattformbetreiber	MUSS	sicherstellen, dass die Ausführung der Container-Runtime und von den instanziierten Containern als root User nicht möglich ist. Ausnahmen hiervon sind Container, welche Aufgaben des Host-Systems übernehmen.				
Plattformbetreiber	MUSS	sicherstellen, dass die Nutzung erweiterter Rechte bei der Ausführung der Container-Runtime und von den instanziierten Containern verhindert wird. Ausnahmen hiervon sind Container, welche Aufgaben des Host-Systems übernehmen.	Beispiele für erweiterte Rechte sind: - Schreibender Zugriff auf persistenten Speicher - Anpassung von Kernelparameter			
Plattformbetreiber	KANN	Container mit privilegierten Rechten in den Plattformbetrieb übernehmen. Dieses muss angemessen dokumentiert werden.				
Plattformbetreiber	SOLLTE	*zusätzliche Maßnahmen* zur Kapselung der Container-Runtime durchführen.				
Plattformbetreiber	MUSS	die Privilegien für Container auf das erforderliche Minimum begrenzen.				

SYS.1.6.A18 Accounts der Anwendungsdienste (S)

Die System-Accounts innerhalb eines Containers SOLLTEN keine Berechtigungen auf dem Host-System haben. Wo aus betrieblichen Gründen diese Berechtigung notwendig ist, SOLLTE diese nur für unbedingt notwendige Daten und Systemzugriffe gelten. Der Account im Container, der für diesen Datenaustausch notwendig ist, SOLLTE im Host-System bekannt sein.

Archiv: BSI 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.

Anmerkung: Maßnahme ergänzt

Rolle	Prio	Anforderung	Anmerkungen	CICD	Whitepaper SWL	per Policy prüfbar
Softwarelieferant	muss	die Software so gestalten, dass die genutzten User- und Group-ID's keine Berechtigungen auf die System- und Datenbereiche des Hosts erfordern.		x	x	P
Softwarelieferant	muss	die erforderlichen User- und Group-ID's und deren Berechtigungen benennen (z.B. in den Konfigurationsdateien).		x	x	o
Softwarebetreiber	muss	die Vorgaben des Plattformbetreibers durch eigene Sicherheitsvorgaben soweit vorhanden ergänzen und an den Softwarelieferanten geben.		x	x	
Softwarebetreiber	muss	die Einhaltung der Sicherheitsvorgaben durch den Softwarelieferanten prüfen, überwachen und durchsetzen (z.B. durch SLAs und in der Konfiguration).		x		
Plattformbetreiber	muss	einen Bereich von User- und Group-ID's zur Verwendung in Containern bereitstellen, die keine Berechtigungen auf die System- und Datenbereiche der Container-Hosts besitzen.	Für Infrastrukturcontainer usw. im Verantwortungsbereich des Plattformbetreibers können dokumentierte Ausnahmen gemacht werden. Eine entsprechende enge Überwachung muss sichergestellt werden.	x		o (Durchsetzung eines Bereichs von IDs über Policy)
Plattformbetreiber	muss	sicherstellen, dass Container nicht unter Root-Rechten laufen.	Innerhalb der Container können Root-Rechte verwendet werden.			o
Plattformbetreiber	muss	die Nutzung privilegierter User- und Group-ID's sowie eine Rechteerweiterung (z.B. Set-UID-Bit / Set-GID-Bit) unterbinden.				o
Plattformbetreiber	sollte	Rechterweiterungen durch den Einsatz erweiterter Zugriffssysteme (Mandatory Access Control Systems) wirksam unterbinden.	Beispiele für Systeme SELinux, AppArmor			

siehe auch:

https://kubernetes.io/docs/concepts/policy/pod-security-policy/#users-and-groups (ab 1.21 deprecated ab 1.25 entfernt)

https://kubernetes.io/docs/concepts/policy/pod-security-policy/#volumes-and-file-systems (ab 1.21 deprecated ab 1.25 entfernt)

https://kubernetes.io/docs/tasks/configure-pod-container/security-context/

Wird durch https://kubernetes.io/docs/concepts/security/pod-security-admission/ ersetzt und könnte durch Kyverno oder opa abgebildet werden.

SYS.1.6.A19 Einbinden von Datenspeichern in Container (S)

Die Container SOLLTEN NUR auf die für den Betrieb notwendigen Massenspeicher und Verzeichnisse zugreifen können. Nur wenn Berechtigungen benötigt werden, SOLLTEN diese explizit vergeben werden. Sofern die Container-Runtime für einen Container lokalen Speicher einbindet, SOLLTEN die Zugriffsrechte im Dateisystem auf denService-Account des Containers eingeschränkt sein. Werden Netzspeicher verwendet, so SOLLTEN die Berechtigungenauf dem Netzspeicher selbst gesetzt werden.

Archiv: BSI SYS.1.6.A17 Einbinden von Massenspeichern in Containern (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.

Rolle	Prio	Anforderung	Anmerkungen	CICD	Whitepaper SWL	per Policy prüfbar
Softwarelieferant	sollte	keine lokalen Speicher der Workernodes benutzen.	Es sollte nur persistent Storage genutzt werden. (vgl. BSI SYS.1.6.A17 ALT) Sollte bietet Ausnahmen für flüchtige Anwendungsfälle [virenscan].		x	P o (hostPath)
Softwarelieferant	muss	notwendige persistente Volumen und deren Nutzung (z. B. RWM, RWO, RW/RO) im Deployment beschreiben.	z.B. Zielpfad im Containerbetrieb, Größe, Berechtigungen, Dateisystem, Performance Die Beschreibung sollte in einer formalen Sprache erfolgen. Das Pysical Volume Claim soll dynamisch erfolgen. Bitte mögliche Einschränkungen im Rechzentrum beachten. (vgl. BSI SYS.1.6.A17 ALT)		x	o
Softwarelieferant	muss	notwendige Berechtigungen im Deployment beschreiben. Diese müssen minimal gewählt werden.				o
Softwarebetreiber	muss	persistente Volumen so beschreiben, dass nur berechtigte Container darauf zugreifen können.	(vgl. BSI SYS.1.6.A17 ALT)			
Softwarebetreiber	sollte	keine lokalen Speicher der Workernodes benutzen.	(vgl. BSI SYS.1.6.A17 ALT)			o (hostPath)
Softwarebetreiber	muss	den Zugriff auf lokalen Speicher der Workernodes auf den Service-Account des Containers einschränken.				
Softwarebetreiber	muss	den Zugriff auf Speicher auf die für den Betrieb erforderlichen Berechtigungen einschränken (Principle of Least Privilege).	Die Einschränkung des Zugriffs ist wesentlich von den eingesetzten Technoligien zu Speicherbereitstellung abhängig.			o
Plattformbetreiber	muss	den Zugriff auf Speicher auf die für den Betrieb erforderlichen Berechtigungen einschränken (Principle of Least Privilege).	Die Einschränkung des Zugriffs ist wesentlich von den eingesetzten Technoligien zu Speicherbereitstellung abhängig.			o
Plattformbetreiber	sollte	die Größe der persistenten Volumen begrenzen.	(vgl. BSI SYS.1.6.A17 ALT)			o
Softwarebetreiber	muss	die Größe der benötigten persistenten Volumen vorgeben.				

SYS.1.6.A20 Absicherung von Konfigurationsdaten (S)

Die Beschreibung der Container-Konfigurationsdaten SOLLTE versioniert erfolgen. Änderungen SOLLTEN nachvollziehbar dokumentiert sein.

Archiv: BSI 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.
Anmerkung: Anforderung reduziert auf Versionierung und Dokumenation.

Rolle	Prio	Anforderung	Anmerkungen	CICD	Whitepaper SWL	per Policy prüfbar
Softwarelieferant	muss	die mitgelieferte Konfiguration der Container versioniert bereitstellen und den Bezug zu Imageversionen sicherstellen.	Entweder z.B. durch Label in der YAML oder als git-repo.		x	---
Softwarebetreiber	muss	den Zugang zur Ablage der Konfigurationsdaten der Container mit definierten Rechten vergeben.	siehe APP4.4 A2	x		
Softwarebetreiber	muss	die Umsetzung, Durchgängigkeit und Nachvollziehbarkeit der Konfigurationsänderungen sicherstellen.		x		
Softwarebetreiber	muss	geeignete Möglichkeiten zur Versionierung von Konfigurationsdaten verwenden.		x		
Plattformbetreiber	muss	geeignete Möglichkeiten zum mandantenfähigen Geheimnismanagement bereitstellen.			x	
Softwarebetreiber	muss	dem Softwarelieferanten geeignete Möglichkeiten zum Geheimnisaustausch bieten.			x	

SYS.1.6.A21 Erweiterte Sicherheitsrichtlinien (H)

Erweiterte Richtlinien SOLLTEN die Berechtigungen der Container einschränken. Mandatory Access Control (MAC) oder eine vergleichbare Technik SOLLTE diese Richtlinien erzwingen. Die Richtlinien SOLLTEN mindestens folgende Zugriffe einschränken:

· eingehende und ausgehende Netzverbindungen,

· Dateisystem-Zugriffe und

· Kernel-Anfragen (Syscalls).

Die Runtime SOLLTE die Container so starten, dass der Kernel des Host-Systems alle nicht von der Richtlinie erlaubten Aktivitäten der Container verhindert (z. B. durch die Einrichtung lokaler Paketfilter oder durch Entzug von Berechtigungen) oder zumindest Verstöße geeignet meldet.

~~*Archiv : B5I 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).~~

~~*Anmerkung: Maßnahme um Anforderungen ergänzt*~~

HINWEIS: Es wurden verschiedene Aspekte aus den alten Ausarbeitungen (SYS.1.6.A31) in die neue Ausarbeitung (SYS.1.6.A21 und A26) übernommen. Änderungen sind farbig markiert.

Rolle	Prio	Anforderung	Anmerkungen	CICD	Whitepaper SWL	per Policy prüfbar
Softwarelieferant	MUSS	Zugriffe und Berechtigungen auf Ressourcen durch seine Software auf die technisch notwendigen Zugriffe beschränken.			x	P
Softwarelieferant	MUSS	benötigte Zugriffe und Berechtigungen auf Ressourcen dokumentieren.			x	
Softwarebetreiber	MUSS	Richtlinien zur Einschränkung von Zugriffen und Berechtigungen auf Ressourcen definieren.		x		o
Softwarebetreiber	SOLLTE	die erweiterten Richtlinien gemeinsam mit dem Plattformbetreiber und dem Softwarelieferanten abstimmen.				
Plattformbetreiber	MUSS	Richtlinien für Softwarebetreiber zur Einschränkung von Zugriffen und Berechtigungen auf Ressourcen vorgeben.	Ziel ist die Vorgabe eines Rahmens, indem sich der Softwarebetreiber bewegen darf.			O20 + O21 + O22 + ?
Plattformbetreiber	MUSS	die Isolation durch die minimal erforderlichen Berechtigungen auf Ressourcen und Kernelfunktionen sicherstellen und Verstöße gegen die Richtlinien unterbinden und protokollieren.	z.B. Umsetzung geeigneter Einstellungen der Ausführungsumgebung (Runtime) und durch kernel capability, seccomp, SELinux, AppArmor, https://falco.org/	x		o
Plattformbetreiber	MUSS	die Isolation des Netzwerkverkehrs zwischen unterschiedlichen Workloads, Anwendungen und Mandanten sicherstellen sowie Verstöße gegen die Richtlinien unterbinden und protokollieren.	z.B. Einsatz einer Ausführungsumgebung (Runtime) mit Unterstützung für VLANs, Firewall-Richtlinien, virtuelle Switche, Software Defined Networks, Network Function Virtualsierung Der Plattformbetreiber implementiert und konfiguriert ein Netzwerk-Plugin so, dass im Standardverhalten keine Kommunikation zwischen Workloads ermöglicht wird. Die erforderlichen Kommunikationsverbindungen der Fachanwendungen werden durch den Softwarebetreiber in den Deployments definiert und umgesetzt.			
Plattformbetreiber	kann	eine Umgebung bereitstellen, um Tests auszuführen und Seccomp-Profile automatisiert zu erstellen.	z.B. zur Unterstützung des Softwarebetreibers https://kubernetes.io/docs/tutorials/clusters/seccomp/ https://kubernetes.io/docs/concepts/policy/pod-security-policy/#seccomp			
Plattformbetreiber	sollte	restriktive Default-Seccomp-Profile bereitstellen, die für Anwendungen verwendet werden können, die keine definierten Seccomp-Profile haben.	https://kubernetes.io/docs/concepts/security/pod-security-standards/	x		
Plattformbetreiber	sollte	werkzeugunterstütztes Richtlinienmanagement betreiben und die Einhaltung von Richtlinien überprüfen.	Der Plattformbetreiber kann Ressourcen vor deren Instanziierung automatisiert im Cluster anpassen um die Einhaltung von erweiterten Richtlinien zu erzwingen (mutation) oder gänzlich ablehnen (validation) wenn diese nicht den Richtlinien genügen. Dabei können gängige (Kubernetes-)Werkzeuge und Praktiken genutzt werden (admission controller). Z.b. mit: https://kyverno.io/ https://www.openpolicyagent.org/ ... https://kubernetes.io/docs/reference/access-authn-authz/admission-controllers/			

SYS.1.6.A22 Vorsorge für Untersuchungen (H)

Um Container im Bedarfsfall für eine spätere Untersuchung verfügbar zu haben, SOLLTE ein Abbild des Zustands nach festgelegten Regeln erstellt werden.

Anmerkung: neue Maßnahme

Rolle	Prio	Anforderung	Anmerkungen	CI/CD	Whitepaper SWL	per Policy prüfbar
Softwarelieferant	sollte	Hilfestellung zu Möglichkeiten für forensische Analysen dem Softwarebetreiber anbieten.	z.B. Log-Funktionalitäten, Konfigurationsdateien, Funktionalitäten zu Rückverfolgung von Änderungen		x	---
Softwarebetreiber	sollte	sicherstellen, dass eine forensische Untersuchung der betriebenen Lösung realisiert werden kann.	SIEM- und Auditierfähigkeit beachten			
Softwarebetreiber	sollte	die Möglichkeiten (Hilfestellung) des Softwarelieferanten so aufbereiten, dass diese durch den Plattformbetreiber umgesetzt werden können.				
Plattformbetreiber	sollte	technisch und organisatorisch in der Lage sein, im Falle eines Sicherheitsvorfalles ein für forensische Untersuchungen geeignetes Abbild zu erstellen.	u.a. Abbild des Arbeitsspeichers			
~~Plattformbetreiber~~	~~sollte~~	~~in der Lage sein, ein Abbild des Arbeitsspeichers der Hardware für mögliche spätere Untersuchungen zur Verfügung zu stellen.~~				

SYS.1.6.A23 Unveränderlichkeit der Container (H)

Container SOLLTEN ihr Dateisystem während der Laufzeit nicht verändern können. Dateisysteme SOLLTEN nicht mit Schreibrechten eingebunden sein.

Archiv: BSI SYS.1.6.A15 Unveränderlichkeit der Container (S)

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

Anmerkung: Scope liegt nun auf den nicht-persistenten Containern

Rolle	Prio	Anforderung	Anmerkungen	CICD	Whitepaper SWL	per Policy prüfbar
Softwarelieferant	MUSS	Regelungen des Softwarebetreibers berücksichtigen und auf Funktionen verzichten, die Veränderungen auf die Datenbereiche / das File-System des Containers erfordern (z.B. Updates, Protokollierung, Nutzdaten). Der Container muss in seinen Ressourcen eingeschränkt werden (z.B. Datenmenge und Speicherzugriffe).			x	P
Softwarelieferant	MUSS	sicherstellen, dass Daten nicht in das Root-File-System geschrieben werden können.		x	x	
Softwarelieferant	MUSS	Daten in eigene Mount-Verzeichnisse schreiben.		x	x	
Softwarelieferant	MUSS	ermöglichen, dass Daten die im Container ausschließlich gelesen werden, als Read-Only Volume in den Container eingebunden werden können.	Hinweis: Ein technischer Ansatz kann die Pod-Security-Policy "ReadOnlyRootFileSystem" sein. TM: PodSecurityPolicy ist jetzt securityContext		x	
Softwarelieferant	MUSS	das temporäre Speichern von Daten in besonders dafür bereitgestellten Volumes vornehmen.		x	x	
Softwarebetreiber	MUSS	Daten die im Container ausschließlich gelesen werden, als Read-Only Volume in den Container einbinden.		x		
Softwarebetreiber	SOLL	sicherstellen, dass Dateisysteme nicht mit Schreibrechten eingebunden werden.		x	x	
Softwarebetreiber	MUSS	sicherstellen, dass nur minimal erforderliche Rechte vergeben werden (Principle of Least Privilege). Insbesondere muss auf beschreibbaren Volumes auf Execute-Rechte verzichtet werden.		x	x	
Plattformbetreiber	MUSS	die Konfiguration der Plattform so bereitstellen, dass der Betrieb unveränderlicher Container ermöglicht und durchgesetzt wird.	Hinweis: Ein technischer Ansatz kann die Pod-Security-Policy "ReadOnlyRootFileSystem" sein. TM: PodSecurityPolicy ist jetzt securityContext	x		
Plattformbetreiber	MUSS	einen kontrollierten Mechanismus zum temporären Speichern von Daten im Container bereitstellen.	Begrenzungen für temporären Speicher: spec.containers[].resources.limits.ephemeral-storage spec.containers[].resources.requests.ephemeral-storage	x	x	

XXXSYS.1.6.A24 Härtung des Host-Systems mittels Read-Only-Dateisystem (H)

HINWEIS: Der Punkt "Härtung des Host-Systems mittels Read-Only-Dateisystem (H)" wurde ersatzlos im Final Draft des BSI gestrichen. A25ff sind demnach um eines nach oben gerückt

~~*Die Integrität des Hosts sollte durch ein Read-Only-Dateisystem sichergestellt werden (Immutable OS).*~~

Archiv: BSI 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.

Anmerkung: (H) anstatt (B), konkrete Maßnahme für Härtung des Host-Systems, alte Anforderung gehen auch in SYS.1.6.A3 Sicherer Einsatz containerisierter IT-Systeme (B) und APP.4.4.A8 Absicherung von Konfigurationsdateien bei Kubernetes auf.

Rolle	Prio	Anforderung	Anmerkungen	CI/CD	Whitepaper SWL
Softwarelieferant	sollte				
Softwarebetreiber	muss				
Plattformbetreiber	kann				

SYS.1.6.A24 Hostbasierte Angriffserkennung (H)

Das Verhalten der Container und der darin betriebenen Anwendungen bzw. Diensten SOLLTE überwacht werden. Abweichungen von einem normalen Verhalten SOLLTEN bemerkt und gemeldet werden. Die Meldungen SOLLTEN im zentralen Prozess zur Behandlung von Sicherheitsvorfällen angemessen behandelt werden.

Das zu überwachenden Verhalten SOLLTE mindestens umfassen:

· Netzverbindungen,

· erstellte Prozesse,

· Dateisystem-Zugriffe und

· Kernel-Anfragen (Syscalls)

~~*Archiv: BSI SYS.1.6.A32 Host Based Intrusion Detection für Container (H)*~~

Rolle	Prio	Anforderung	Anmerkungen	CICD	Whitepaper SWL	per Policy prüfbar
~~Softwarelieferant~~	~~sollte II muss~~	~~ein neues Images ohne Schwachstellen bereitstellen, sofern Schwachstellen im durch ihn erstellten Image erkannt wurden und behebbar sind.~~	~~z.B. bei Schwachstellenscans während der Laufzeit, sofern Patch vorhanden~~ ~~vgl. SYS.1.6.A14~~ ~~Was, wenn Image mit Schwachstelle, aber kein patch?~~	~~x~~	~~x~~	—
Softwarelieferant	sollte	ein für seine Software erwartbares Verhalten (Systemaufrufe, Kommunikationsbeziehungen usw.) definieren, beschreiben und dem Softwarebetreiber vorlegen.	Hinweis: Wenn der Softwarelieferant das normale Verhalten -wie oben angesprochen- nicht angeben kann, dann muss der Softwarebetreiber das normale Verhalten durch Erprobung feststellen.		x	
Softwarebetreiber	muss	einen Maßnahmenkatalog zur Abarbeitung mit dem Plattformbetreiber abstimmen, wenn Container ein verdächtiges Verhalten aufweisen.	Hierbei muss der zentrale Prozess zur Behandlung von Sicherheitsvorfällen angemessen behandelt werden.			
Softwarebetreiber	muss	auf Meldungen von verdächtigem Verhalten reagieren bzw. automatisierte Reaktionen (bspw. Alarmierung, Beendigung oder Neustart) festlegen.	Eine mögliche Reaktion wäre der Nustart eines Containers bei verdächtigem Verhalten, wenn keine Sicherheitsbedenken für einen solchen Neustart vorliegen. Bei wiederholt verdächtigem Verhalten sollten weitere Maßnahmen wie z.B. Sandboxing abgestimmt werden.			
Softwarebetreiber	muss	Schwellenwerte für die Klassifizierzung abweichenden Verhaltens festlegen, insbesondere wenn automatisierte Reaktionen gewünscht sind.				
Softwarebetreiber	sollte	normales Softwareverhalten durch Erprobung festlegen, um im Produktivbetrieb Abweichungen von diesem erkennen und melden zu können.	Hinweis: Wenn der Softwarelieferant das normale Verhalten -wie oben angesprochen- nicht angeben kann, dann muss der Softwarebetreiber das normale Verhalten durch Erprobung feststellen. z.B. syscalls, Anzahl und Art von Netzwerkverbindungen sowie Dateizugriffen und Kubernetes-API-Calls in Kubernetes nativen Anwendungen		x	
Softwarebetreiber	muss	Ansprechpartner für die Meldung von Anomalien dem Plattformbetreiber benennen.				
Plattformbetreiber	muss	ein System zur Überwachung der Container und der darin betriebenen Anwendungsdienste betreiben. Diese Überwachung sollte mindestens die folgenden Punkte beinhalten: · Netzverbindungen, · erstellte Prozesse, · Dateisystem-Zugriffe und · Kernel-Anfragen (Syscalls)	z.B.: Falco (https://falco.org/)			
Plattformbetreiber	sollte II muss	die Infrastruktur z. B. ein zentrales SIEM zur Meldung von verdächtigem Verhalten bereitstellen.				
Plattformbetreiber	muss	ein externes System zur Protokollierung von Logdaten bereitstellen und die Meldungen des Host Based Intrusion Detection System (HIDS) der Containerplattform revisionssicher speichern.				
Plattformbetreiber	muss	Meldewege respektive Ansprechpartner bei Anomalien vom Softwarebetreiber einfordern.				
Plattformbetreiber	muss	einen Maßnahmenkatalog zur Abarbeitung mit dem Softwarebetreiber abstimmen, wenn Container ein verdächtiges Verhalten aufweisen.	Hierbei muss der zentrale Prozess zur Behandlung von Sicherheitsvorfällen angemessen behandelt werden.			

SYS.1.6.A25 Hochverfügbarkeit von containerisierten Anwendungen (H)

Bei hohen Verfügbarkeitsanforderungen der containerisierten Anwendungen SOLLTE entschieden werden, auf welcher Ebene die Verfügbarkeit realisiert werden soll (z. B. redundant auf der Ebene des Hosts).

Archiv: BSI 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.

Anmerkung: Neue Anforderung: Hier wird nun Bezug auf die containerisierten Anwendungen genommen. Die "alte" Anforderung findet sich in APP.4.4.A19 Hochverfügbarkeit von Pods wieder.

Rolle	Prio	Anforderung	Anmerkungen	CICD	Whitepaper für SWL	per Policy prüfbar
Softwarelieferant	sollte	die Möglichkeiten der Hochverfügbarkeit der Anwendung darstellen.			x	P
Softwarebetreiber	muss	entscheiden welche Verfügbarkeit notwendig ist und wie Hochverfügbarkeit realisiert wird.	Hier MUSS, weil SB hat hierfür den Hut auf und muss auf die anderen zugehen Möglichkeiten für ihn z.B. - Redundant auf der Ebene des Hosts - lässt 2 Cluster parallel laufen mit Load-Balancer oder Traffic-Switch (active bzw. passive) - Autoscaling	x		
Plattformbetreiber	sollte	die Möglichkeit der Hochverfügbarkeit der Plattform darstellen.	Folgende Möglichkeiten wären denkbar: - HV Cluster (spannt über mehrere Brandabschnitte / Availability zones)			

SYS.1.6.A26 Weitergehende Isolation und Kapselung von Containern (H)

Wird eine weitergehende Isolation und Kapselung von Containern benötigt, dann SOLLTEN folgende Maßnahmen nach steigender Wirksamkeit geprüft werden:

· feste Zuordnung von Containern zu Container-Hosts,

· Ausführung der einzelnen Container und/oder des Container-Hosts mit Hypervisoren,

· feste Zuordnung eines einzelnen Containers zu einem einzelnen Container-Host.

~~*Anmerkung: neue Anforderung, keine inhaltliche Überdeckung mit altem Baustein gefunden - evtl. sind Umsetzungshinweise aus DSI SYS.1.6.A5 Separierung der Container (B) verwendbar*~~

HINWEIS: Es wurden verschiedene Aspekte aus den alten Ausarbeitungen (SYS.1.6.A31) in die neue Ausarbeitung (SYS.1.6.A21 und A26) übernommen. Änderungen sind farbig markiert.

Anm.: Container im Sinne von Pods (Kubernetes)

siehe auch: APP.4.4.A15 Trennung von Anwendungen auf Node- und Cluster-Ebene (H)

Rolle	Prio	Anforderung	Anmerkungen	CI/CD	Whitepaper SWL	per Policy prüfbar
Softwarelieferant	muss	dem Softwarebetreiber die vom Ihm definierten erweiterten Maßnahmen mitteilen, sofern vorhanden	· feste Zuordnung von Containern zu Container-Hosts, · Ausführung der einzelnen Container und/oder des Container-Hosts mit Hypervisoren, · feste Zuordnung eines einzelnen Containers zu einem einzelnen Container-Host.	X	X	P
Softwarebetreiber	muss	ein Risikoanalyse zum Nachweiß der Notwendigkeit der weiteren Maßnahmen durchführen und sofern notwenig geeignete weitere Maßnahmen definieren.	· feste Zuordnung von Containern zu Container-Hosts, · Ausführung der einzelnen Container und/oder des Container-Hosts mit Hypervisoren, · feste Zuordnung eines einzelnen Containers zu einem einzelnen Container-Host.	X		
Softwarebetreiber	muss	dem Softwarelieferanten die vom Ihm definierten erweiterten Maßnahmen mitteilen, sofern vorhanden.	· feste Zuordnung von Containern zu Container-Hosts, · Ausführung der einzelnen Container und/oder des Container-Hosts mit Hypervisoren, · feste Zuordnung eines einzelnen Containers zu einem einzelnen Container-Host.		X	
Softwarebetreiber	muss	dem Plattformbetreiber die von ihm definierten Maßnahmen mitteilen.	Sollte der Plattformbetreiber die Maßnahme nicht umsetzten können, muss der Softwarebetreiber einen geeigneten Plattformbetreiber aussuchen.			
Plattformbetreiber	muss	die geforderten Maßnahmen vom Softwarebetreiber umsetzen.		X		