DEUTSCHE VERWALTUNGSCLOUD
EIN PRODUKT DES IT-PLANUNGSRATS

Detailstandard 08: Grundannahmen zu Kubernetes an Cloud Standorten

Version 2.0 (28.12.2025)

Inhaltsverzeichnis

Zusammenfassung

Dieser Detailstandard regelt die "Grundannahmen zu Kubernetes an Cloud Standorten" für die DVC (für Cloud-Service-Anbieter der DVC im Sinne von Plattformbetreibern und Softwarebetreibern, sofern letztere eigene Cloud-Standorte unterhalten). Der Detailstandard „Grundannahmen zu Kubernetes an Cloud Standorten" beschreibt ergänzend zum Detailstandard #01 ("Zonenmodell am (DVC) Cloud Standort") die qualitativen und fachlichen Anforderungen, die bei der Nutzung von Kubernetes als Containerorchestrierungsschicht beachtet werden müssen.

Disclaimer

Nachfolgend wird ausschließlich auf den Begriff "Plattformbetreiber" referenziert. Dabei ist unerheblich, ob es sich um ausschließlich "Plattformbetreiber" mit Kubernetes PaaS-Angeboten für die DVC handelt oder ob es sich um Softwarebetreiber handelt, die im Kontext Kubernetes ihr eigener Plattformbetreiber sind.

Schutzbedarf

Die nachfolgenden Ausführungen fokussieren auf die Schutzbedarfsklasse "Normal" angewendet werden (in Umsetzung IT-Grundschutz).

Hinweise: - Bei höherem Schutzbedarf und/oder VS-Anforderungen kommen ggf weitere Zonenaufteilungen erzwungen werden (nach Ermessen/Beschreibung des Anbieters) - Bei hohem Schutzbedarf würden ggf weitere Komponenten an Sicherheitssystemen (wie Integritätschecker) ergänzt werden (nach Ermessen / Beschreibung des Anbieters)

Anforderung

Für die Belange der DVC ist die Nutzung **cloud-nativer und cloud-fähiger Software** für die Bereitstellung von DVC Services im SaaS-Umfeld empfohlen. In diesem Kontext sollte Software wo möglich **containerisiert** werden. Als **Containerorchestrierungsumgebung ist gegenwärtig Kubernetes** empfohlen. Dieser Detailstandard regelt dafür **Grundannahmen für den Einsatz von Kubernetes an Cloud Standorten.** Wie in der Zusammenfassung herausgearbeitet gehen wir dabei für das Kapitel "Standardisierung" von einem erweiterten Begriff des (DVC) "Plattformbetreibers" aus, der auch Softwarebetreiber umfasst, die an eigenen Cloud-Standorten (quasi als eigener Plattformbetreiber) Kubernetes verwenden.

Der Einsatz von Kubernetes in einer DMZ der DVC (vergleiche Detailstandard 1) ist grundlegend **nur vorzusehen**, solange zwischen dem Zugangspunkt des Cloud-Standorts und anwendungsspezifischen Workloads in Kubernetes-Clustern immer eine PAP-Struktur (Paketfilter - Application Level Gateway - Paketfilter) gewährleistet bleibt. Details können beispielsweise Detailstandard #2 entnommen werden. Für die "klassische" Trennung von Webservice, Anwendungsdiensten

und Datenbanken ist festzuhalten, dass diese Dienste in Kubernetes Clustern **zusammengefasst werden können**, solange dabei **nicht gegen entsprechende Vorgaben des BSI** verstossen wird. Es können dabei allerdings auch separate Cluster genutzt werden, die wiederum durch geeignete Strukturen getrennt sind.

Verwandt damit regelt BSI SYS.1.6.A2 auch, dass der Softwarebetreiber(/Kunde) **die Entwicklungsumgebung(en) und die Produktivumgebung(en) in verschiedenen Kubernetes-Clustern** betreiben müssen.

Ergänzende Regelungen zu den nachfolgenden Ausführungen werden in **weiteren Detailstandards** (z.B. über die bereits genannten #1 und #2 auch #25, #26, #27, #28, #48 und #49) abgebildet.

Standardisierung

A - Grundlegende Vorgaben des BSI (BSI SYS.1.6.A2 & BSI SYS.1.6.A5)

ID	Rolle	Modalverb	Detailanforderung
DS_08_A001	Plattformbetreiber	MUSS	Sicherstellen, dass Nutzer-Workloads grundsätzlich **keine (System-) Namespaces mit dem Host** teilen können. (BSI SYS.1.6.A5)
DS_08_A002	Plattformbetreiber	MUSS	Die **Isolation der Container** durch geeignete Berechtigungen auf Ressourcen und Kernel-Funktionen sicherstellen. (BSI SYS.1.6.A5)
DS_08_A003	Plattformbetreiber	MUSS	Sicherstellen, dass **Master-Nodes keine Nutzer-Workloads** ausführen dürfen (BSI SYS.1.6.A5)
DS_08_A004	Plattformbetreiber	MUSS	Die **Control-Plane von den Worker-Nodes** trennen (BSI SYS.1.6.A2)
DS_08_A005	Plattformbetreiber	MUSS	Anwendungen mit verschiedenen Schutzbedarfen in getrennten Clustern betreiben (BSI SYS.1.6.A2) Wenn als Service ein **kompletter Cluster** angefordert wird, gibt der unterstützte Schutzbedarf gemäß der Einstufung des Plattformbetreibers dem Softwarebetreiber(/Kunden) den Handlungsspielraum vor. Der Softwarebetreiber(/Kunden) entscheidet, ob die Schutzziele durch die betriebenen Verfahren eingehalten werden.Wenn als Service ein **Namespace** angefordert wird, muss der Plattformbetreiber sicherstellen, dass die Schutzziele der Fachverfahren erfüllt bleiben. Beispiel: Der Cluster soll SB hoch ermöglichen, dann müssen alle Fachverfahren im Cluster die Anforderungen hinsichtlich SB erfüllen. Disclaimer BSI SYS.1.6.A2 regelt auch, dass der Softwarebetreiber(/Kunde) die Entwicklungsumgebung(en) und die Produktivumgebung(en) in verschiedenen Kubernetes-Clustern betreiben MUSS.

B - INGRESS/EGRESS Konfiguration

ID	Rolle	Modalverb	Detailanforderung
DS_08_A101	Plattformbetreiber	MUSS	sicherstellen, dass er die komplette **Kontrolle über einen zentralen INGRESS/EGRESS** für den Kubernetes Cluster behält
DS_08_A102	Plattformbetreiber	MUSS	jeweils einen **zentralen INGRESS/EGRESS** über den kube-system Namespace der Worker-Nodes bereitstellen
DS_08_A103	Plattformbetreiber	MUSS	den **kube-system Namespace vor dem unmittelbaren Zugriff** der Kunden schützen

Fortsetzung auf nächster Seite

Fortsetzung von vorheriger Seite

ID	Rolle	Modal-verb	Detailanforderung
DS_08_A104	Plattform-betreiber	MUSS	die **network-policies des Clusters vor dem unmittelbaren Zugriff** der Kunden schützen
DS_08_A105	Plattform-betreiber	SOLL	prüfen, ob er den zentralen **INGRESS/EGRESS über spezifische Worker-Nodes** bereitstellen kann, auf denen keine Kunden-Workloads laufen ("Infrastruktur Nodes")
DS_08_A106	Plattform-betreiber	MUSS	gewährleisten, dass der Kunde beim **Deployment (von kundeneigenen Namespaces) die network-policy** in einem durch den Plattformbetreiber definierten Maß konfigurieren kann
DS_08_A107	Plattform-betreiber	MUSS	gewährleisten, dass der Kunde beim **Deployment (von kundeneigenen Namespaces) den ingress/egress** in einem durch den Plattformbetreiber definierten Maß konfigurieren kann

C - Separierung Control Plane ("Master Nodes") vs. Worker Nodes

ID	Rolle	Modal-verb	Detailanforderung
DS_08_A201	Plattform-betreiber	MUSS	die **Master-Nodes vor Kompromittierung** durch die aufgeschalteten Kunden schützen (Rechte & Rollenkonzept)
DS_08_A202	Plattform-betreiber	MUSS	**die Kubernetes API (kubectl) durch RBAC-Mechanismen** mit einem Rollen- und Rechtemodell schützen
DS_08_A203	Plattform-betreiber	MUSS	seinen Kunden **begrenzten Zugang zur Kubernetes API (kubectl) gewähren**, damit diese ihre Namespaces direkt oder indirekt deployen können.

D - Trennung "Externe Services" (= Internet Zugang) vs. "Interne Services" (= Verwaltungszugang)

ID	Rolle	Modal-verb	Detailanforderung
DS_08_A301	Plattform-betreiber	MUSS	Gemäß Zonenkonzept (Detailstandard 1) der DVC ist sicherzustellen, dass der Plattformbetreiber **für die Aufschaltung von (Kubernetes-basierten) Anwendungen zu DVC Cloud Services** so genannte **"Externe Services"** (im Sinne von mit dem Internet gemäß Detailstandard 2 für Nutzerzugriff eingehend verbundene Anwendungen) von so genannten **"Internen Services"** (im Sinne von für Nutzerzugriff nur mit Verwaltungsnetzen eingehend verbundenen Anwendungen) **logisch separiert**
DS_08_A302	Plattform-betreiber	SOLL	Gemäß Zonenkonzept (Detailstandard 1) der DVC ist zu prüfen, ob der Plattformbetreiber **für die Aufschaltung von (Kubernetes-basierten) DVC Cloud Services** so genannte **"Externe Services"** (im Sinne von mit dem Internet gemäß Detailstandard 2 für Nutzerzugriff eingehend verbundene Systeme) von so genannten **"Internen Services"** (im Sinne von für Nutzerzugriff nur mit Verwaltungsnetzen eingehend verbundenen Systemen) **physisch separiert**

Fortsetzung auf nächster Seite

Fortsetzung von vorheriger Seite

ID	Rolle	Modal-verb	Detailanforderung
DS_08_A303	Plattform-betreiber	KANN	Ein Plattformbetreiber kann auf eine Zone für "Externe Services" bewusst verzichten, wenn er dies möchte. Eine Vermengung von Zonen für "Interner Services" und "Externer Services" ist jedoch gemäß der Ausführungen von DS_08_A301 und DS_08_A302 nicht zulässig.
DS_08_A304	Plattform-betreiber	SOLL	Ein Plattformbetreiber sollte eine Zone für **"Interne Services"** etablieren Eine Vermengung von Zonen für "Interner Services" und "Externer Services" ist jedoch gemäß der Ausführungen von DS_08_A301 und DS_08_A302 nicht zulässig.

E - Unterschiede "(Kubernetes) Cluster as a Service" vs "(Kubernetes) Namespace as a Service

ID	Rolle	Modal-verb	Detailanforderung
DS_08_A401	Plattform-betreiber	MUSS	Der Plattformbetreiber muss **diversifizieren**, ob er einen **kompletten Kubernetes-Cluster** an seine Kunden (**dediziert**) übergibt oder ob er einen Arbeitsbereich auf einer (**shared**) Kubernetes-Cluster-Infrastruktur bereitstellt. Im letzteren Fall kommt dem **Namespace** eine entscheidende Rolle zu. Diese Modelle werden entsprechend als **(Kubernetes) "Cluster-as-a-Service"** und **(Kubernetes) "Namespace as a Service"** deklariert
DS_08_A402	Plattform-betreiber	KANN	Ein Plattformbetreiber kann auf Basis von **IaaS-Angeboten** auch komplette Kubernetes Installationen für das Management durch den Kunden ("unmanaged") anbieten. In dieser Konstellation übernimmt der Kunde die weiteren **Obligationen eines Plattformbetreibers, sofern er sein System DVC-konform betreiben will**.
DS_08_A403	Plattform-betreiber	SOLL	Der Plattformbetreiber sollte auf Basis von **PaaS-Angeboten** (Kubernetes) "Cluster-as-a-Service" und/oder (Kubernetes) "Namespace as a Service" **ausschließlich "managed"** anbieten
DS_08_A404	Plattform-betreiber	KANN	Der Plattformbetreiber kann dabei frei entscheiden, dass er einzelne Produktkategorien ((Kubernetes) "Cluster-as-a-Service" und (Kubernetes) "Namespace as a Service") **nicht anbietet**

F - Netzübergänge nach Außen

Disclaimer

Diese Fragestellung wird primär in anderen Detailstandards, z.B. #1, #2, #27, #28, #48 und #49 geregelt. Daher wird diese Passage bewusst kurz gehalten. |

ID	Rolle	Modal-verb	Detailanforderung
DS_08_A501	Plattform-betreiber	MUSS	eine für einen produktiv konsumierbar als DVC Cloud-Service bereitgestellte Kubernetes Umgebung eine den **regulatorischen Vorgaben entsprechende Absicherung der Netzübergänge nach "außen"** sicherstellen
DS_08_A502	Plattform-betreiber	SOLL	sich dabei **anderer Detailstandards der DVC anschließen**, wo dies möglich ist.

G - Netzübergänge innerhalb des Cluster

Disclaimer

Diese Fragestellung wird primär in DS #25 (“Trennung von Verfahren innerhalb eines Clusters”) & DS #26 (“Microsegmentierung für Services”) aufgenommen

ID	Rolle	Modal-verb	Detailanforderung
DS_08_A601	Plattform-betreiber	MUSS	eine für einen produktiv konsumierbar als DVC Cloud-Service bereitgestellte Kubernetes Umgebung eine den **regulatorischen Vorgaben entsprechende Absicherung der Netzübergänge nach “innen”** sicherstellen
DS_08_A602	Plattform-betreiber	SOLL	sich dabei **anderer Detailstandards der DVC** anschließen, wo dies möglich ist.

Referenzdokumente

Dieser Abschnitt führt alle für die Bearbeitung und das Verständnis des Produktes erforderlichen Dokumente an, dies schliesst BSI-Grundschutz-Bausteine als auch Blaupausen mit ein. Die Dokumente sollten hinsichtlich ihrer Verwendung (intern, extern) unterschieden werden. Über die referenzierten Dokumente sind folgende Informationen zu halten: Bezeichnung, Identifikation mit Versionsangabe und Art der Verwendung (z. B. Quelle, weiterführende Literatur, usw.)

Kapitel	Seite	Dokument	Version	Ablageort (Link)
(n/a)	(n/a)	IT-Grundschutz Kompendium	2023	IT-Grundschutzkomependium

Abkürzungsverzeichnis

Abkürzung	Bezeichnung
Web-Zone	Wird im Sinne einer DMZ unter Bereitstellung von Application Level Gateway bzw. Web-Proxy als “Brücke” von Anbindung an externe Netze und Kubernetes Cluster genutzt
Anwendungs-Zone	Wird bezüglich von Kubernetes zur Bereitstellung von sowohl Frontend-Services wie Backend-Services von Anwendungen genutzt
Datenbank-Zone	Wird zur Bereitstellung von Datenbankmanagementsystemen genutzt; diese können (sofern containerisiert) innerhalb von Kubernetes betrieben werden oder sind (im Falle von eigenen Instanzen) über P-A-P Strukturen von Kubernetes Clustern über Schnittstellen anzubinden
P-A-P Struktur	Paketfilter - Application Level Gateway - Paketfilter Ein vom BSI genutztes Modell, um Zonenübergänge geeignet abzusichern