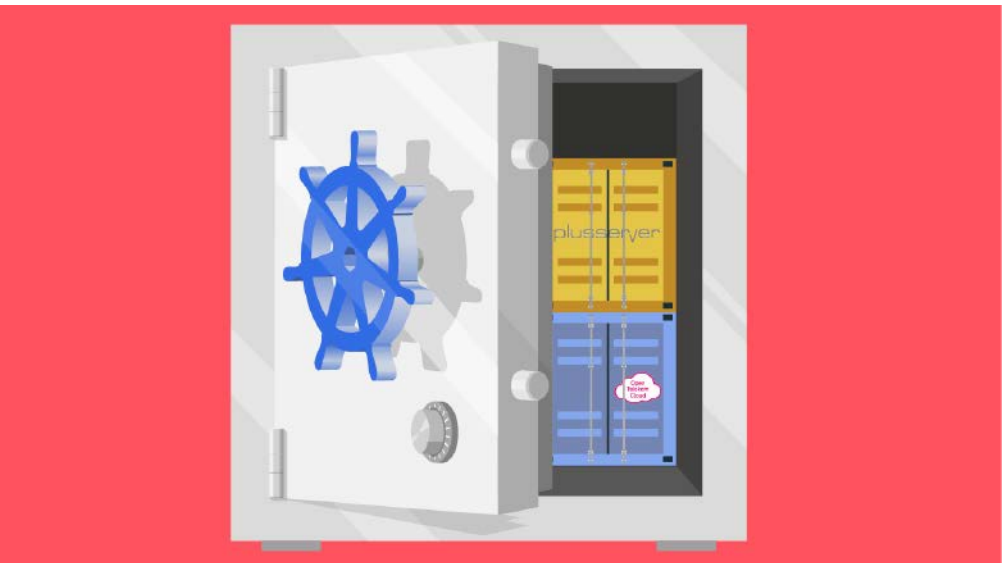


Open Telekom Cloud und PlusServer härten

Auch wenn die Angebote kleinerer Anbieter ein unverfälschteres Kubernetes versprechen als die großen Hyperscaler, sollte man die Umgebungen gründlich absichern. Was bei OTC und PlusServer zu tun ist.

Von Christoph Puppe

Diese Artikelreihe betrachtet die Sicherheit von Kubernetes bei unterschiedlichen Cloud-Anbietern. Nach den bekannten Angeboten von Google, Azure, AWS und IONOS sind diesmal die einheimischen Cloud-Service-Provider (CSP) Open Telekom Cloud (OTC) und PlusServer an der Reihe. Digitale Souveränität, einfachere Datenschutz-Folgenabschätzungen und weniger Risiko von Industriespionage durch die Geheimdienste der Heimatländer der CSP sind für viele Organisationen gewichtige Argumente. Auch preislich sind die kleineren CSP oft attraktiver als die Hyperscaler. Informationen zu den Voraussetzungen liefert der Kasten „Details zur Testumgebung“.

Für Kunden ist der Vergleich der Anbieter der Anfang der Absicherung: Die Entscheidung über einen Managed Service oder eine Distribution ist dabei der erste Schritt. Sobald sie getroffen ist, müssen die Kunden ihren Teil der Verantwortung übernehmen und für eine sichere Konfiguration sorgen. In zwei Tabellen sind die Punkte aufgeführt, die die Anbieter bereits erfüllt haben, die Kunden mit Bordmitteln umsetzen können und für die zusätzliche Software erforderlich ist.

Dieser Artikel konzentriert sich auf die To-do-Liste für OTC und PlusServer. Vergleichbare Informationen zu Google und Azure sowie weitere technische Hintergründe finden sich im dreiteiligen Tutorial zum Absichern von Kubernetes [1, 2, 3]. Details zu AWS und IONOS liefert der Artikel aus der Ausgabe 3/2023 [4]. Mit der Härtung von OpenShift und Rancher wird sich demnächst ein weiterer Artikel befassen.

iX-TRACT

- Sowohl die Open Telekom Cloud als auch PlusServer bieten ihren Kunden weitgehend pures Kubernetes an.
- Im Portfolio der Open Telekom Cloud finden sich einige zusätzliche Dienste, die auch bei der Härtung helfen.
- Um die Absicherung müssen sich Kunden selbst kümmern und dafür einige zusätzliche Werkzeuge einsetzen.

Genutzte Demo-Cluster

Open Telekom Cloud: OTC bietet K8s als Cloud Container Engine (CCE) an. Kunden haben die Wahl zwischen einem normalen und einem „Turbo“-Cluster. Für den Test sollte zunächst letzterer zum Einsatz kommen, der wäre aber mit der K8s-Version 1.19 sehr alt gewesen und das Web-UI erlaubte es nicht, Worker Nodes anzulegen. Zu einem späteren Zeitpunkt funktionierte dies wieder. Der normale Clustertyp, auf dem die Tests erfolgten, nutzt K8s 1.23. Zum Zeitpunkt des Tests war Kubernetes 1.25 aktuell.

Voraussetzung für den Cluster ist ein Virtual-Private-Cloud-Netzwerk (VPC), das vorher einzurichten ist. Enthalten ist ein SNAT-Gateway (Source NAT) für Verbindungen ins Internet. Wer aus dem Cluster das Internet erreichen möchte, muss ein NAT-Gateway im VPC einrichten. Statt einer Cloud-Konsole, also einer Shell auf einem vom Anbieter verwalteten Dienst, ist ein Server zu installieren, der entweder per DNAT (Destination NAT, Port Forwarding) oder mit externer IP aus dem Internet erreichbar ist und Log-ins per hinterlegtem SSH-Schlüssel erlaubt.

Beim Log-in über die Webshell werden der User und das für diesen Server gültige Passwort angezeigt. Unpraktisch an diesem Vorgehen ist, dass ein bereits länger laufender Server seine Passwörter nicht mehr anzeigt. Das ist eher ungewöhnlich, aber ein User kann bei allen Anbietern entweder das Passwort oder den SSH-Schlüssel hinterlegen. Also im Vergleich dazu kein Sicherheitsproblem. Immerhin zeigt diese Webshell auch die Konsolenausgaben beim Booten. Dieser Bastion- oder Jump-Host ist der Arbeitsplatz, um mit dem Hidden Master zu kommunizieren. Der ist zunächst nicht aus dem Internet erreichbar, wer die API öffentlich freigeben will, kann ihm eine externe IP zuordnen.

PlusServer: Der Hoster hat für diesen Artikel einen Account auf dem als plusserver Kubernetes Engine (PSKE) vertriebenen Gardener zur Verfügung gestellt. Gardener ist eine Kubernetes-Management-Distribution der SAP, die als Open Source unter der Apache-2.0-Lizenz steht. Es ist dabei die mandantenfähige Umgebung, die jedem Projekt eine eigenständige Umgebung auf einer geteilten Hardware bereitstellt. Als Infrastruktur

dient in der PSKE die pluscloud open selbst, aber auch AWS ist verfügbar.

Es steht die zum Zeitpunkt des Artikels aktuelle Kubernetes-Version 1.25 zur Verfügung, Version 1.22 ist aber ebenfalls möglich. Als Netzwerk stehen Cilium und Calico zur Wahl. Für den Demo-Cluster kommt die Standardeinstellung Cilium zum Zug. Noch mehr Auswahl bietet der optionale DNS-Provider: Hier sind AWS Route53, Azure- und GCP-DNS sowie OpenStack Designate möglich. Für den Test blieb diese Option aber ungenutzt. Die Nodes erstellt man in der gleichen Maske und hat die Wahl zwischen einigen Maschinentypen und auch Autoscaling ist einstellbar. Das Betriebssystem ist dabei immer Ubuntu 22.4. Als CPU gibt es nur AMD. Auch gibt es nur eine Verfügbarkeitszone. Als Container Runtime Interface sind containerd und dockerd verfügbar.

Schon beim Erstellen des Clusters wird das Wartungsfenster definiert, in dem die automatischen Updates für Be-

Details zur Testumgebung

Jeder Anbieter nimmt mit einem Demo-Cluster an der Auswertung teil. Diese sind soweit möglich gleich aufgebaut. Die Installation folgt dabei den Empfehlungen des Anbieters, die in den Anleitungen zu finden sind. Die Cluster sind für den Test aus dem Internet erreichbar und auch der Master ist öffentlich zugänglich, was in einer Produktionsumgebung natürlich tunlichst zu vermeiden ist. Wo es möglich ist, sind die Master-Server als Hidden Master konfiguriert. Dabei ist der Server zwar sichtbar, aber der CSP verwaltet diesen vollständig und der Kunde hat keinen Zugriff auf den Server, auf dem der K8s-API-Server läuft. Viele Sicherheitstests nach dem CIS-Benchmark sind damit nicht möglich.

Dieser Artikel betrachtet die Sicherheit der CSP und listet auf, was Kunden bei diesen Anbietern selbst tun müssen, um eine ausreichende Sicherheit für die Container zu erreichen. Auch wenn die im Artikel „Kubernetes mit Capabilities, SECCOMP und SELinux“ [5] aufgeführten allgemeinen Schritte weiterhin gleich sind, unterscheidet sich die Umsetzung bei den Plattformen erheblich. Die kleineren Anbieter wie IONOS bieten im Vergleich zu den großen Hyperscalern wie AWS ein unverfälschtes Kubernetes. Es ist weniger verändert, die Images kommen eher von den Herstellern der Werkzeuge statt aus der Registry des CSP. Besonders merkbar ist der Unterschied bei der Zahl der zusätzlich verfügbaren Dienste, was sich auch auf die Absicherung auswirkt. Wo Kunden bei AWS, Azure und GCP etwa die Protokollierung als SaaS direkt in der Cloud bekommen, müssen sie sie bei den kleineren CSP mit einigem Aufwand selbst implementieren.

Empfehlungen zum BSI-IT-Grundschutz-Baustein SYS.1.6 Containerisierung

Anforderung[1]	Open Telekom Cloud[2]	PlusServer[2]
SYS.1.1.A16 Sichere Grundkonfiguration von Servern (S)	Es stehen sehr viele Images zur Verfügung. Das für den Artikel verwendete Image hätte besser gehärtet sein können. Keine Schwachstellen in der Software.	Im Ubuntu-22.4-Image fand der Scanner einige Verwundbarkeiten. Für viele gibt es bereits Updates.
OPS.1.1.2.A18 Durchgängige Protokollierung administrativer Tätigkeiten (H)	Es gibt keine voreingestellte Protokollierung aller Tätigkeiten. Diese ist über den Cloud Trace Service möglich. Administratoren können die Daten allerdings auch löschen.	Es gibt keine voreingestellte Protokollierung aller Tätigkeiten.
OPS.1.1.3.A1 Konzept für das Patch- und Änderungsmanagement [Fachverantwortliche] (B)	Cluster können auf neue K8s-Versionen umgezogen werden. Das Update umfasst dann auch Nodes. Dies ist in der Praxis teilweise schwierig, weshalb sich oft ein Neuaufbau empfiehlt. Automatische Updates mit OSMT-Agent sind nicht möglich.	Tägliche Updates sind voreingestellt.
SYS.1.6.A5 Separierung der Administrations- und Zugangsnetze bei Containern (B)	Die Trennung erfolgt in den VPC, die der Anwender vor dem Start eines Clusters anlegt. Im Test verweigerte das Web-UI das Anlegen weiterer Subnetze mit einer irreführenden Fehlermeldung. Die Netzwerkinterfaces der Nodes sind in Security Groups mit Firewallregeln unterteilt und realisieren so die Netztrennung.	Bei der Installation legt Gardener die Netze für die Pods fest. Network Policies sind nicht vorgegeben. Diese muss der Nutzer selbst anlegen.
SYS.1.6.A6 Verwendung sicherer Images (B)	Die optional einzustellende Registry ist sehr einfach. Für Funktionen wie Scans der Images nach Verwundbarkeiten oder Regeln ist zusätzliche Software nötig.	Es wird keine Registry bereitgestellt. Daher muss der Kunde eine eigene nutzen und dort auch eine Software zum Scan der Images implementieren.[3]
SYS.1.6.A7 Persistenz von Protokollierungsdaten der Container (B)	Nutzer können dies über den Dienst Log Tank Service aktivieren.	Kunden müssen die Logs im Cluster selbst sammeln und eventuell ausleiten.
SYS.1.6.A8 Sichere Speicherung von Zugangsdaten bei Containern (B)	Dies ist über den K8s Secret Service möglich. Es steht auch ein Key-Management-Dienst zur Verfügung.	Es steht ein Secrets Management zur Verfügung.
SYS.1.6.A10 Richtlinie für Images und Container-Betrieb (S)	Nutzer müssen hier selbst Hand anlegen und eine Software installieren.	Nutzer müssen hier selbst Hand anlegen und eine Software installieren.
SYS.1.6.A18 Accounts der Anwendungsdienste (S)	Die Anwendungsdienste selbst sind nur in K8s zu verwalten.	Die Anwendungsdienste selbst sind nur in K8s zu verwalten.
SYS.1.6.A21 Erweiterte Sicherheitsrichtlinien (H)	Nutzer müssen hier selbst Hand anlegen und eine Software installieren.	Nutzer müssen hier selbst Hand anlegen und eine Software installieren.[3]
SYS.1.6.A22 Vorsorge für Untersuchungen (H)	Nutzer müssen hier selbst Hand anlegen und eine Software installieren.	Nutzer müssen hier selbst Hand anlegen und eine Software installieren.
SYS.1.6.A24 Hostbasierte Angriffserkennung (H)	Nutzer müssen hier selbst Hand anlegen und eine Software installieren.	Nutzer müssen hier selbst Hand anlegen und eine Software installieren.[3]
SYS.1.6.A25 Hochverfügbarkeit von containerisierten Anwendungen (H)	Es gibt drei Rechenzentren, Nodes dürfen aber nur im selben RZ wie der Managementdienst laufen.	Im Test stand nur eine Zone zur Verfügung.

[1](B) Basisanforderung, (H) Anforderung bei erhöhtem Schutzbedarf, (S) Standardanforderung. [2] Erläuterung der Farben siehe Text. [3] Ein entsprechendes Angebot ist in Vorbereitung, siehe Text.

triebssysteme und K8S erfolgen. Ungewöhnlich ist die Option, einen täglichen Schlafrhythmus einzustellen. Für Cluster, die nur tagsüber – beispielsweise für Entwicklung – im Einsatz sind, eine gute Option, Strom und Geld zu sparen. Einstellungen für VPC oder Netze insgesamt erfolgen automatisch und die Konfiguration des Clusters steht in Sekunden zur Verfügung. Innerhalb eines Projekts in Gardener können mehrere Cluster existieren und es gibt eine gemeinsame Verwaltung der Nutzenden und der Secrets.

Nach eigenen Angaben arbeitet PlusServer an einer Erweiterung des Funktionsangebots. Das soll die Überwachung von Images und Containern (Schwachstellen), Runtime Protection (XDR, File-Überwachung et cetera), Scans von Quellcode und Infrastructure as Code (DevSecOps und IAC), Compliance und Auditing der Konfiguration, Platform Protection (beispielsweise für AWS) sowie SOC-Integration bieten.

Hintergrundinformationen zur Härtungsliste

Die beiden Tabellen „Empfehlungen zum BSI-IT-Grundschutz-Baustein SYS.1.6 Containerisierung“ und „Empfehlungen zum BSI-IT-Grundschutz-Baustein APP.4.4 Kubernetes“ enthalten nur die Anforderungen, die technisch auf dem Cluster umzusetzen sind. Die organisatorischen Anforderungen wie Regelungen für den Betrieb von Containern, Freigaben oder Aktualisierungen liegen in der Verantwortung der Kunden. Auch bleiben hier die Anforderungen unberücksichtigt, die den eigentlichen Betrieb des Servers betreffen.

Da bei den Managed-Kubernetes-Angeboten der Cloud-Service-Provider für den Betrieb in der Pflicht ist, ist von den Anforderungen der Bausteine „SYS.1.1 Allgemeiner Server“ und „SYS.1.3 Server unter Linux“ nur „SYS.1.1.A16 Sichere Grundkonfiguration von Servern (S)“ relevant. Mit aufgeführt sind drei übergeordnete Anforderungen, die das BSI im Zuge der Modularisierung des IT-Grundschutz-Kompendiums aus den SYS-Bausteinen in die oberen Schichten verlagert hat. Die Kommentare zur Umsetzung sind farblich hervorgehoben. Die Anforderungen werden wie folgt nach der Art der Umsetzung kategorisiert:

- Grün: Die Standardinstallation über die Weboberfläche reicht aus. Es ist keine weitere Konfiguration erforderlich. Wer eine andere Methode zum Erstellen des Clusters nutzt, muss auch die grün markierten Anforderungen explizit aktivieren.
- Rot: Nutzer können und sollten die Anforderungen mit den Bordmitteln umsetzen, die notwendige Konfiguration ist jedoch bei der Standardinstallation über die Weboberfläche nicht voreingestellt.
- Gelb: Es ist zusätzliche Software erforderlich.
- Blau: Die Umsetzung ist nicht möglich.

Informationen, für welche Anforderungen die Umsetzung empfohlen ist, finden sich im zugehörigen Kommentar.

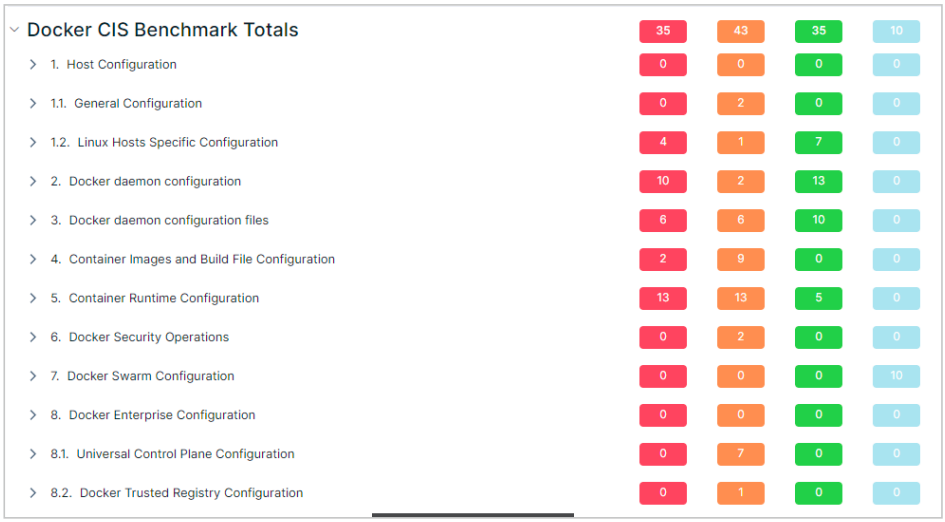
Verwundbarkeiten im Cluster

Wie im zweiten Teil des Kubernetes-Tutorials [2] beschrieben, wird jeder der CSP auch auf die Sicherheit der Cluster untersucht. Da die CIS-Benchmarks mangels Rechten auf den Master-Servern ausfallen, beschränkt sich die Untersuchung auf den Stand der Images. Trivy, der Image Scanner für Verwundbarkeiten und fehlende Patches von AquaSec, hat auf dem Demo-Cluster die Images auf den Nodes untersucht. AquaSec Enforcer dient dazu, die Images auf den Nodes zu erreichen.

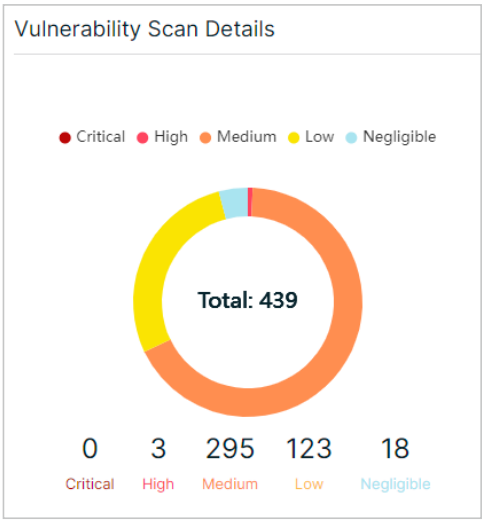
Empfehlungen zum BSI-IT-Grundschutz-Baustein APP.4.4 Kubernetes

Anforderung[1]	Open Telekom Cloud[2]	PlusServer[2]
APP.4.4.A1 Planung der Separierung der Anwendungen (B)	Die geplanten Netzzonen und die Separierung in Namespaces und Cluster sind umzusetzen.	Die geplanten Netzzonen und die Separierung in Namespaces und Cluster sind umzusetzen.
APP.4.4.A3 Identitäts- und Berechtigungsmanagement bei Kubernetes (B)	Das eingebaute IAM erlaubt die Zuteilung von Berechtigungen auf Cluster und Namespaces.	Das IAM im Gardener erlaubt die Verwaltung von Identitäten und Berechtigungen auf das Projekt, also alle Cluster im Projekt.
APP.4.4.A4 Separierung von Pods (B)	per Default umgesetzt	per Default umgesetzt
APP.4.4.A5 Datensicherung im Cluster (B)	Es gibt einen Backup-Service für Buckets und Images. Auch kann der Nutzer Snapshots von PVCs der Namespaces erstellen.	Es steht kein Backup-Dienst zur Verfügung.
APP.4.4.A7 Separierung der Netze bei Kubernetes (S)	siehe SYS.1.6.A5	siehe SYS.1.6.A5 Einschränkend ist hier, dass die Hidden Master immer aus dem Internet erreichbar sind. Eine Konfiguration, bei der der K8s-API-Server nur intern erreichbar ist, war nicht möglich.
APP.4.4.A9 Nutzung von Kubernetes Service-Accounts (S)	Alle nicht ins OTC-IAM integrierten K8s-Standardfunktionen stehen zur Verfügung.	Die Berechtigungsvergabe funktioniert nur über die RBAC-Funktionen von K8s.
APP.4.4.A12 Absicherung der Infrastruktur-Anwendungen (S)	Die einzige hier relevante Anwendung ist der in das OTC-IAM eingebundene Image-Dienst.	Es gibt keine weiteren Infrastrukturanwendungen im Angebot. Diese sind anderweitig bereitzustellen und abzusichern.
APP.4.4.A13 Automatisierte Auditierung der Konfiguration (H)	Nutzer müssen hier selbst Hand anlegen und eine Software installieren.	Nutzer müssen hier selbst Hand anlegen und eine Software installieren.[3]
APP.4.4.A14 Verwendung dedizierter Nodes (H)	Management Nodes sind separat und in der Verwaltung durch OTC, daher gibt es für Nutzer keine Shell-Zugriffe. Nodes für Speicher sind nicht notwendig. Die Aufgabe der Bastion Nodes übernehmen die Loadbalancer.	Management Nodes sind separat und in der Verwaltung durch PlusServer, daher gibt es für Nutzer keine Shell-Zugriffe. Nodes für Speicher sind nicht notwendig. Die Aufgabe der Bastion Nodes übernehmen die Loadbalancer.
APP.4.4.A16 Verwendung von Operatoren (H)	möglich, aber kein Standard	möglich, aber kein Standard
APP.4.4.A17 Attestierung von Nodes (H)	Wird nicht angeboten.	Wird nicht angeboten.
APP.4.4.A18 Verwendung von Mikro-Segmentierung (H)	Nutzer müssen hier selbst Hand anlegen und eine Software installieren.	Nutzer müssen hier selbst Hand anlegen und eine Software installieren.
APP.4.4.A19 Hochverfügbarkeit von Kubernetes (H)	siehe SYS.1.6.A25	siehe SYS.1.6.A25
APP.4.4.A20 Verschlüsselte Datenhaltung bei Pods (H)	Verschlüsselung der Speicher ist optional möglich.	Die Backend-Systeme sind at-rest-verschlüsselt; jedoch mit Schlüsseln des CSP. Eigene Schlüssel sind nicht möglich.

[1] (B) Basisanforderung, (H) Anforderung bei erhöhtem Schutzbedarf, (S) Standardanforderung. [2] Erläuterung der Farben siehe Text. [3] Ein entsprechendes Angebot ist in Vorbereitung, siehe Text.



Der Scan der OTC-Docker-Engine auf dem Worker Node gemäß den Empfehlungen des CIS-Benchmarks ergab einen nicht ausreichend sicher konfigurierten Server, bei dem einige Verbesserungen möglich sind (Abb. 1).



Auf den Worker Nodes bei PlusServer fand der Scanner einige Verwundbarkeiten (Abb. 2).

Bei PlusServer fand der Scanner auf den Worker Nodes doch einige Schwachstellen. Von den 439 Verwundbarkeiten gibt es für 30 ein Update. Hier verwundert es, dass eigentlich Autoupdate möglich ist, aber eine neue Installation mit derart vielen, auch schweren Verwundbarkeiten ausgeliefert wird. Auch nach einem nächtlichen Update hat sich die Zahl nicht geändert.

Hier schneidet das Angebot der OTC im Vergleich sehr gut ab. Dies liegt daran, dass der Anbieter auf den Nodes nur relativ wenige Images bereitstellt, die allerdings in einem guten Zustand waren: Sie waren aktuell und enthielten wenige Verwundbarkeiten. Beim Scan der Images der Nodes bei PlusServer sieht es nicht ganz so gut aus. In den siebzehn auf den Servern gefundenen Images gab es doch einige als kritisch oder hoch bewertete Schwachstellen.

Die Tabelle mit den von Trivy (der Open-Source-Version von AquaSec) ge-

Von Trivy gefundene Verwundbarkeiten

	Critical	High	Medium	Low	Summe
OTC	2	109	52	10	173
PlusServer	21	47	57	7	132
AWS[1]	2070	3901	2490	270	8731
IONOS[1]	25	124	55	6	210
Azure[1]	240	1111	630	85	2066
GCP[1]	2	44	14	1	61

[1]zum Vergleich die bisherigen Ergebnisse anderer Plattformen [4]

Verwundbarkeiten gemäß AquaSec-eigener Bewertung

	Critical	High	Medium	Low	Summe
OTC	2	109	52	10	173
PlusServer	19	27	32	11	89
AWS	270	2041	5430	990	8731
IONOS	25	126	54	6	211
Azure	182	764	632	290	1868
GCP	1	41	9	0	51

fundenen Verwundbarkeiten führt alle Ergebnisse der Scans aus allen Artikeln dieser Reihe zusammen und enthält auch die Daten für Plattformen, die dieser Teil nicht bespricht. Somit ist eine Vergleichbarkeit zwischen allen Anbietern in dieser Artikelreihe gegeben.

Diese Tabelle entstand nach den Einstufungen des CVSS v3 Severity der NVD (National Vulnerability Database), die als offizieller Standard für Verwundbarkeiten gelten. Dieser abschließende Artikel der Serie, die die Managed-Kubernetes-Angebote vergleicht und die notwendigen Maßnahmen zur Absicherung aufzeigt, enthält deshalb auch die zweite Tabelle mit den Einstufungen des Scan-Produkts, das für die gesamte Serie im Einsatz war. Diese sind oft realistischer und mehr daran orientiert, ob sich die Schwachstellen praktisch ausnutzen lassen.

Die Unterschiede zwischen den Anbietern sind weiterhin frappierend. Die Bewertung der Verwundbarkeiten durch AquaSec ist überall niedriger als bei der NVD. Besonders die kritischen Schwachstellen bei AWS sind von über 2000 auf 270 reduziert und auch die als „High“ bewerteten sinken auf die Hälfte. Daher ist der Abstand zu GCP nicht mehr das Tausendfache, sondern nur noch das 270-Fache.

Interessant ist in diesem Zusammenhang auch die gesamte Zahl der Images auf allen Nodes und wie viele Verwundbarkeiten diese im Schnitt enthalten. Man sieht dabei gut, wie hoch der Aufwand ist, Kubernetes wirklich in die eigenen Mehrwertdienste zu integrieren. Das bringt für Nutzende viele Vorteile, benötigt aber auch viel Software und damit Images, die der Anbieter dann pflegen muss. Wenn Nutzende diese Dienste nachträglich installieren, sind sie dann natürlich selbst in der Verantwortung.

Ein Ausreißer ist dabei GCP: Die Integration von Kubernetes in die restlichen Dienste und insbesondere die Verwaltung der Identitäten steht AWS und Azure in nichts nach, aber die Zahl der dafür notwendigen Images auf den Worker Nodes ist erheblich kleiner. Auch haben diese Images die wenigsten Verwundbarkeiten.

Fazit

PlusServer bietet mit seinem auf OpenStack und Gardener aufbauenden Managed K8s ein fast pures Kubernetes mit Hidden Master. Es gibt wenig Integration in andere Dienste, was für kleinere CSP typisch ist. Die Nutzung ist auch ohne große Spezialkenntnisse möglich, aber für die Absicherung sollten Nutzende sich gut mit K8s auskennen, da hier doch einiges zu tun ist.

Bei der Open Telekom Cloud sieht es ähnlich aus. Nur sind bereits mehr Dienste vorhanden, Nutzende haben also weniger Arbeit bis zu einem produktiv einsetzbaren und gut abgesicherten Cluster. Etwas mehr Arbeit wartet allerdings bei der Einrichtung. Hier bietet OTC sehr viel mehr Optionen und Flexibilität als PlusServer und somit ist auch mehr Wissen und mehr Aufwand bei der Einrichtung der Cluster notwendig. Die Cluster lassen sich dann aber auch gut in die weiteren bei der OTC genutzten Dienste integrieren.

Die großen Hyperscaler bieten einiges für das teilweise deutlich teurere Angebot. Wer möglichst wenig selbst machen möchte, kann dort mit wenigen Schritten K8s-Cluster betreiben und mit teilweise einigem zusätzlichen Aufwand auch absichern. OTC und PlusServer haben gute Angebote. Der Unterschied bei den im Preis enthaltenen und den zusätzlich buchbaren Diensten sowie der Absicherung ab Werk ist erheblich. Wer diese Angebote wahrnehmen möchte, sollte den zusätzlichen Aufwand für die Absicherung auf sich nehmen. (avr@ix.de)

Images auf den Worker Nodes

Anbieter	Anzahl Host-Images	Ø Verwundbarkeiten pro Image
OTC	5	35
PlusServer	11	12
AWS	271	32
IONOS	8	26
Azure	86	24
GCP	15	4

Quellen

[1] Christoph Puppe; Tutorial: Kubernetes absichern, Episode 1; iX 12/2022, S. 54

[2] Christoph Puppe; Kubernetes-Tutorial, Teil 2: IAM erklärt, AKS und GKE härten; iX 1/2023, S. 126

[3] Christoph Puppe; Tutorial: Admission Controller überwachen K8s-API, Episode 3; iX 2/2023, S. 132

[4] Christoph Puppe; Kubernetes-Sicherheit: Kubernetes von AWS und IONOS härten; iX 3/2023, S. 100

[5] Christoph Puppe, Jan Walther; Kubernetes mit Capabilities, SECCOMP und SELinux; iX 12/2022, S. 60

CHRISTOPH PUPPE

ist Managing IT Security Architect und Auditteamleiter für ISO 27001 nach Grundschutz bei SVA System Vertrieb Alexander GmbH, Mitautor des Grundschutz-Kompendiums und ehemaliger Penetrationstester.