OpenShift und Rancher nach BSI härten

Im letzten Teil der Artikelreihe zur Kubernetes-Absicherung gemäß den Anforderungen des BSI IT-Grundschutzes treten zwei Distributionen an. Was können OpenShift und Rancher in puncto Sicherheit und was lässt sich wie nachrüsten?

Von Christoph Puppe

Mit OpenShift und Rancher sind in diesem letzten Teil der Artikelreihe zu Kubernetes-Sicherheit zwei Distributionen an der Reihe. Er beleuchtet die eingebaute und nachrüstbare Sicherheit der Pakete von Red Hat und SUSE. Azure, AWS, Google, IONOS, Open Telekom Cloud und PlusServer standen im Rahmen der Serie zum Absichern von Kubernetes sowohl bei Cloud-Anbietern als auch on Premises bereits im Fokus.

Auch die Distributionen werden dabei möglichst vergleichbar mit den Managed-Kubernetes-Angeboten betrachtet. Die Artikelserie will Lesern den Vergleich der Anbieter erleichtern, denn der erste Schritt zur Absicherung ist die Entscheidung über einen Managed Service oder eine Distribution. Sobald sie getroffen ist, müssen die Administratoren ihren Teil der Verantwortung übernehmen und für eine sichere Konfiguration sorgen. Zwei Tabellen führen für die Grundschutz-Bausteine Containerisierung und Kubernetes die Punkte auf, die bereits erfüllt sind, die Admins mit Bordmitteln umsetzen können und für die zusätzliche Software erforderlich ist.

Demo-Cluster für OpenShift

Für den Aufbau des OpenShift-Demo-Clusters dienten die offiziellen Anleitungen. In der Google-Cloud setzte der Autor dabei statt auf GKE auf IaaS. Der über die Cloud-Shell ausgeführte Installer legt mit einem entsprechend berechtigten Serviceaccount per Terraform alle zugehörigen Ressourcen an. Die Installation der zum Zeitpunkt der Entstehung des Artikels aktuellen Version 4.12.13 hatte kleine Bugs, war aber innerhalb von zwei Stunden mit allem Drum und Dran erledigt. Zum Einsatz kommt Kubernetes 1.25 mit 35 Operatoren, die sich um den Betrieb aller wichtigen Teile kümmern. Hier hat Red Hat Großartiges geleistet. Die Operatoren übernehmen zum großen Teil die Aufgaben, die man in den Managed-Kubernetes-Angeboten beim CSP verorten würde. Wäre der Cluster ein Linux, wären sie die von systemd verwalteten Basisdienste.

Auch die Sicherheit ist durch Operatoren bereits gut vorkonfiguriert. Seit OpenShift 4.11 sind die Pod Security Policies nicht mehr unterstützt. Dafür gibt es jetzt Security Context Constraints (SCCs), die einen Operator in jedem Namespace erzwingen, Standard ist `restricted`. Elf SCC gibt es und neue lassen sich einfach erstellen.

Allerdings funktioniert das Löschen von Constraint-Labels eines Namespace nicht, da sie ein Operator sofort wieder setzt. Es muss auch das Label `security.openshift.io/scc.podSecurityLabelSync=false` gesetzt sein. Privilegierte Container sind dann in diesem Namespace möglich, sofern der `ServiceAccount` die Berechtigung dafür hat. Diese setzt der Befehl:

```
oc adm policy add-scc-to-user ↵
   privileged system:serviceaccount:↵
                          aqua:aqua-sa
```

hier für den `ServiceAccount` für das Daemon-Set des AquaSec Enforcers. Der benötigt diese Berechtigungen, um alle Container und auch den Node zu untersuchen.

Leider fehlen in der Defaultinstallation die für die Absicherung erforderlichen Operatoren. Alle drei sind über den Operator Hub nachzurüsten. Der Compliance Operator scannt mit OpenSCAP die Nodes, die CIS-Benchmarks führt wiederum OpenShift direkt durch. Die Ergebnisse der Scans sind allerdings nicht in die Webkonsole eingebunden und etwas umständlich abzurufen – da ist sicherlich noch Luft nach oben. Der File Integrity

iX-TRACT

- OpenShift bietet mehr Integration von benötigten Diensten als manches Managed Kubernetes der kleineren Anbieter.
- Rancher liefert eine ausgereifte Kubernetes-Distribution und einen Multi-Cluster-Manager, der ein sehr originales Kubernetes installiert.
- Wer alles aus einer Hand will, dürfte eher OpenShift bevorzugen – wer lieber mehr Freiheit bei Installation und Betrieb bevorzugt, eher bei Rancher landen.

Details zur Testumgebung

Jede Distribution nimmt mit einem Demo-Cluster an der Auswertung teil. Die Cluster sind soweit möglich gleich aufgebaut. Die Installation folgt dabei den Empfehlungen aus den Anleitungen der Anbieter. Die Cluster und auch die Control Plane Nodes sind für den Test aus dem Internet erreichbar, was in einer Produktionsumgebung natürlich tunlichst zu vermeiden ist. Bei den Distributionen ist es nicht möglich, die Control-Plane-Server als Hidden Master zu konfigurieren, die Verantwortung für diese liegt auch hier beim Kunden.

Dieser Teil der Serie betrachtet nicht nur die Sicherheit der Standardinstallation der Kubernetes-Distributionen, sondern bewertet auch die vom Hersteller bereitgestellten Container-Images. Ferner listet er auf, was Kunden bei diesen Distributionen selbst tun müssen, um eine ausreichende Sicherheit für die Container zu erreichen. Auch wenn die im Artikel „Kubernetes mit Capabilities, SECCOMP und SELinux“ [1] aufgeführten allgemeinen Schritte weiterhin gleich sind, unterscheidet sich deren Umsetzung bei den Distributionen doch erheblich. Wie bei den Cloud-Service-Providern (CSP) sind auch bei den Distributionen unterschiedlich viele Dienste bereits in der Installation enthalten.

Der größte Unterschied in diesem Teil der Serie liegt darin, dass Kunden im Vergleich zu den Managed-Kubernetes-Angeboten selbst für die Control Plane zuständig sind. Es gibt kein „nicht möglich“. Im eigenen Cluster kann der Kunde alles installieren, was notwendig oder gewünscht ist – wenn auch mit unterschiedlichem Aufwand.

Operator führt ein Advanced Intrusion Detection Environment (AIDE) auf allen Nodes aus. Es vergleicht die Prüfsummen aller Dateien gegen eine lokale Datenbank und berichtet Veränderungen. Unter Linux hat sich AIDE nie so richtig durchgesetzt, da es leicht zu umgehen ist, denn die Datenbank liegt auf dem Node selbst und die Zahl der fehlerhaften Meldungen (False Positives) ist oft sehr hoch. Von daher ist es nachvollziehbar, dass dies nicht Default ist. Der letzte sicherheitsrelevante Kandidat ist der Security Profiles Operator. Er lernt selbst SECCOMP- und SELinux-Profile und wendet sie auf laufende Container an. Seit Februar 2023 ist er allgemein verfügbar und ergänzt eine Absicherung zur Laufzeit gut.

Weder die Constraints noch die drei weiteren Sicherheitsoperatoren sind allerdings ein Ersatz für eine ausgereifte Cloud Workload Protection Platform (CWPP). Es fehlen viele Richtlinien für Image Assurance, die bei allen CWPPs Standard sind. Auch die Überwachung der Container zur Laufzeit besteht bei den CWPPs aus mehr als nur SECCOMP und SELinux.

Testumgebung für Rancher

Das seit Dezember 2020 SUSE gehörende Rancher ist eine Software zur Verwaltung mehrerer Kubernetes-Cluster, aber die Firma hat auch drei eigene K8s-Distributionen. K3s eignet sich für kleine Umgebungen wie das IoT-Segment. Die Rancher Kubernetes Engine (RKE) deckt größere Einsatzbereiche ab. Hinzu kommt die relativ neue Variante RKE2, die für besonders sicherheitsbewusste Kunden gedacht ist. Wer weitere Cluster verwalten will, kann entweder existierende anbinden, einen neuen Managed-K8s-Cluster von AWS, GCP oder Azure aufsetzen oder einen neuen RKE- oder RKE2-Cluster bei einem IaaS-Anbieter erstellen.

Für diesen Test wurde mit der Quick-Start-Anleitung Rancher mit einem Beispielcluster aufgesetzt. Wer Terraform ausführt, erhält nach wenigen Minuten zwei Cluster: Local, ein K3s für die Multi-Cluster-Verwaltung, und einen weiteren, auf dem der von Rancher verwaltete RKE2 läuft. Um sicherzugehen, dass der Artikel einen möglichst realistischen Cluster betrachtet, sollte ein zusätzlicher Cluster (Rancher-Test) in Azure aufgesetzt werden, was auf Anhieb nicht funktionierte. Die Scans der Images erfolgten daher in den beiden QuickStart-Clustern. Leider nutzen sie noch Kubernetes 1.24 und nicht 1.25, also sind hier auch noch Pod Security Policies enthalten, auch wenn bereits das Template Pod Se-

Ein neuer Namespace – in der Red-Hat-Sprache ein Projekt – hat per Default eine Reihe von Constraints als Labels (Abb. 1).

curity Admission „Rancher-Restricted“ ausgewählt ist. Neue Projekte sind allerdings nicht per Default mit einem der Templates ausgestattet, dies ist jeweils in den Einstellungen vorzunehmen. Ein Update der Kubernetes-Version ist in der Oberfläche „Edit Cluster“ versteckt und nach der Auswahl der aktuellen Version 1.25 startet es sofort. Der Vorgang ist nach zwei Minuten abgeschlossen, ohne die laufenden Workloads zu stören.

Bei der Installation eines Clusters in Azure verwunderte etwas, dass per Default noch ein altes Ubuntu 18.04 LTS ausgewählt ist, das kurz vor dem Supportende steht – aktuell ist Version 22.04 LTS. Nach Anpassung der Zahl der Nodes und des Node-Typs wurden alle Einstellungen auf den vorgeschlagenen Werten belassen. Die Liste der Einstellungen lässt keine Wünsche offen. Von etcd-Backups, Vorgaben für Pod Security Admissions, Network Namespace Separation, Updates bis zu editierbaren YAML-Dateien etwa für den CNI ist die Maske schon ein guter Start für die Härtung.

Etwas unpraktisch ist die fehlende Persistenz der Cloud-Shell. Die CLI im Web-UI speichert zwischen zwei Sessions weder History noch Dateien. Zwischendurch musste die VM mit dem RKE2-Cluster für eine Anpassung der Größe der Festplatte booten, was Rancher allerdings in keiner Weise störte.

Im Standard ist NeuVector nicht mit installiert. Dies kann über die Cluster-Tools erfolgen, die auch CIS-Benchmarks, Logging, OPA und ISTIO bereitstellen. Eine Installation von NeuVector scheiterte leider. Immerhin wurde der Dienst ins Web-UI zumindest als Link eingebunden und der Scan der Images war möglich: nur Verwundbarkeiten ohne Exploits, wenn auch drei kritische dabei sind.

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 ausschließlich 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.

Wie auch bei den Managed-Kubernetes-Angeboten sind für diesen Artikel 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:

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

Anforderung[1]	OpenShift 4[2]	Rancher/RKE2[2]
SYS.1.1.A16 Sichere Grundkonfiguration von Servern (S)	Die Images für die Nodes sind gehärtet. Allerdings einige vermeidbare Verwundbarkeiten. CIS-Benchmark bringt 9 Abweichungen. Keine davon muss behoben werden.	Die Nodes sind standardmäßig Ubuntu 18.04 LTS, hier sollte ein gehärtetes Image zum Einsatz kommen. CIS-Benchmark bringt 5 Abweichungen, die zu beachten sind.
OPS.1.1.2.A18 Durchgängige Protokollierung administrativer Tätigkeiten (H)	Protokollierung ist eingeschaltet, lässt sich aber ausschalten. Weiterleiten der Logs an einen externen Speicher ist dringend empfohlen.	Protokollierung ist eingeschaltet, lässt sich aber ausschalten. Weiterleiten der Logs an einen externen Speicher ist dringend empfohlen.
OPS.1.1.3.A1 Konzept für das Patch- und Änderungsmanagement [Fachverantwortliche] (B)	OpenShift selbst und auch alles, was als Operator installiert ist, kann auf Knopfdruck aktualisiert werden.	Updates sind vorbereitet, aber manuell auszuführen.
SYS.1.6.A5 Separierung der Administrations- und Zugangsnetze bei Containern (B)	Hier hat OpenShift große Mängel, da die Admin-Webkonsole über den gleichen Loadbalancer freigegeben ist wie die Anwendungen. Dies zu separieren ist sehr aufwendig. Daher blau markiert.	Bei der Installation legt Rancher die Netze für Pods fest. Network Policies sind keine vorgegeben. Diese muss der Kunde selbst anlegen.
SYS.1.6.A6 Verwendung sicherer Images (B)	Scan der Images in einer Registry kann mit dem Quay Container Security Operator im Cluster sichtbar werden. Dieser ist, wie auch der Image-Scanner in der Registry, nachträglich zu installieren. Die Images von OpenShift selbst enthalten allerdings viele Verwundbarkeiten. Dies können Nutzende nicht beheben.	Es wird keine Registry bereitgestellt. Daher muss der Kunde eine eigene nutzen und dort auch eine Software zum Scan der Images implementieren.
SYS.1.6.A7 Persistenz von Protokollierungsdaten der Container (B)	Protokollierung ist eingeschaltet, lässt sich aber ausschalten. Weiterleiten der Logs an einen externen Speicher ist dringend empfohlen.	Protokollierung ist eingeschaltet, lässt sich aber ausschalten. Weiterleiten der Logs an einen externen Speicher ist dringend empfohlen.
SYS.1.6.A8 Sichere Speicherung von Zugangsdaten bei Containern (B)	Das Secrets Management von Kubernetes ist nutzbar und der etcd kann verschlüsselt werden. Empfohlen ist hier, eine externe Verwaltung der Secrets über Clustergrenzen hinweg zu integrieren.	Das Secrets Management von Kubernetes ist nutzbar und auch verschlüsselt. Empfohlen ist hier, eine externe Verwaltung der Secrets über Clustergrenzen hinweg zu integrieren.
SYS.1.6.A10 Richtlinie für Images und Container-Betrieb (S)	Ist mit dem SCC vorinstalliert und in einem sicheren Default konfiguriert.	Pod Security Admission ist vorbereitet, aber vom Nutzer zu aktivieren.
SYS.1.6.A18 Accounts der Anwendungsdienste (S)	Die Anwendungsdienste selbst sind vom Kunden in K8s zu verwalten.	Die Anwendungsdienste selbst sind vom Kunden in K8s zu verwalten.
SYS.1.6.A21 Erweiterte Sicherheitsrichtlinien (H)	Der Security Profiles Operator erfüllt diese Anforderung und sollte daher zum Einsatz kommen, sofern keine CWPP vorhanden ist.	Mit NeuVector ist hier eine gute Lösung im Lieferumfang, aber dies ist nachträglich zu installieren.
SYS.1.6.A22 Vorsorge für Untersuchungen (H)	Nur mit zusätzlicher Software möglich.	NeuVector bietet dies immerhin für Netzwerkverkehr an. Snapshots der Container sind mit separater Software möglich.
SYS.1.6.A24 Hostbasierte Angriffserkennung (H)	Empfehlung ist, mindestens den File Integrity Operator einzusetzen.	Mit NeuVector ist hier eine gute Lösung im Lieferumfang, aber dies ist nachträglich zu installieren.
SYS.1.6.A25 Hochverfügbarkeit von containerisierten Anwendungen (H)	Aufbau der Cluster in mehreren Brandabschnitten ist gemäß dem Schutzbedarf der Anwendungen vom Kunden umzusetzen.	Aufbau der Cluster in mehreren Brandabschnitten ist gemäß dem Schutzbedarf der Anwendungen vom Kunden umzusetzen.

[1] (B) Basisanforderung, (H) Anforderung bei erhöhtem Schutzbedarf, (S) Standardanforderung. [2] Erläuterung der Farben siehe Text.

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

Anforderung[1]	OpenShift 4[2]	Rancher/RKE2[2]
APP.4.4.A1 Planung der Separierung der Anwendungen (B)	Die geplanten Netzzonen und die Separierung in Namespaces und Cluster sind umzusetzen. Separierung zwischen den Projekten auf Netzwerkebene ist vom Kunden einzurichten. Es gibt Beispiele in der Dokumentation.	Die geplanten Netzzonen und die Separierung in Namespaces und Cluster sind umzusetzen. Separierung zwischen den Projekten auf Netzwerkebene ist vom Kunden einzurichten. Dies kann auch bei der Installation als Default gesetzt werden.
APP.4.4.A3 Identitäts- und Berechtigungsmanagement bei Kubernetes (B)	OpenShift bringt eine eingebaute Benutzerverwaltung mit, auch sind die Roles in Kubernetes nutzbar. Dies reicht für den Anfang oder zur Installation. Dringend empfohlen ist die Anbindung an einen externen Verzeichnisdienst. Hier unterstützt OpenShift alle gängigen.	Rancher bringt eine eingebaute Benutzerverwaltung mit, auch sind die Roles in Kubernetes nutzbar. Dies reicht für den Anfang oder zur Installation. Dringend empfohlen ist die Anbindung an einen externen Verzeichnisdienst. Hier unterstützt Rancher alle gängigen.
APP.4.4.A4 Separierung von Pods (B)	Per Default umgesetzt.	Per Default umgesetzt. Hier sind allerdings auch die Kubernetes-Prozesse bereits als Container auf den Nodes gestartet, daher noch etwas besser separiert.
APP.4.4.A5 Datensicherung im Cluster (B)	Muss der Kunde mit zusätzlicher Software realisieren. Bekannte Produkte sind im Operator Hub verfügbar.	Snapshots des etcd und der Clustereinstellungen sind über das UI und automatisiert möglich und extern zu speichern.
APP.4.4.A7 Separierung der Netze bei Kubernetes (S)	siehe SYS.1.6.A5	siehe SYS.1.6.A5
APP.4.4.A9 Nutzung von Kubernetes-Service-Accounts (S)	Die K8s-Standardfunktionen stehen zur Verfügung und müssen beim Einrichten der Images entsprechend konfiguriert werden.	Die K8s-Standardfunktionen stehen zur Verfügung und müssen beim Einrichten der Images entsprechend konfiguriert werden.
APP.4.4.A12 Absicherung der Infrastruktur-Anwendungen (S)	Das Verwaltungs-UI und die diversen Operatoren sind hier als Infrastrukturanwendungen zu sehen. Diese verwenden RBAC, Verschlüsselung und eine zentrale Verwaltung in eigenen Namespaces. Das ist als umgesetzt zu sehen. Weitere Anwendungen wie CI/CD etc. organisieren die Kunden.	Bis auf Rancher selbst sind keine Infrastrukturanwendungen im Lieferumfang enthalten.
APP.4.4.A13 Automatisierte Auditierung der Konfiguration (H)	Sollten Kunden mit dem Compliance Operator umsetzen.	Es gibt einen CIS-Benchmark als Werkzeug und auch NeuVector kann dies umsetzen. Der Kunde muss beides installieren und einsetzen.
APP.4.4.A14 Verwendung dedizierter Nodes (H)	Zumindest die Master Nodes sind immer separiert. Weiter gehende Separierung ist mit Kubernetes möglich und sollte vom Kunden so eingerichtet werden.	Separierung ist mit Kubernetes möglich und sollte vom Kunden so eingerichtet werden.
APP.4.4.A16 Verwendung von Operatoren (H)	Dies ist grüner als grün, da Red Hat wohl den Rekord an Operatoren hält.	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)	Ist mit Network Polices teilweise umsetzbar. Diverse Produkte stehen zur Auswahl und können teilweise als Operator installiert werden.	Ist mit Network Polices teilweise umsetzbar. ISTIO kann über das Menü Werkzeug installiert werden.
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)	Speicher kann verschlüsselt werden, so wie auch etcd und Netzwerk (IPSEC im CNI). Bei der Installation kann der Kunde für die Verschlüsselung der Speicher den FIPS 140-2 Mode aktivieren.	Wird nicht angeboten.

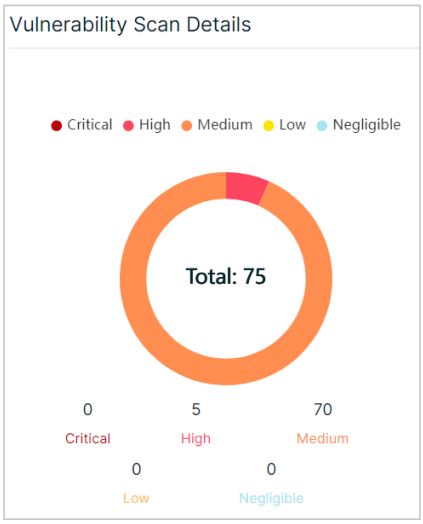
[1] (B) Basisanforderung, (H) Anforderung bei erhöhtem Schutzbedarf, (S) Standardanforderung. [2] Erläuterung der Farben siehe Text.

- 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 in allen Artikeln der Serie [2, 3, 4, 5, 6] wird jeder Anbieter auch auf die Sicherheit der Cluster untersucht. Wo möglich, wurden die CIS-Benchmarks ausgeführt. 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 und die Nodes selbst auf Verwundbarkeiten und Malware zu scannen. Auf den Worker Nodes bei OpenShift fand der Scanner einige Verwundbarkeiten (siehe Abbildung 2). Exploits sind für diese laut Scanner keine verfügbar, die Risikoeinschätzung ist also niedriger, als der CVSS vermittelt. Für alle existieren allerdings bereits Updates.



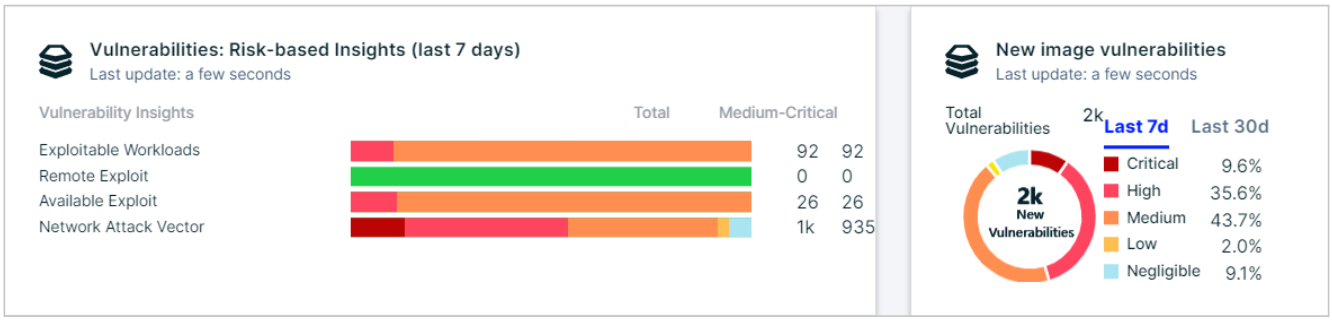
Der Scanner fand auf den OpenShift Worker Nodes einige Schwachstellen (Abb. 2).

Wer einen Cluster neu installiert, bekommt nach dem Scan das in Abbildung 3 gezeigte Bild zu sehen. OpenShift leistet sich auch bei den Verwundbarkeiten in Container-Images einige Lücken. In der Praxis sind diese Verwundbarkeiten zwar nicht von außen ausnutzbar, aber für immerhin 26 existieren Exploits.

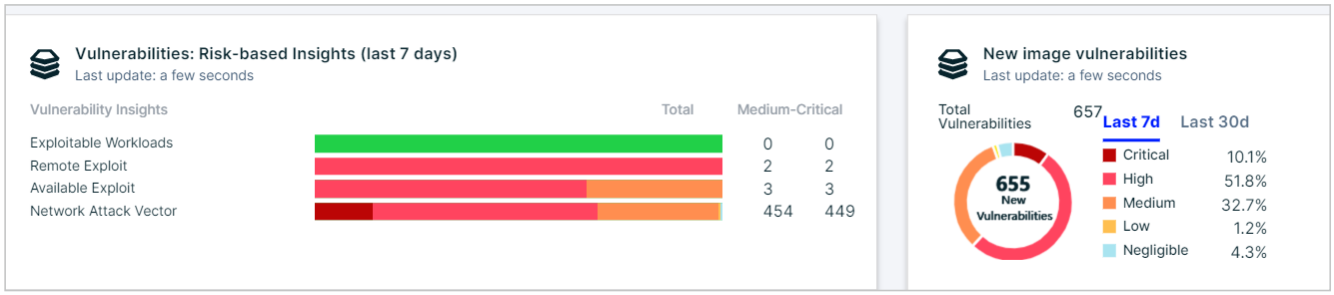
Die Scans des Nodes des Rancher-Beispielclusters aus dem QuickStart sehen gut aus, was die Verwundbarkeiten im Node selbst angeht – hier hat AquaSec keine gefunden. Der Scan nach CIS-Benchmark Kubernetes 1.24 ergab zehn Warnungen.

Abbildung 5 mit den von AquaSec Enforcer gefundenen Verwundbarkeiten führt alle Ergebnisse der Scans aus allen Artikeln dieser Reihe zusammen. Sie enthält zum Vergleich auch die Daten für Plattformen aus den anderen Teilen.

Die offizielle Einstufung in der Grafik ist nach NVD CVSS v3 Severity erfolgt. Die CVSS-Einstufungen stehen in Securitykreisen aber in der Kritik, da sie nicht die realen Risiken zum Missbrauch



Auch bei den Verwundbarkeiten in Container-Images schneidet OpenShift eher unterdurchschnittlich ab (Abb. 3).



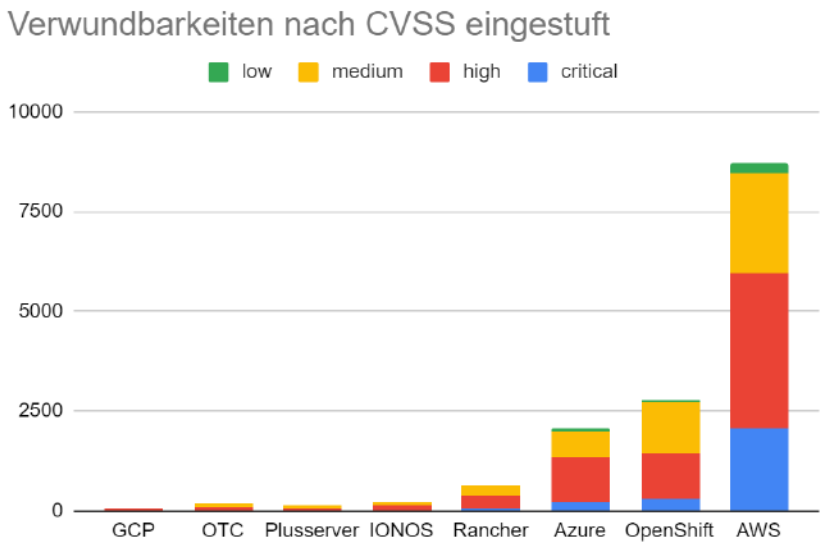
Im RKE2-Cluster gab es viele Images auf den Nodes, auf denen sich allerdings keine direkt ausnutzbaren Schwachstellen fanden (Abb. 4).

in produktiven Umgebungen betrachten. Abbildung 6 zeigt die Ergebnisse mit den Bewertungen des Scanners, der für die gesamte Serie im Einsatz war: AquaSec. Diese sind oft realistischer und orientieren sich vor allem an der praktischen Ausnutzbarkeit der einzelnen Schwachstellen.

Die Unterschiede zwischen den Anbietern sind weiterhin frappierend: Die Bewertung der Verwundbarkeiten durch AquaSec ist überall niedriger als bei der NVD. Besonders die kritischen des Angebots von AWS sind von über 2000 auf 270 reduziert und auch die als „High" bewerteten sinken auf die Hälfte. Daher ist der Abstand zu den anderen Angeboten nicht mehr das Tausendfache von beispielsweise GCP, 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 auch pflegen muss. Wer diese Dienste nachträglich installiert, ist dann natürlich selbst in der Verantwortung. Die Werte für OpenShift und Rancher zeigen, dass Administratoren für einen sicheren Betrieb noch Hand anlegen müssen.

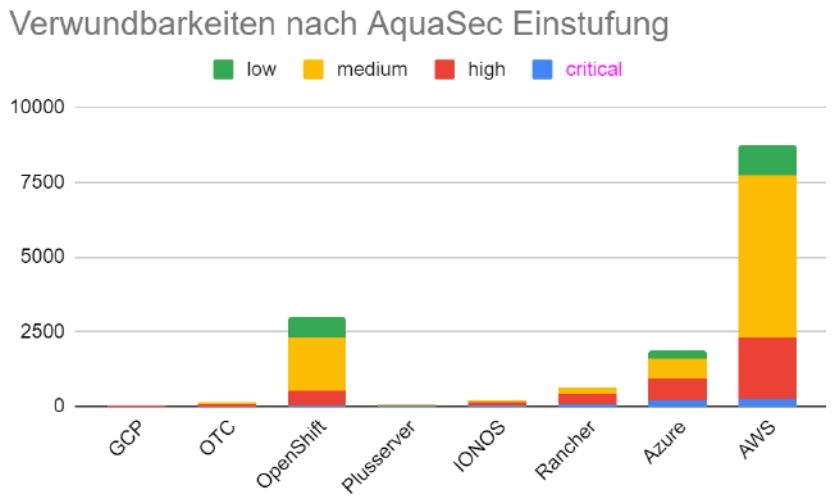
Ein Ausreißer ist dabei GCP: Die Integration von Kubernetes in die restlichen Dienste und insbesondere die Verwaltung der Identitäten steht den beiden anderen Hyperscalern in nichts nach. Allerdings sind diese Images die sichersten, was die Zahl der Verwundbarkeiten angeht.



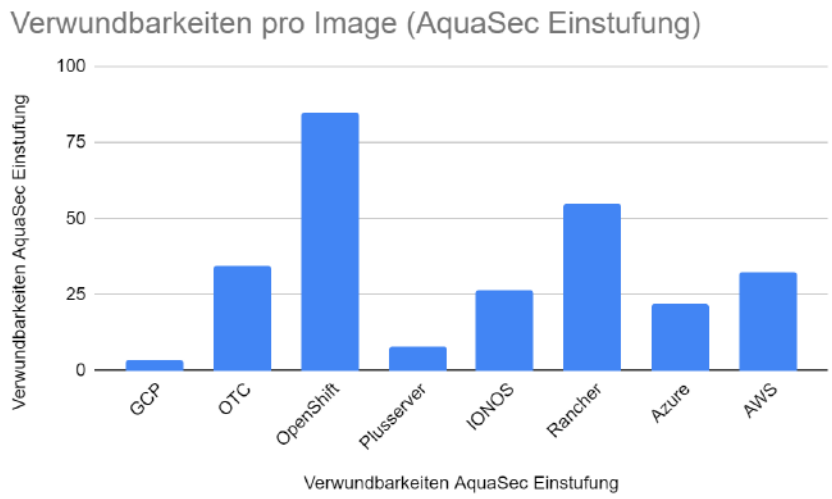
Nach Zahl der kitischen Lücken sortiert: Die von Trivy Premium Edition (OSS-Variante von AquaSec) gefundenen Verwundbarkeiten, bewertet nach NVD CVSS v3 (Abb. 5).

Fazit

OpenShift ist eine ausgereifte Kubernetes-Distribution, die keine wirklichen Schwächen hat und bereits in der Standardinstallation viele Anforderungen des BSI-Grundschutz-Kompendiums abdeckt. Nach oben bietet Red Hat auch Multi-Cluster-Management und nach unten steht mit OpenStack eine Software zur Verwaltung der Hardware zur Verfügung. Die Zahl der im Operator Hub verfügbaren Softwarepakete ist mit fast 500 im Hub und 250 im Marketplace riesig und muss den Vergleich mit den Angeboten der Hyperscaler nicht fürchten. Daher überrascht es nicht, dass OpenShift die mit Abstand am meisten eingesetzte Kubernetes-Distribution ist. Die Zahl der Verwundbarkeiten in den Images und auf den Nodes könnte sicherlich kleiner sein. Ein unveränderliches Audit-Log, wie es die Hyperscaler haben, ist für eine On-Premises-Lösung leider nicht möglich. Mit RKE2 und K3s hat SUSE seit dem



Die gleichen Verwundbarkeiten wie in Abbildung 5, aber mit der AquaSec-Bewertung der Schwere der Verwundbarkeit aufsteigend nach Zahl der kritischen sortiert (Abb. 6).



Die nach AquaSec eingestuften Verwundbarkeiten pro Image geben einen guten Einblick, welcher Anbieter sich Mühe gibt und wo die Sicherheit des Angebots vielleicht nicht die erste Priorität hat (Abb. 7).

Kauf zwei im Markt sehr bekannte und ausgereifte Distributionen im Einsatz. Rancher hat hier das Multi-Cluster-Management bis in die Details der Einstellungen im Griff. Etwas verwundert, dass SUSE noch keine eigenen Images für die Nodes als Default nutzt, sondern weiterhin Ubuntu in einer sehr alten Version für neue Cluster einsetzt. Rancher setzt beim Angebot von zusätzlicher Software nicht auf Marktplätze, sondern auf Helm-Repositorys, für die es bedeutend mehr Auswahl gibt. Allerdings liegt hier die Aufgabe der Parametrisierung der Helm Charts auf die eigene Umgebung beim Kunden und ist damit teilweise doch recht anspruchsvoll. (avr@ix.de)

Quellen

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

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

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

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

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

[6] Christoph Puppe; Kubernetes-Sicherheit: Open Telekom Cloud und PlusServer härten; iX 5/2023, S. 142

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.