Antrag für die betriebliche Projektarbeit

Projektbezeichnung:

Erhöhung der Sicherheit von Kubernetes Umgebungen durch automatisierte CVE-Checks der dort laufenden Container.

Antragsteller:

Sören H. Haferkorn

1. Projektbezeichnung

Erhöhung der Sicherheit von Kubernetes Umgebungen durch automatisierte CVE-Checks der dort laufenden Container.

1.1 Problembeschreibung und Übersicht über das Projekt

Ein Cybersicherheitskonzept ist ein wesentlicher Bestandteil jedes IT-Systems und jeder IT-Umgebung und schützt vor Angriffen und Datenlecks welche direkt (bspw. durch Verschlüsselung von unternehmenskritischen Daten) oder indirekt (bspw. durch Strafen von Regulierungsbehörden) hohe wirtschaftliche Schäden verursachen können.

In modernen Cloud-nativen Umgebungen die auf Kubernetes basieren, muss ein gutes Cybersicherheitskonzept über den Schutz der zugrunde liegenden Infrastruktur wie Netzwerk und Server hinausgehen. Für eine umfassende Sicherheit in solchen Umgebungen ist die Implementierung von Sicherheitsmaßnahmen direkt in Kubernetes essenziell.

Eine solche Sicherheitsmaßnahme ist die Überwachung der auf Kubernetes laufenden Container auf CVEs. Ohne eine solche Überwachung ist es schwierig, Schwachstellen in der dort laufenden Software zu erkennen, welche böswillige Akteure ausnutzen könnten, um den Betrieb der Software, des Kubernetes Clusters oder des gesamten Unternehmensnetzwerkes zu stören. Dies kann zu erheblichen finanziellen Schäden führen und sogar die Existenz eines Unternehmens bedrohen.

1.2 Ist-Analyse

Aktuell befinden sich mehrere Kubernetes Cluster in Betrieb. Es existiert ein Harbor als Container Registry. Der Harbor kann sowohl selbst entwickelte Container Images speichern als auch als Proxy und Cache für externe Container Registries (GHCR, Dockerhub etc.) fungieren. Hierbei muss für jede externe Container Registry welche verwendet werden soll ein eigenes Proxy-Cache Projekt im Harbor angelegt werden. Der Harbor bietet die Möglichkeit, statische Scans der Images (sowohl lokale als auch Proxy Images im Cache) mit Trivy oder Clair durchzuführen.

Welche Container Registry ein Nutzer beim Deployment auf Kubernetes verwendet, ob er den Harbor als Proxy verwendet oder direkt von der externen CR pulled, bleibt ihm überlassen. Es existieren hierfür keine Policies auf Kubernetes. Auch ist es nicht immer möglich den Harbor als Proxy zu verwenden, bspw. wenn externe Helm-Charts genutzt werden. Der Harbor kann offensichtlich nur dann Images scannen, wenn diese über ihn bezogen wurden. Dies führt dazu, dass auch nicht überprüfte Images in den Clustern verwendet werden können.

Hierdurch besteht weiterhin die Möglichkeit, dass Container welche im Cluster laufen CVEs aufweisen, welche unerkannt bleiben.

2. Zielsetzung und Nutzen

2.1 Beschreibung des Soll-Konzeptes

Es soll eine Lösung implementiert werden, welche die Images aller auf Kubernetes laufender Container scannt. Der Scan soll regelmäßig (bspw. einmal pro Tag) erfolgen. Hierdurch können weiterhin Images verwendet werden, welche nicht über den Harbor bezogen wurden. Die Ergebnisse der Scans sollen leicht zugänglich verfügbar sein. Die Lösung soll sich auch in weitere Cybersecurity-Systeme integrieren lassen.

2.2 Anforderungen an das Lösungskonzept

Das Lösungskonzept und die Komponenten müssen:

- Opensource und ohne Lizenzkosten sein
- Geringe Betriebskosten und Administrationsaufwand verursachen
- Möglichst automatisiert CVE Checks für alle in Kubernetes laufenden Container Images
- Verhindern, dass Kubernetes Nutzer die CVE Checks umgehen können
- Die Ergebnisse der Scans übersichtlich darstellen, um das Erkennen von Schwachstellen zu erleichtern
- Automatisiert nach DevOps Prinzipien (IaC / GitOps) auf Kubernetes Clustern deployed werden
- Leicht in bestehende und zukünftige Systeme und Lösungen integrierbar sein

2.3 Wirtschaftlicher Nutzen des Projektes

Laut einer Bitkom Studie sind bis zu 90% aller Unternehmen in Deutschland von Cyberangriffen betroffen, 65% der Unternehmen fühlen sich durch solche Angriffe sogar in ihrer Existenz bedroht. Hierbei entstehen Schäden von über 200 Milliarden Euro pro Jahr.[1] Laut BSI stellen Schwachstellen in Software oft das Einfallstor für Angreifer dar.[2]

Das hier beschriebene Projekt ermöglicht in Kubernetes Umgebungen laufende Software regelmäßig auf bekannte Schwachstellen und deren Kritikalität zu überprüfen. Hierdurch können entsprechende Maßnahmen getroffen werden, um Einfallstore für Angreifer und das Schadenspotential bei Angriffsversuchen zu minimieren. Dies kann dem Unternehmen nicht nur viel Geld sparen, sondern in einigen Fällen sogar existenzsichernd wirken.

3. Projektphasen

3.1 Tabellarische Übersicht über die Projektphasen und Zeitplanung

Entwurf	**15 h**
➔ Recherche bzgl Funktionalität von infrage kommender Software	8 h
➔ Erste Deployments und Tests der infrage kommenden Software	5 h
➔ Deployment Diagramm Entwurf erstellen	2 h
Implementierung und Deployment	**6 h**
➔ Schreiben von IaC für das Deployment der Projektkomponenten	3 h
➔ Deployment der Projektkomponenten	3 h
Tests	**8 h**
➔ Atomare Tests der Komponenten	4 h
➔ Deployment von Containerimages mit bekannten CVEs und durchlaufen des Scanprozesses (Testen des Zusammenspiels der Komponenten)	4 h
Anfertigung Dokumentation	**11 h**
➔ Erstellung der Projektdokumentation	5 h
➔ Erstellung der Betriebsdokumentation	6 h

4. Ausbildungsbetrieb und Zielgruppe

5. Sonstiges Berufsschule

5.1 Tech-Stack

In diesem Projekt wird der Fokus hauptsächlich auf Trivy gelegt. Trivy wird genutzt, um die in Kubernetes laufenden Container auf CVEs zu scannen.

5.2 Alternative Möglichkeiten

Ein eventuell besserer Weg wäre, Trivy nicht direkt zum Scannen der Container images zu verwenden, sondern nur um SBOMs der Images zu erstellen. Diese SBOMs würden dann in einem weiteren Tool (wie beispielsweise Dependency Track; Trivy kann auch SBOMs scannen) auf CVEs überprüft werden. Dies ermöglicht das generieren von SBOMs mehrerer Entitäten (Server, Software, Container) und das Scannen dieser an einem zentralen Ort.

6. Quellen

1: https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2024

2: https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html