Allgemeine Sicherheit

Datensicherung

Im Open Source Bereich sieht es im Thema Datensicherung nicht so gut aus. Jedoch bieten auch einige Hersteller abgespeckte Versionen ihrer Professionellen Produkte kostenlos an.

Ich bevorzuge die Produkte vom Hersteller Veeam - so bietet er z.B.die folgenden Produkte an:

- Sicherung Windows / Linux Rechner
- Sicherung VMWare / HyperV Hypervisor
- Sicherung Office /Microsoft 365
- Und noch vieles mehr ...

Die Downloads findet ihr hier.

BSI bietet auch kostenlos Unterstützung an

Das BSI bietet mehrere Mittel um zu Unterstützen.

So bietet es für Privatpersonen einen Newsletter an welcher über Software und Geschehnisse berichtet für den privaten Sektor.

Diese Newsletter bietet das BSI auch den Kommerziellen Bereich an, hier wird jedoch eher auf Firmenprodukte eingegangen.

Weiterhin bietet es ein Magazin an, welches viele Informationen rund um die IT - und Cyber - Sicherheit bietet: BSI - BSI-Magazin (bund.de).

Auch eine interessanter Dienst, ist die Allianz für Cybersicherheit - hier kann man einen Bündnis beitreten, welches viele Informationen und auch eine Anlaufstelle bietet rund um das Thema Cybersicherheit. Hier gibt es jedoch nicht nur Hilfe zur Prävention, sondern auch wenn schon was vorgefallen ist.

Containersicherheit

Fast immer nutzt man Docker Container, die von anderen bereitgestellt werden. Dabei ist man darauf angewiesen, das diese sich um die Sicherheit kümmern.

So gibt es mehrere Punkte zum Thema Sicherheit die man beachten sollte:

- Zum einen sollten die verwendeten Quellen keine Sicherheitslücke (CVE) aufweisen.
- Viele Komponenten setzen Web- oder Datenbankkomponente ein, hier gibt es auch bestimmte Probleme mit SQL Injection, Cross Site Scripting usw.
- Es könnten Keys oder fest eingerichtete User oder gar Backdoors eingerichtet sein.

Ein Open Source Tool, welches als CLI installiert werden kann direkt auf den Docker host selber ist z.B. Triny.

Installation

```
sudo apt-get install wget apt-transport-https gnupg lsb-release
wget -qO - https://aquasecurity.github.io/trivy-repo/deb/public.key | gpg --dearmor | sudo tee /usr/share/keyrings/trivy.gpg > /dev/null
echo "deb [signed-by=/usr/share/keyrings/trivy.gpg] https://aquasecurity.github.io/trivy-repo/deb $(lsb_release -sc) main" | sudo tee -a /etc/apt/sources.list.d/trivy.list
sudo apt-get update
sudo apt-get install trivy
```

Befehle

```
# Beispiel
trivy image --ignore-unfixed --scanners vuln <image> > <dateiname>
Scan:
trivy image --ignore-unfixed --scanners vuln vaultwarden/server:latest > /home/pleibling/240420_vaultwarden_report.txt
```

Formulare

Erstellen sie eine lokale Formatvorlage, als Beispiel könnte diese hier dienen:
https://github.com/aquasecurity/trivy/blob/main/contrib/html.tpl

Passen sie diese Vorlage ihren wünschen entsprechend an und speichern sie diese ab.

Mit dem folgenden Befehl können Sie dann diese Vorlage verwenden:

```
# Vorlage:
trivy image --format template --template "@html.tpl" -o <dateiname> <image>
# Beispiel:
trivy image --format template --template "@html.tpl" -o report.html phpmyadmin
```

Weitere Informationen

- https://www.heise.de/hintergrund/Marktuebersicht-Sicherheitsscanner-fuer-Container-Images-9682078.html?seite=all
- https://github.com/aquasecurity/trivy
- https://medium.com/@maheshwar.ramkrushna/scanning-docker-images-for-vulnerabilities-using-trivy-for-effective-security-analysis-fa3e2844db22
- https://aquasecurity.github.io/trivy/v0.48/docs/configuration/filtering/
- https://www.youtube.com/watch?v=Em_DdKkPUR8