QUANT-X SECURITY & CODING

Wie man Container-Umgebungen vor Malware schützen kann

secIT by Heise
HANNOVER 2022

https://quant-x-sec.com/ | stefan.alfeis@quant-x-sec.com

Inhalte

- Was ist Malware?
- Was sind Container?
- Container out of the box?
- Grundlegende Einstellungen
- Malware Schutzprogramme
- Aktuelle Kampagnen und Gefahren
- Zusätzliche Maßnahmen zum Schutz der Systeme

stefan.alfeis@quant-x-sec.com


MALWARE

Was ist Malware?

- Malware ist ein Programm oder Code mit bösartiger Intention

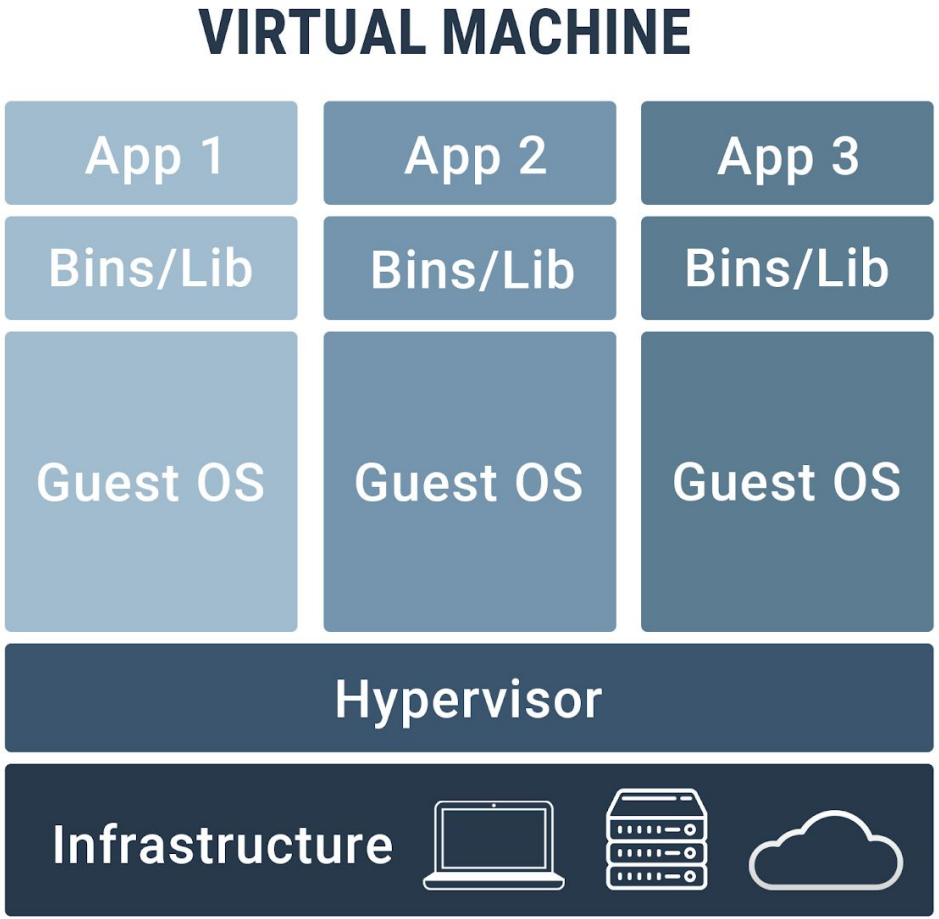
- Arten von Malware
  - Ransomware
  - Wiper
  - Spyware
  - Trojaner
  - Viren und Würmer
- https://www.youtube.com/watch?v=HYv15BInzas

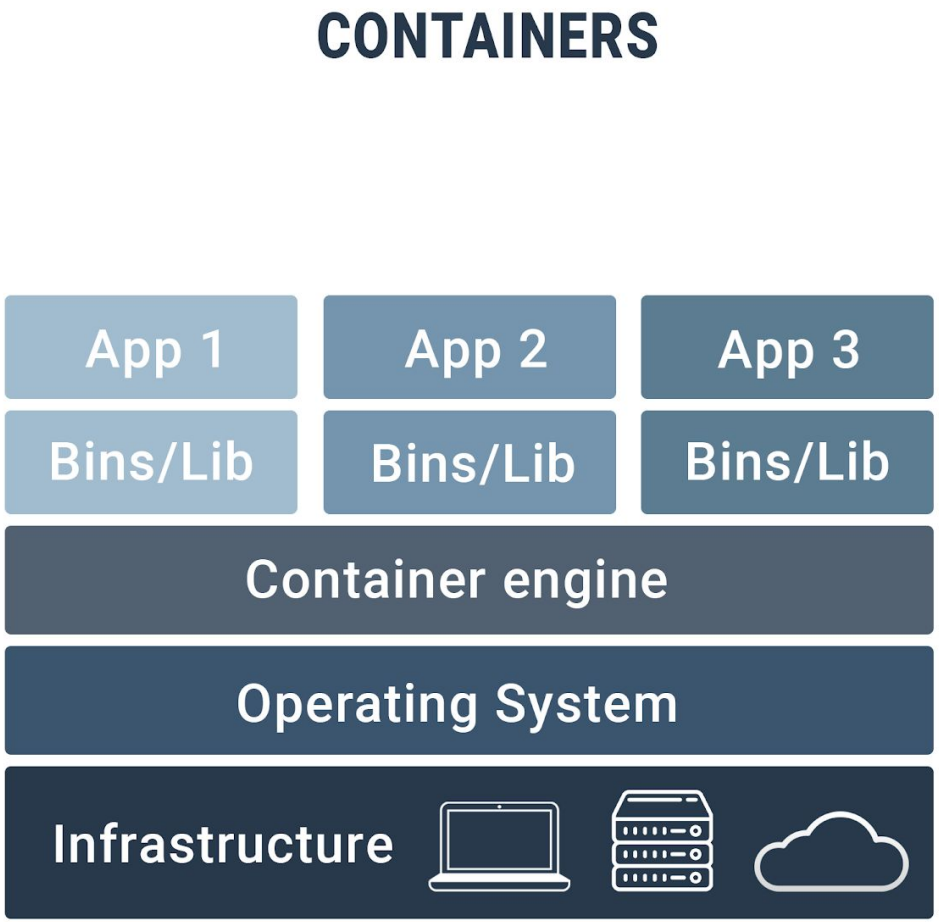
stefan.alfeis@quant-x-sec.com

Was ist Malware?

- Infektionswege
  - aktiv -> Schadsoftware wird von innen oder außen durch Angreifer eingebracht
  - passiv -> Nutzer lädt Schadsoftware als “Trittbrettfahrer” mit herunter

stefan.alfeis@quant-x-sec.com





stefan.alfeis@quant-x-sec.com

Was sind Container?

PRO		CONTRA	
● VM	einfache Verwaltung Flexibiltät	● VM	Belastung Host-Ressourcen Performance
● Container	geringere Kosten Portabilität	● Container	nicht alle Anwendungen profitieren Sicherheit erfordert Aufwand

stefan.alfeis@quant-x-sec.com

stefan.alfeis@quant-x-sec.com

Container out of the box?

- viele vorgefertigte Container verfügbar
- genaue Informationen einholen, wie das Setup des Downloads vorgefertigt ist
  - Download-Quelle verifizieren
  - alles nicht benötigte ausschalten/deaktivieren

stefan.alfeis@quant-x-sec.com

Grundlegende Einstellungen

- Host System / Container härten
  - Apparmor, SELinux, Smack, Loadpin… konfigurieren
  - nicht benötigte Prozesse ausschalten
  - nur notwendige Portfreigaben (lokale Firewall)

stefan.alfeis@quant-x-sec.com

Grundlegende Einstellungen

- Host System / Container härten
  - Rechte- und Rollenkonzepte
  - Updates, Updates, Updates
    (aber vorher prüfen!!!)
  - Schwachstellen behandeln

stefan.alfeis@quant-x-sec.com

Grundlegende Einstellungen

- gesamtes Netzwerk im Blick haben
  - Firewalls, DMZ, Router Konfiguration etc.
  - wenn Container nicht selber gehostet werden Verbindung sicher gestalten
- Passwörter ändern
- Multi-Factor Authentifikation

stefan.alfeis@quant-x-sec.com

Malware Schutzprogramme

- diverse am Markt verfügbar
- einige unterstützen ab Development der Container
- Forensische Daten können erfasst werden
- Übersicht über die Containerlandschaft möglich

stefan.alfeis@quant-x-sec.com

Aktuelle Kampagnen und Gefahren

- log4Shell / log4j
- emotet
- cryptocurrency mining malware 04/21
- Supply chain attacks 03/22
- Exploits für OS in den Containern
- Cyber-War 02/22

stefan.alfeis@quant-x-sec.com

Zusätzliche Maßnahmen zum Schutz der Systeme

- Monitoring der eigenen Systeme
  - wer blind ist, kann nicht handeln
- regelmäßige Schwachstellen Scans
- Nachrichten und Foren beachten

stefan.alfeis@quant-x-sec.com

Zusammenfassung

Es ist wichtig, IT-Systeme aktuell zu halten!

Vielen Dank

Find these slides on https://quant-x-sec.com/published.htm
(in the section Talks/Presentations at Conferences and Events)

stefan.alfeis@quant-x-sec.com