Technische Hochschule Wildau
FB Wirtschaft, Informatik, Recht
Prof. Dr. – Ing. Stephan Rein

Technische Hochschule Wildau
Technical University of Applied Sciences
WILDAU

Bachelor Arbeit

Forensische Speicher-Analyse mittels Container-Checkpoints

Beschreibung

Die Container-Technologie wird in vielen Unternehmen als Alternative zu klassischen Virtuellen Maschinen (VMs) eingesetzt. Container müssen ähnlich wie VMs aus unterschiedlichen Gründen migriert werden, z.B. für den Umzug auf andere Hardware oder Standorte. Eine Methode dafür ist, den Container anzuhalten, dann alle relevanten Konfigurationen und Daten auf den neuen Host zu verschieben und schließlich den Container am Zielhost wieder zu starten. Diese Methode wird auch „cold migration“ genannt. Im Gegensatz dazu wird bei der sogenannten „warm migration“ versucht, ein vollständiges Abbild des Containers zu erzeugen, dass u.a. auch den Zustand des Speichers erfasst. So können z.B. angefangene Verbindungen zu einem Web-Server fortgesetzt werden. Das Erfassen eines „warmen“ Abbildes wird auch „Checkpoint“ genannt. Da ein solcher Checkpoint auch den Speicher eines Containers umfasst, bietet es sich an, diesen auf mögliche Schadsoftware zu untersuchen. Durch eine auf diese Art durchgeführte forensische Analyse wird sichergestellt, dass mögliche Einbrecher die Untersuchung nicht bemerken. Die Analyse des Speichers erlaubt es, besonders raffinierte Schadsoftware zu erkennen.

Aufgaben

In dieser Arbeit sollen neue Ansätze entwickelt werden, wie eine Schadsoftware im Speicher eines Containers mittels Checkpoints erkannt und der Container davon bereinigt werden kann. Die Erkennung und Bereinigung sollte idealerweise automatisiert ablaufen können. Zur Erstellung der Checkpoints soll das Linux-Tool CRIU (https://criu.org) unter einer Container-Umgebung (Docker, LXC/LXD oder CRI-O für Kubernetes) eingesetzt werden. Zur Erkennung von Schadsoftware im Speicher können weitere Linux-Tools verwendet werden, z.B. das Tool „volatiity“ (kurzes Tutorial hier) .

Voraussetzungen

- Linux-Kenntnisse
- Python

Mögliche Literatur:

- Sascha Winkelhofer, **Konzeption und Umsetzung von Live-Migration für Docker-Container**, Bachelorarbeit Univ. Ulm 2017
- Sang-Hoon Choi, iContainer: **Consecutive checkpointing with rapid resilience for immortal container-based services**, Elsevier Journal of Network and Computer Applications, Sept 2022
- Adrian Reber, **Container Live Migration**, Devconf 2021
- Adrian Reber, **CRIU and SELinux**, Linux Security Summit EU 2019
- Adrian Reber, **CRIU and the PID dance**, Linux Plumbers Conference 2019

- Ranjan Sarpangala Venkatesh et al., **Fast in-memory CRIU for docker containers**, MEMSYS‘19

Kontakt: stephan.rein@th-wildau.de

https://th-wildau.de/stephan-rein