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

Technische Hochschule Wildau
Technical University of Applied Sciences

Bachelor oder Master Arbeit

# Praktikabilität von Standard-Security-Regelsätzen für Container-Systemcall-Logging

**Beschreibung**

Die Container-Technologie wird in vielen Unternehmen als Alternative zu klassischen Virtuellen Maschinen (VMs) eingesetzt. Im Vergleich zu virtuellen Maschinen wird bei den Containern der Linux-Kernel des Host-Rechners gemeinsam verwendet. Die Isolierung zum Host-System ist also Prinzip-bedingt bei Containern schwächer, weshalb Container in der Regel zusammen mit verschiedenen Sicherheits-Tools betrieben werden.

Eine bestimmte Klasse von Sicherheitstools loggt dabei möglicherweise gefährliche Systemaufrufe - das sind bestimmte Funktionen, die vom Kernel bereit gestellt werden und für den Betrieb von Applikationen notwendig sind (z.B. Zugriffe auf Dateien oder das Netzwerk). Mittels der Log-Files kann untersucht werden, ob ein Container kompromittiert wurde. Der Erfolg einer solchen Untersuchung hängt allerdings von der Auswahl von geeigneten Security-Regeln ab, mit denen die Sicherheitstools konfiguriert werden. Werden zu wenige Regeln konfiguriert, kann der Sicherheitsvorfall nicht erkannt werden, werden zu viele Regeln eingesetzt, kann es zu einer Überflutung der Log-Systeme kommen oder bedeutsame Ereignisse werden übersehen.

In dieser Arbeit soll die Praktikabilität eines Default-Regelsatzes für die Erkennung von Sicherheitsvorfällen untersucht und verbessert werden. Zunächst soll hierfür ein System aufgebaut werden, das möglicherweise gefährliche Aktivitäten, die in einem Container statt finden, protokolliert. Für die Aufnahme der Systemcalls soll dabei die Software *Falco* (https://falco.org) in Kombination mit der Datenalalyse-Software *Elasticsearch* eingesetzt werden. Anhand von einem gegebenen Default-Regelsatz von Falco und einer Auswahl von aktuelleren Kernel Exploits (z.B. „dirty cow“ oder „kinsing“), ggf. auch kombiniert mit Denial-of-Service-Angriffen, sollen die folgenden Aspekte untersucht werden:

- Können die bösartigen Aktivitäten über das Log-System erkannt werden (auf der Ebene von Falco oder von Elasticsearch) ?
- Sind die Regeln praktikabel im Hinblick auf verfügbare System-Ressourcen und einer zielführenden Analyse ?

Als mögliche Applikationen können Web-Server (z.B. Apache2) oder Content-Management-Systeme (z.B. Wordpress) verwendet werden. Die Beantwortung der offenen Fragen soll idealerweise zu Verbesserungen des Sicherheitsinformationssystems führen, z.B. durch mehrstufige Regelsätze, wobei bestimmte aufwändigere Logs nur durchgeführt werden, wenn bestimmte vorherige Ereignisse eingetreten sind.

**Voraussetzungen**

- Linux-Kenntnisse (z.B. durch Besuch von Veranstaltungen)
- Python oder vergleichbare Programmierkenntnisse

**Mögliche Literatur**

- **Luca Guerry and Nicolas Lacasse**, Strengthen K8s & Container Security without Loosing Visibility, Cloud Native Computing Foundation Webinar, Sept 2022
- **Federico Lago**, Building a SIEM: centralized logging of all Linux commands with ELK + auditd, Infosec Writeups, August 2020, (link)
- **Thanh Nguyen** et al., Live system call trace reconstruction on Linux, Elsevier Journal on digital/multimedia forensic science and evidence-based incident response, Vol. 42, Juli 2022

**Datenbanken für Sicherheits-Fehler**

- https://www.cvedetails.com/vendor/13534/Docker.html
- https://security-tracker.debian.org/tracker/source-package/docker.io
- https://cve.mitre.org

**Kontakt:** stephan.rein@th-wildau.de

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