Zürcher Hochschule
für Angewandte Wissenschaften

School of Engineering

InIT Institut für angewandte Informationstechnologie

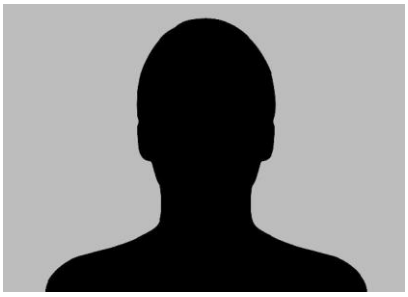
Angriffserkennung auf einer abgesicherten Plattform mit Hilfe von Honeypots

Honeypots können dabei helfen, Angriffe zu erkennen und die verwendeten Methoden des Angreifers nachzuvollziehen. Herausfordernd ist hierbei das erfolgreiche Anlocken und Täuschen eines Angreifers sowie die zuverlässige Erkennung des Angriffs. Der Industriepartner setzt bereits Honeypots ein, hat jedoch Probleme mit hohen False-Positive-Raten und wünscht sich eine umfassendere Lösung und eine abgesicherte Plattform, welche im Rahmen dieser Bachelorarbeit als Proof-of-Concept-Implementierung erarbeitet worden ist.

Mittels der Analyse der Umgebung des Industriepartners und dem Erstellen eines Angreifer- und Bedrohungsmodells ist eine, den Anforderungen entsprechende, Architektur und Proof-of-Concept-Implementierung entwickelt worden. Ziel der Lösung ist die möglichst identische Nachbildung der produktiven Umgebung des Industriepartners, das Erkennen von neuen Angriffstechniken und die Optimierung der False-Positive-Rate der Angriffserkennung.

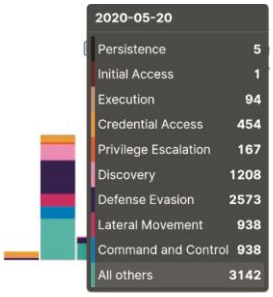
Die Honeynet-Lösung kombiniert mehrere High-Interaction-Honeypots und implementiert einen modernen Ansatz auf Basis des ELK-Stack mit Detection-Rules und Machine-Learning gestützter Anomalieerkennung, um die definierten Angreifer zu erkennen und die False-Positive-Rate zu optimieren. Durch die Automatisierung und Konfigurierbarkeit des Deployments wird der Wartungsaufwand und die Wiederverwendbarkeit der Lösung bewerkstelligt. Anhand der Analyse wurden sinnvolle Angriffsszenarien definiert, welche zum Testen der Lösung verwendet wurden.

Die eingesetzten Machine-Learning-Jobs zur Erkennung von Anomalien konnten in den Testfällen nicht überzeugen, da zu viele False-Positives generiert wurden oder potenzielle Angriffe nicht erkannt wurden. Die Verwendung von klassischen Detection-Rules funktioniert hingegen sehr gut. Die Proof-of-Concept-Implementierung imitiert einzelne Komponenten der produktiven Umgebung bereits glaubhaft und bietet eine gute und flexible Basis für Erweiterungen.



Diplomierende
Rémy Andres Keil
Benjamin Pereto

Dozent
Peter Berlich



Detektierte Angriffe auf die Honeynet-Lösung kategorisiert nach Angriffstaktiken.

Code-Injection, welche mit der Honeynet-Lösung erkannt wird.