Anomalie Detection in Netzwerken

Statusbericht Nr.1

Ives Schneider

1. Projektarbeit

Am 02.09.2019 sendete ich ihnen den erarbeiteten Projektantrag. am 13.09.2019 bekam ich ihr Feedback und habe den Antrag dementsprechend angepasst.
Seit unserem initialem Gespräch, habe ich angefangen eine Vorstudie durchzuführen, um in der POC Umgebung noch einen fehlenden Log-Collector, sowie ein NMS zu evaluieren.
Des Weiteren erstellte ich eine Risiko und SWOT-Analyse, um die Umgebung, momentan sowie in Zukunft besser einschätzen zu können.

Viel Zeit floss in die Evaluation der Log-Collector Lösung.

Angeschaute Log-Collectors

- Graylog
- ELK-Stack
- Splunk

Für jede Lösung wurde eine VM erstellt, um sie genauer anzuschauen und festzustellen, ob die APIs die gewünschte Funktionalitäten unterstützen. Für die Testserver wurde folgende Konfiguration verwendet:

Hardware Konfiguration

- CPU: 2 Core
- RAM: 4 GB
- Speicher: 16GB

Einige Probleme gab es mit dem Setup der ELK-Stack Umgebung, da meine Testclients eine andere Beats-Version benötigten um Logs weiterzuleiten.
Bei Graylog und Splunk hingegen lief alles ohne Probleme ab.

2. Reflexion

Ich habe das Gefühl, dass ich in dieser Projektphase weniger Zeit mit Details verbringen und nur grob Informationen Sammeln. Die meiste Zeit wird schlussendlich darin liegen, die Software zu entwickeln, welche mit den restlichen Systemen kommuniziert. Ob nun Splunk, Graylog oder ELK-Stack verwendet wird, ist nicht extrem von belangen (Alle besitzen dieselben APIs). Daher werde ich bei der NMS Evaluation weniger auf die Details gehen.

3. Zukünftig

Die Vorstudie hat noch eine unfertige Punkte, welche noch nachgeführt werden müssen.
Das Ziel ist es, die Vorstudie zumindest vorzeige fähig bis Montag (16.09.2019) fertig zu haben und danach mit der Hauptstudie / dem Programmieren anzufangen.