Anomalie Detection in Netzwerken

Projektantrag

Ives Schneider

Index

1. Projektinformationen

Auftraggeber

Technische Berufsschule Zürich
Sihlquai 101
8090 Zürich
admin.hf@tbz.zh.ch

Projektleitung

Ives Schneider
Binzstrasse 19
8712 Stäfa
ives.schneider@i-401.xyz

Experte

Marco Sieber
marco.sieber@tbz.ch

Studiengang

IT Service Engineer HF

Klasse

ITSE17a

2. Projektbeschreibung

Basierend auf dem Netzwerk der TBZ HF soll eine Lösung zur Anomalie Detection evaluiert werden und in einem POC aufgebaut und entsprechend dokumentiert werden (inkl. Betriebsdokumentationen).
Die Lösung soll die Fähigkeit bieten, unautorisierte Aktivitäten im Netzwerk erkennen zu können.

2.1. Problemstellung

Netzwerkanomalien können weitreichende folgen haben. Angefangen von kleineren Paketverlusten, bis hin zum Ausfall ganzer Komponenten.
Die Erkennung solcher Anomalien ist meist mühselig und schwierig und kann unter Umständen mehrere Ressourcen aufbrauchen bis der Standard wiederhergestellt werden kann.

2.2. IST-Zustand

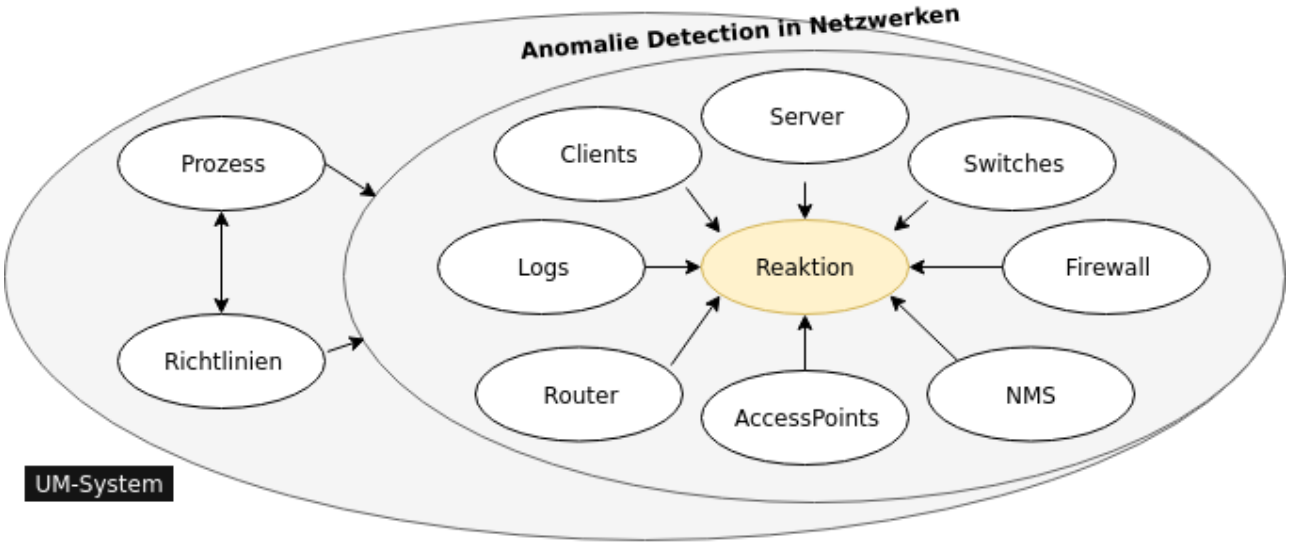
Das POC LAN @Gitlab besitzt ein NMS (Network Monitoring System) welches bereits rudimentär den Status des Netzwerkes überwacht (Throughput). Anomalien können allerdings nicht näher erkannt werden, noch kann mit Genauigkeit gesagt werden, wo die Anomalie aufgetreten ist.

2.3. Würdigung des IST-Zustandes

Die Infrastruktur bietet eine Basis, um Ausfälle einzelner Dienste zu sehen und die Administratoren zu informieren. Paketverlust oder andere Anomalien können zzt. noch nicht erkannt werden. Da bereits Switches, welche via SNMP überwacht werden, kann darauf aufgebaut werden, um weitere Informationen zu bekommen.

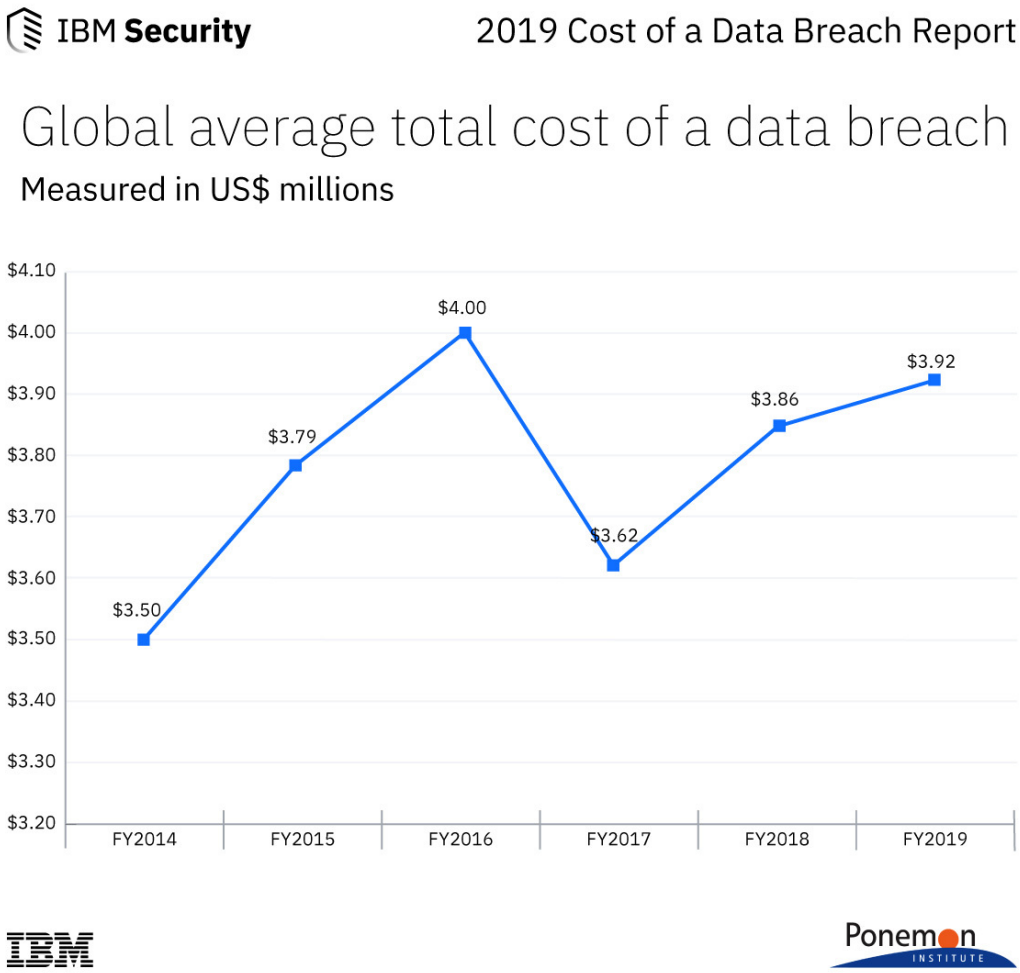
2.4. Aufgabenabgrenzung

Um Anomalien frühzeitig und um möglichst "False Positives" zu vermeiden, ist es unabdingbar, möglichst viele Netzwerkgeräte miteinzubeziehen. Prozesse sowie bereits vorhandene Richtlinien werden durch das Projekt nicht abgeändert, sondern eventuell noch durch neue Prozesse ergänzt.



3. Wirtschaftlichkeit

Initial betrachtet, ist der Finanzielle nutzen eines Anomalie Detection Systems nicht direkt sichtbar. Allerdings muss dabei die Kosten eines erfolgreichen Angriffs in Augenschein genommen werden.



Natürlich ist dabei zu beachten, dass umso länger ein Angreifer im Netz ist, umso kostspieliger wird das entfernen der Spuren.

Da die zu evaluierende Software unter Umständen gewisse Kosten nach sich ziehen könnte, wird in der Vorstudie genauer auf das Lizenzmodell eingegangen. Da es sich allerdings um ein POC handelt, kann grundsätzlich auf Community Versionen zurückgegriffen werden, welche in der Regel frei zur verfügung stehen. Das Tool selbst soll inhouse entwickelt werden, daher fallen ausser Personenstunden keine zusätzlichen Kosten an.

4. Anforderungen und Kriterien

4.1. Anforderungen

- Anomalien werden am Ende schnell und nachvollziehbar aufgezeichnet und sind verfolgbar.
- Die nicht vorhandene Baseline soll durch eine übersichtliche Grafik bis zum Ende des Projekts erstellt werden.
- Das entwickelte Tool ist nach der Fertigstellung durch weitere Module ausbaufähig.
- Am Ende des Projekts ist es möglich mehrere Log-Collectoren gleichzeitig zu überwachen.
- Der Sourcecode wird während der Entwicklung offen gehandelt und steht dritten zur Verfügung.
- Vollumfängliche Dokumentationen sind für die Wartung/Konfiguration am Ende des Projekts verfügbar.
- Ein Systemadministrator ist am Ende des Projekts fähig, Installationen anhand einer Dokumentation selbst vorzunehmen.
- Anomalien werden nach der Installation, direkt via Mail den zuständigen Administratoren gemeldet.
- Das Tool kann nach der Installation durch ein Web/-CLI Interface direkt gemanagt werden.

4.2. Kann Kriterien

- Administratoren werden am Ende des Projekts über Push Benachrichtigungen über Anomalien informiert.
- Administratoren können sich via Single-Sign On Lösung am Tool authentifizieren, um Konfigurationen zu ändern.
- Das Tool ist am Ende des Projekts auf mehreren Architekturen verfügbar.
- Nach der Entwicklung setzt die Installation nicht auf ein bestimmtes OS, sondern ist auf mehreren betriebsfähig.

4.3. Bewertungskriterien

API	Die Applikation besitzt ein ausführliches und umfassendes API.
Dokumentateion	API sowie andere Konfigurationsmöglichkeiten sind ausführlich dokumentiert.
Performance	Ein single-node muss auch bei höheren Lasten noch immer eine gute Performance liefern.
Skalierbarkeit	Clusterfunktionalität der Applikation.
Lizenz	Wie offen ist die Lizenz, kann die Applikation geändert werden?
Ausgereift	Wie ausgereift ist die Applikation?
Aktivität	Wie aktiv wird an der Applikation weiterentwickelt?

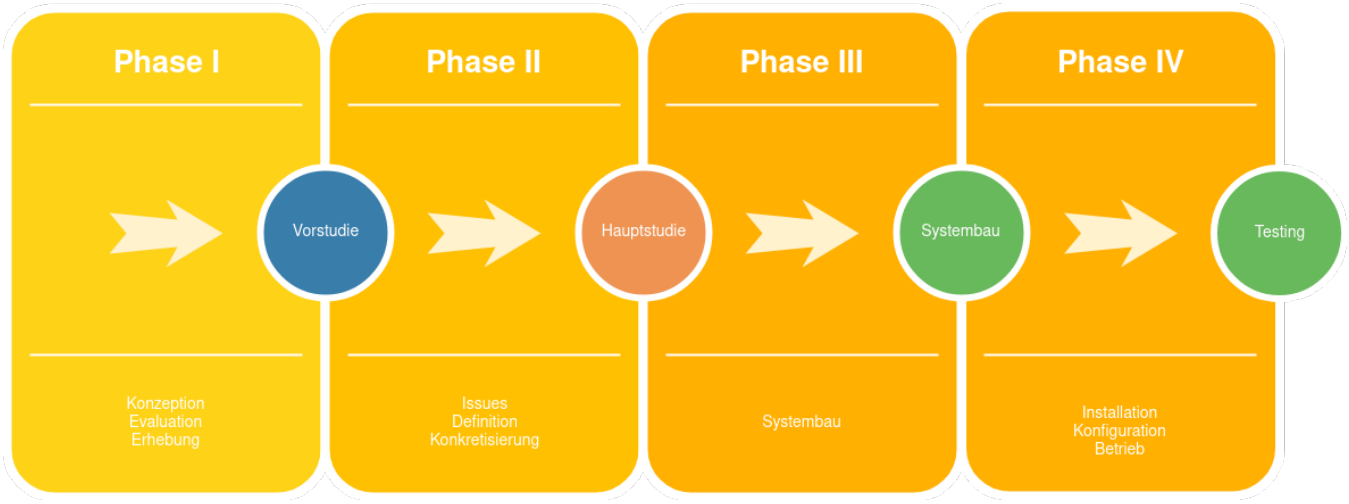
5. Vorgehenssystematik

5.1. Projektablauf

Das Projekt wird in einer Mischung aus Wasserfall und Agiler Projektform ablaufen.
Dieses Dokument beinhaltet den Antrag darüber, die Vorstudie durchführen zu können. Es soll dazu dienen, die *Initiative* **Projektphase** abzudecken. Die Planung (Vorstudie) wird danach gemäss Planungszyklus abgearbeitet um die aufgelisteten *Anforderungen*, sowie *Kann* Kriterien abzudecken. Folglich wird auf die abgeschlossene Vorstudie wird mithilfe der getroffenen Entscheidungen eine Hauptstudie durchgeführt und die Systeme implementiert und dokumentiert werden.
Wichtig ist dabei, dass die Transparenz jederzeit gewährt ist und der Kunde Einblick in den Vortschritt des Projektes hat.

5.2. Projektphasen

Den jeweiligen Vortschritt kann auf dem Projektspezifischem Github Repository nachvollzogen werden.



5.2.1. Phase I | Vorstudie

Da fehlende Systeme in der Infrastruktur eine Konzeption des Tools für eine Anomalie Erkennung schwierig gestalten, wird in einer Vorstudie die bestehende Infrastruktur analysiert und zusätzliche Software evaluiert.

Zur evaluierenden Software gehören folgende Komponenten:

- Centralized Log Management
- Network Monitoring System

Für die Erhebung wird auf das bestehende Umfeld, sowie die Erfahrung mit den Tools zurückgegriffen.

5.2.2. Phase II | Hauptstudie

In der Hauptstudie werden Issues für die Realisierung erarbeitet und konkretisiert. Es wird auf die Hilfe des Projekt Features von Github zurückgegriffen, sodass der Kunde jederzeit Einsicht auf die momentane Situation des Projekts hat. Des weiteren wird der Begriff "Anomalien" konkretisiert und erste Tests durchgeführt.

5.2.3. Phase III | Systembau

Das Tool welches Informationen aus den verschiedenen Netzwerkdevices zieht um Anomalien zu erkennen wird in dieser Phase, anhand der definierten Issues gebaut und getestet. Welche Sprache und in welchem Umfang das Tool entwickelt wird, wurde in der Phase II entschieden.

6. Freigabe

Dieses Dokument soll die groben Ressourcen für das kommende Projekt beinhalten.
Änderungen vorbehalten.

Technische Berufsschule Zürich

Marco Sieber
Sihlquai 101
8090 Zürich
marco.sieber@tbz.ch

Projektleiter
Ives Schneider
Binzstrasse 19
8712 Stäfa
ives.schneider@i-401.xyz