Vorstudie

Anomalie Detection in Netzwerken

Ives Schneider

Index

1. Management Summary

TODO

2. 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

2.1. Projektauftrag

2.1.1. 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.

2.1.2. 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.

2.1.3. Projektorganisation

Figure 1. Projekt Mitarbeiter

2.1.4. Projektzeitplan

TODO

2.1.5. Ausgangslage

TODO

3. Projektziele

Die Anforderungen sollen die nötigen Funktionen erfüllen, um eine gute Übersicht über das bestehende Netzwerk aufzuzeigen, Anomalien erkennen und deuten zu könenn.

3.1. Muss Kriterien

- Baseline muss umfänglich ersichtlich sein

  Es muss eine grundlegende Analyse des normalen Netzwerkverkehrs erstellt werden.
- Lösung soll Modular sein

  Die Lösung soll mit mehreren NMS sowie Switches arbeiten können.

  Falls ein "Modul" nicht erwünscht sein sollte, kann es deaktiviert werden.
- Scaleability soll vorhanden sein

  Es soll die Möglichkeit bieten mehrere Log-Collectoren anzuschliessen.
- OpenSource Lösung

  Der Sourcecode soll für Erweiterungen veröffentlicht werden.
- Betriebsdokumentation

  Der Betrieb kann klar anhand einer Dokumentation nachvollzogen und nachgestellt werden.
- Installationsdokumentation

  Es ist eine Installationsdokumentation vorhanden, um Installationen ohne Experten nachzustellen.
- Alerts müssen gemeldet werden

  Anomalien werden via Mail an die zuständigen Administratoren gemeldet.
- Web oder CLI Interface

  Es ist ein Web und/oder CLI Interface vorhanden um die Applikation zu managen.

3.2. Kann Kriterien

- Push Benachrichtigungen

  Alerts können via Push notification abgesendet/empfangen werden.
- SSO Authentifizierung

  Single-Sign-On Anbindung an bestehende SSO Lösungen.
- Multiarch

  Die Lösung soll sowohl unter x86 sowie x86_64 laufen.
- OS Independent

  Die Lösung soll keine Abhängigkeit des unterliegenden Betriebssystem haben.

3.3. Bewertungskriterien

- API

  Die Applikation besitzt ein ausführliches und umfassendes API.
- Dokumentation

  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

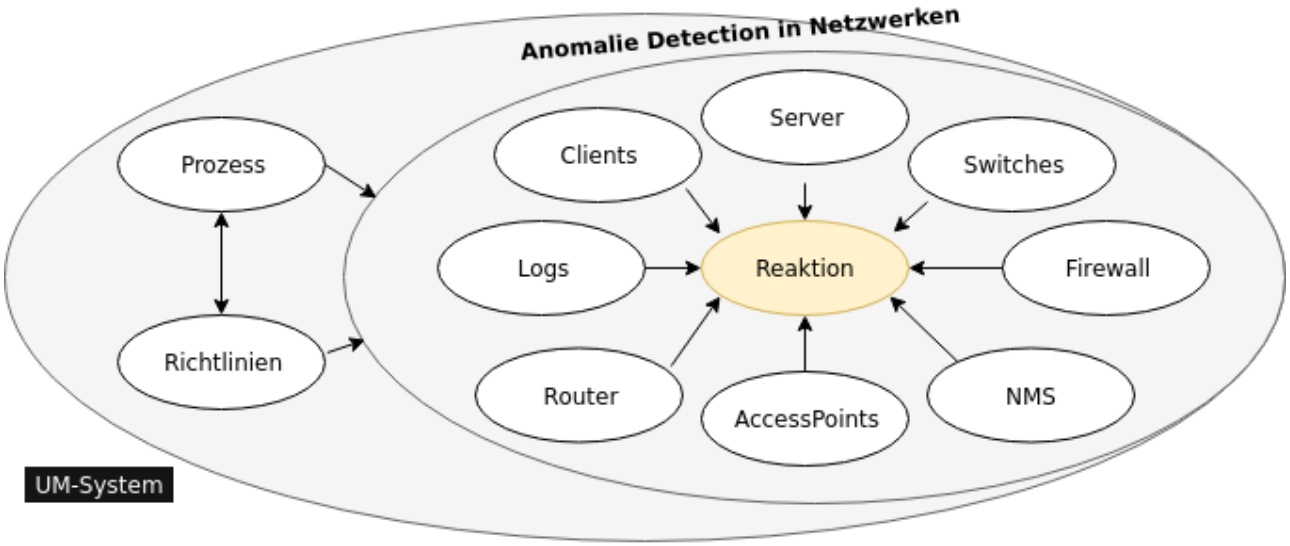
  Wie aktiv wird an der Applikation weiterentwickelt?

4. Analysetechnik

4.1. Abgrenzung

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.

4.2. Systemgrenzen



4.3. Analyse der Teilsysteme

Clients

TODO

Server

TODO

Switches

TODO

Firewall

TODO

NMS

TODO

AccessPoints

TODO

Router

TODO

Logs

TODO

4.4. Umsysteme

Prozess

TODO

Richtlinien

TODO

4.5. Schnittstellen

TODO

4.6. Systemgrenzen

TODO

5. Erhebung

5.1. 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.

TODO

5.2. Risiken

TODO

5.2.1. Risikoanalyse

6. Würdigung

6.1. IST-Zustand

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.

6.2. SWOT-Analyse

TODO

6.2.1. Rahmenbedingungen

TODO

6.2.2. Stärken/Schwächen Profil

TODO

6.2.3. Matrix

TODO

7. Lösungsvarianten

TODO

7.1. Log-Collector

TODO

7.1.1. V0 | Null

TODO

7.1.2. V1 | Graylog

TODO

7.1.3. V2 | ELK-Stack

TODO

7.1.4. SW-Bewertung

7.1.5. V-Bewertung

7.2. Network Monitoring System

TODO

7.2.1. V0 | Null

TODO

7.2.2. V1 | PRTG

TODO

7.2.3. V2 | Nagios

TODO

7.2.4. SW-Bewertung

7.2.5. V-Bewertung

8. Weiteres Vorgehen

9. Freigabe

10. Darstellungsverzeichnis

11. Glossar