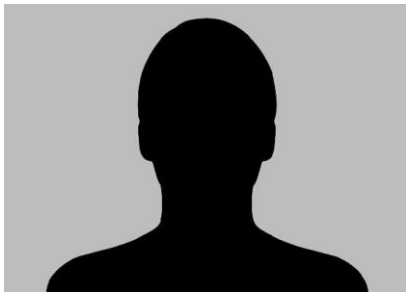
Zürcher Hochschule
für Angewandte Wissenschaften

School of Engineering

Network-based Anomaly Detection in Cloud Environments



Diplomierende
Micha Hüssy
Valentin Zahnd

Dozent
Bernhard Tellenbach

In der heutigen Zeit, in welcher immer mehr Dienste in der Cloud genutzt werden, ist es unabdingbar dass Anomalien, welche die Sicherheit und Verfügbarkeit dieser beeinträchtigen, schnell und akkurat erkannt werden. In Hinsicht auf häufig auftretende Anomalien und Cloud-spezifische "normale" Ereignisse, wie das zur Verfügung stellen und entfernen von Hosts und Diensten, soll evaluiert werden wie sensitiv verschiedene Anomaliedetektionsalgorithmen in dieser Umgebung sind. Die Daten als Basis für eine solche Evaluation sind Metainformationen, gesammelt im Schweizerischen Hochschulnetzwerk, in Form von NetFlow-Daten. Um solch eine Evaluation zu ermöglichen, müssen verschiedene Vorarbeiten durchgeführt werden. Diese werden in dieser Bachelorthesis ausgeführt.
Zuerst wurde eine Übersicht über bestehende Anomaliedetektionstechniken erarbeitet, aus welcher die vielversprechendsten Kandidaten ausgewählt wurden. Aus dieser Auswahl wurden zwei Hauptgruppen gebildet, welche sich gegenübergestellt worden sind. Zum einen wurden klassisch statistische und zum anderen neuronale Netzwerke als selbstlernende Algorithmen verglichen. Für die spätere Sensitivitätsanalyse sind aus dieser Selektion drei Algorithmen ausgewählt worden. In einem nächsten Schritt wurde eine Auswahl an Anomalien in die NetFlow-Traces injiziert. Diese bilden zusammen mit einer Baseline, in welche diese Anomalien injiziert wurden, die Basis für solche Analysen. Zuletzt wurden zwei neue Funktionalitäten zu einem Software-Framework für die Verarbeitung von NetFlow-Daten hinzugefügt. Als erstes wurde ein Modul für die Extraktion der Basismetriken, welche als Eingabe für die Anomaliedetektionsalgorithmen dienen, implementiert. Danach wurde eine Möglichkeit für die Anomalieinjektion, basierend auf einer Modellbildung durch anpassbare Konfigurationsdateien, geschaffen.

Bild klein 1.

Bild klein 2.