# Anomalie Detection in Netzwerken

Statusbericht Nr.2

Ives Schneider

## 1. Projektarbeit

Hauptsächlich befasste ich mich seit dem letzten Statusbericht damit, die Vorstudie abzuschliessen, sowie das POC Lan mit der evaluierten Software auszurüsten.

Bei der NMS Evaluation hat nun PRTG gewonnen. (Entscheidung ist ersichtlich in der Vorstudie).

Des weiteren habe ich damit angefangen, die Applikation zu programmieren. Soweit ist es noch ziemlich am Anfang, da ich mehr Zeit damit verbracht habe best practices zu studieren, als produktiv am Code zu arbeiten.

Die Entwicklung wird momentan noch im Labor zu Hause vorgenommen (SNMP wird gemockt mit SNMP Mock) und Splunk/PRTG laufen auf einem ESXi. Bisher ist die featurelist noch etwas klein (einzelne SNMP Value kann abgefragt werden), allerdings werden zusätzliche feautures schnell folgen.

## 2. Reflexion

Die restlichen Teile der Vorstudie sind relativ schnell zustande gekommen. Allerdings scheint mir, dass ich mehr Zeit in die Applikation stecken muss, um die definierte Ziele alle abdecken zu können.

Aufgrund hoher Arbeitslast, konnte ich leider nicht die gewünschte Zeit in das Projekt stecken. Allerdings sollte sich dies in den nächsten Tagen verbessern.

## 3. Zukünftig

Hauptstudie sowie Applikationsprogrammierung wird mehr oder weniger aufgrund time constraints simultan erfolgen. Installationsanleitungen werden direkt mit Beispielen im Code geschrieben und danach generiert.

Ich denke, dass ich einen grossen Teil in den Schulferien erledigen kann.