Zürcher Hochschule
für Angewandte Wissenschaften

School of
Engineering

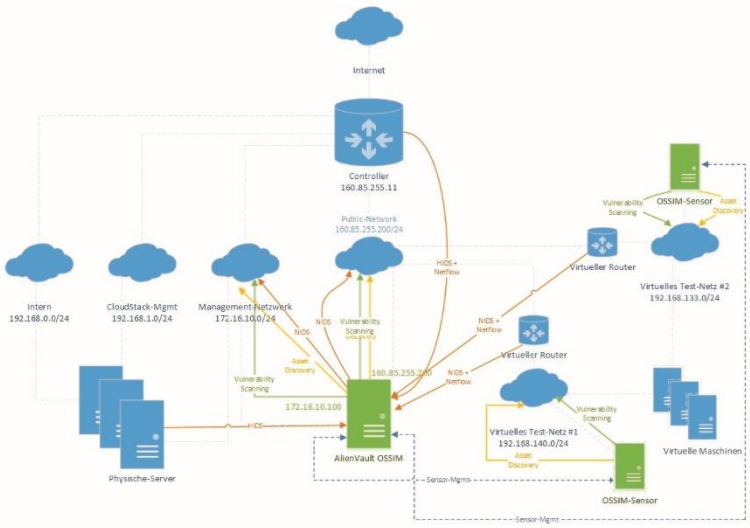
InIT Institut für angewandte
Informationstechnologie

# IAM und Security Monitoring für die Lab Infrastruktur des Schwerpunkts Information Security

Diplomand
Tobias Balschun

Dozierende
Bernhard Tellenbach
Kevin Lapagna

Das Institut für angewandte Informationstechnologie (InIT) betreibt eine Laborserverinfrastruktur, auf welcher Dienste für Lehre sowie Forschung und Entwicklung betrieben werden. In der Umgebung gibt es keine zentrale Identity- und Access-Management-Lösung (IAM) und es wird auch kein Security-Monitoring betrieben. Ziel dieser Bachelorarbeit war es, passende Lösungen für die fehlenden Teile zu evaluieren und ein Konzept zu entwickeln, welches beschreibt, wie die Lösungen in die bestehende Infrastruktur integriert werden können.
Im ersten Teil der Arbeit wurde die IAM-Lösung PrivacyIDEA evaluiert und aufbauend auf dieser ein Konzept verfasst. Dieses beschreibt, wie die Benutzer-Zugriffe zukünftig über PrivacyIDEA zentral autorisiert werden können. Dabei wird zusätzlich die Einführung einer sicheren Zwei-Faktor-Authentifizierung mit Hilfe von Yubikeys beschrieben. Die Umsetzbarkeit des Konzepts wurde anschliessend in einer Testumgebung verifiziert.Im zweiten Teil wurde das Open Source Security-Information und Event-Management-System OSSIM von AlienVault evaluiert. Aufbauend auf dieser Lösung wurde anschliessend ein Security-Monitoring-Konzept entwickelt. Das Konzept beschreibt, wie sämtliche Komponenten der Infrastruktur sowie der Netzwerk-Verkehr überwacht werden können. Die Lösung wurde während der Arbeit erfolgreich in die bestehende Infrastruktur integriert.




Darstellung der Integration von AlienVault OSSIM in die bestehende Infrastruktur inklusive zugehöriger Kommunikationsströme.