Cloud-basierte Netzwerksicherheits-Sensoren und -Aktoren

Studiengang: BSc in Informatik | Vertiefung: IT-Security
Betreuer: Prof. Hansjürg Wenger
Experte: Prof. Dr. Andreas Spichiger (Berner Fachhochschule Wirtschaft)

BeeHive - Honeypots in der Cloud steht für Sensoren und Aktoren, die bei Cloudanbietern, anhand von definierbaren Parametern automatisiert bereitgestellt und weltweit betrieben werden. Die dabei gewonnenen Daten bestehend aus Netzwerkpaketen, Log-Files und Systemzustand werden zentral gesammelt und analysiert. Eine grafische Auswertung erlaubt eine Übersicht nach gewünschten Merkmalen und Ableitung von weiteren Massnahmen für die eigene Infrastruktur.

Ausgangslage

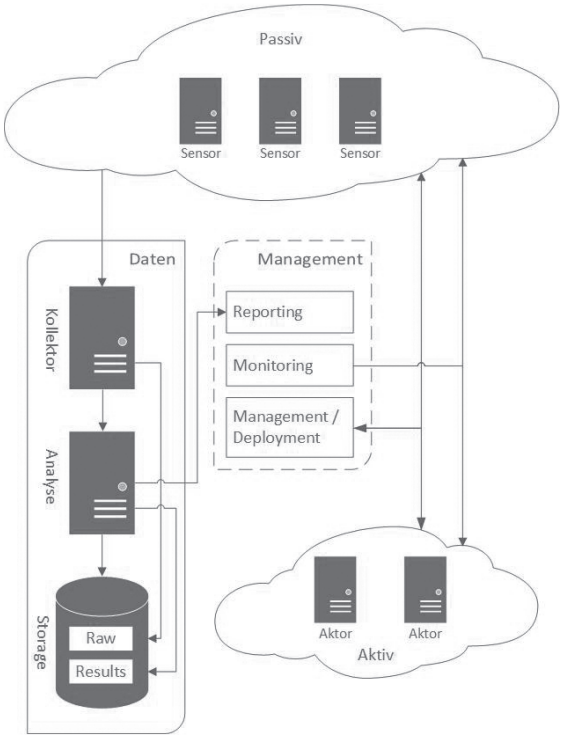
Im Rahmen dieser Arbeit soll versucht werden, passive Netzwerk-Sicherheits-Sensoren, sogenannte Honeypots, in die Cloud-Datencenter diverser weltweit operierender Cloud-Anbieter zu platzieren, Daten zu erfassen und auszuwerten. So soll es möglich sein, Bedrohungen, erhöhtes Verkehrsaufkommen oder Abnormitäten in geeigneter Form nach einer Aufbereitung darzustellen. Der Einsatz von aktiven Komponenten soll evaluiert werden, um eigene Systeme gezielt auf die gefundenen Ergebnisse zu testen und zu bewerten.

Realisierung

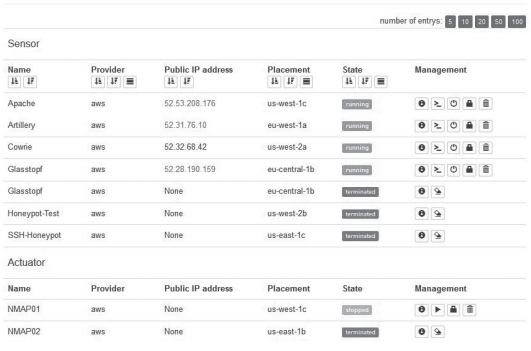
In einer ersten Phase wurden mögliche Cloud-Anbieter, für die Nutzung als Sensor geeignete Honeypots und mögliche Werkzeuge für Aktoren evaluiert. Zusätzlich wurde ein Konzept ausgearbeitet, um die anfallenden Daten zu sammeln, zu analysieren und auszuwerten. Aufgrund der Evaluation wurde Amazon Web Services (AWS) als Cloud-Anbieter ausgewählt. Auf Basis der zur Verfügung gestellten API wurde ein Web-Frontend für das Management, das einfache Deployment und die Überwachung der virtuellen Systemen entwickelt. Die Sensoren und Aktoren lassen sich so zentral und automatisch installieren und entsprechend konfigurieren. Für die Sensoren wurden diverse Webserver-, ein SSH- und ein generischer Honeypot implementiert. Die gewonnen Daten werden anschliessend zentral gesammelt und weiterverarbeitet. Je nach Zielgruppe können die Daten übersichtlich auf einem Dashboard dargestellt und ausgewertet oder zu einem Bericht zusammengefasst werden.

Erkenntnisse

Dank heutiger Cloud-Infrastrukturen können schnell weltweit Systeme installiert werden. Mithilfe unserer Implementierung lassen sich Netzwerk-basierende Angriffe feststellen und auswerten. Die gewonnen Daten sollen es zukünftig ermöglichen eigene Systeme automatisiert vor Bedrohungen zu schützen.



Konzeptioneller Aufbau



Management Frontend – Übersicht virtuelle Server

Fabian Jürg Affolter

Arthur van Ommen

Pascal von Ow