Logfile Auswertung und Metadatenanreicherung

Vortrag für Chemnitzer Linux-Tage 2016
Daniel Riegel <daniel.riegel@to.com>
Thinking Objects GmbH, https://to.com/

Log Daten geben einen Einblick in die internen Abläufe der IT-Infrastruktur eines Unternehmens. Sie bieten die Grundlage für SIEM (Security Information and Event Management) und das Erkennen von Cyber-Angriffen auf die Unternehmens-Infrastruktur. Doch wie lässt sich die Nadel im Heuhaufen finden, wenn schon in mittelständigen Unternehmen täglich Millionen von Ereignissen auftreten und Datenmengen im Gigabyte-Bereich auszuwerten sind?

Vorgestellt wird eine eine Log Management Architektur basierend auf den OpenSource Komponenten Linux, Logstash, Elasticsearch, Kibana und RabbitMQ:

- Vorstellen verschiedener Dashboards zum Visualisieren der Logs (Live-Präsentation)
- Kurzvorstellung der Gesamt-Architektur
- Herausforderungen bei der Anreicherung mit Metadaten und der Normalisierung von Logs verschiedener Quellen in Echtzeit

Schwerpunkte werden folgende Fragen sein:

- Wie überträgt und speichert man 1000 Logs/Sekunde?
- Wie gelingen reverse DNS Lookups in Echtzeit?
- Wie genau sind GeoIP Informationen?
- Wie werden Dienste (z.B. SSH, HTTPS, DNS) erkannt?
- Welche Ereignisse sind kritisch?
  Über das Zuordnen der Logs zu Security-Zonen wie DMZ und Internet.

Besucher des Vortrags sollten Erfahrung mit Linux und Netzwerken mitbringen.

Weitere Informationen:
https://en.wikipedia.org/wiki/Security_information_and_event_management
https://www.elastic.co/downloads
https://www.elastic.co/guide/index.html
https://www.rabbitmq.com/