EsperTech

Trend Micro

Threat-Detection / Event-Correlation mit Esper von Espertech Inc.

Ausgangssituation

Die Bedrohungen im Internet durch Malware, Spam und kompromittierte Websites ändern sich sehr häufig. Hersteller von Antivirensoftware müssen daher genau beobachten, ob bereits bekannte Szenarien oder neue Szenarien auftreten. Zu diesem Zweck bietet Trend Micro seinen Kunden einen sog. Web Reputation Service. Die Antivirensoftware teilnehmender Kunden kann die Reputation einer URL erfragen. Häufig werden bösartige URLs nicht direkt angesurft, sondern durch Links auf gehackten Websites oder in Spam-Mails aufgerufen. Bösartige URLs werden als Blacklist geführt. Aus diesem Grund versuchen Anbieter mit schädlichen Inhalten diese Blacklists durch ständig wechselnde und neue URLs zu umgehen. Aufgrund der hohen Dynamik und dem hohen sowie dezentralen Datenaufkommen wird das Web Reputation System als Cloud-Anwendung bei dem Dienstleister Akamai gehostet. Die Reputation bekannter URLs kann der Antivirensoftware direkt mitgeteilt werden, neue URLs werden so weltweit eingesammelt und können beurteilt werden. Die Beurteilung neuer URLs ist eine datenintensive Anwendung mit dem Anspruch, innerhalb kurzer Zeit schädliche URLs zu identifizieren. Aufgrund der hohen Datenmenge und der häufigen Änderungen kann hier von einem BigData-Problem gesprochen werden. Der Aufruf einer URL kann nicht für sich betrachtet werden, sondern steht im Zusammenhang einer Aufrufkette, deren Struktur Anhaltspunkte für die Schadhaftigkeit einer URL liefert.

Neben verschiedenen Speicherstrategien soll auch ein auf Streaming basierter CEP-Ansatz evaluiert werden. Die technische Umsetzung dieser Evaluation war Aufgabe der iTransparent GmbH.

Zur genauen Definition der Anforderungen hat die iTransparent GmbH einen Workshop in Nürnberg veranstaltet. Trend Micro hat dazu Threat-Researcher aus der ganzen Welt nach Nürnberg eingeflogen (Deutschland, Philippinen, Frankreich, Irland, USA, Niederlande), um einen Austausch von technischen Möglichkeiten eines CEP-Ansatzes und fachlichen Ansätzen des Threat Research zu gewährleisten. In diesem Workshop wurden Möglichkeiten diskutiert, die im Anschluss von iTransparent in einem Prototyp umgesetzt wurden.

TREND MICRO

Fast Facts:

Unternehmen
Trend Micro

Branche
Software

Lösung
Espertech

Ergebnis
- Internationales Projekt
- 150 000 Events pro Sekunde
- Java Performance Tuning
- Realtime Threat Analysis von unbekannten Bedrohungsszenarien im Internet

iTransparent
BUSINESS TECHNOLOGY EXPERTS

Ziele

Der Web Reputation Service bekommt von Clients aus aller Welt aufgerufene URLs, die für Trend Micro von dem Cloud-Anbieter Akamai dezentral gesammelt werden. Die dabei entstehenden Log-Dateien werden permanent zu einer zentralen Forschungsstelle des Threat Research geschickt und dort mittels Multicast allen re-levanten Projekten zur Verfügung gestellt.

Umsetzung

- Aufsetzen verketteter Esper-Instanzen (1st step: Filtern, 2nd step: corellation)
- Oracle/Sun Java Version 7 Garbage Collector Optimierung (G1)
- Implementierung von Multicast-Listener
- Serialisierung/Deserialisierung mit Protobuf
- Einbinden von ActiveMQ als Datensenke
- Multi-Threaded Anwendung im Sinne einer Staged-Event-Driven-Architecture (SEDA)
  zur vollen Ausnutzung der verfügbaren CPUs

Der erste Server mit reinen Vorfilter-Aufgaben mit 16 Kernen und 72GB Hauptspeicher war für diese Aufgabe mehr als ausreichend ausgestattet. Der zweite Server mit 24 Kernen und 144 GB Hauptspeicher wurde dagegen mit parallelen Anfragen bis zur Vollauslastung betrieben.

Resumée

Mit Hilfe zweier handelsüblicher Server konnte eine durchschnittliche Eingangsrate von 150000 Events/s verarbeitet werden. Das Vorfiltern hat etwa 15% der Events verworfen, so dass diese für die nachgelagerte Betrachtung nicht mehr relevant war. Die wesentliche Stärke von CEP-Ansätzen im Sinne einer Datenstromverarbeitung liegt darin, Events verwerfen zu können, sobald sie für die Anfragen nicht mehr von Bedeutung sind.

Kontakt

iTransparent GmbH | **Business Technology Experts**

Office Nürnberg
Bad Brückenauer Str. 23
90409 Nürnberg
T +49 (0)911- 93754499

info@itransparent.de / www.itransparent.de