WAF Logging mit Kafka

Studiengang: MAS | Vertiefung: MAS Information Technology

Als Teil von DevSecOps und als «first line of defense» ist der Einsatz von Web Application Firewalls nicht mehr wegzudenken. Gleichzeitig ist die Analyse der riesigen und unübersichtlichen Logdaten nur mit erheblichem Aufwand möglich. Die neu entwickelte Software ermöglicht, die Daten mehrerer WAFs in «near realtime» zu aggregieren und aufzubereiten.

Ausgangslage

Zur Steigerung der Effizienz und Qualität setzt die Firma Puzzle ITC GmbH auf DevSecOps und Continuous Integration (CI) and -Delivery (CD). Als «first line of defense» wird eine Web Application Firewall (WAF) eingesetzt, welche laufend überwacht wird. Zusätzlich werden Applikationen bereits vor der Auslieferung gegen das Regelwerk der WAF getestet. Die Überwachung einer WAF wird in der Regel mit der Analyse von Log-Dateien derselben sichergestellt. Allfällige Erkenntnisse fliessen zurück an die betroffenen Applikationen oder führen zu einer Anpassung des Regelwerks der WAF.

Die Analyse der riesigen Log-Dateien und die anschliessende Weiterverarbeitung der Erkenntnisse wird heute primär manuell oder mit primitiven technischen Mitteln erledigt. Es besteht das Risiko, dass kritische Einträge übersehen oder nicht rechtzeitig behandelt werden und dadurch Sicherheitsprobleme oder Betriebsbehinderungen entstehen können. Durch das manuelle Vorgehen ist die Nachvollziehbarkeit nicht gewährleistet und detaillierte Auswertungen sind nicht oder nur mit erheblichem Aufwand möglich.

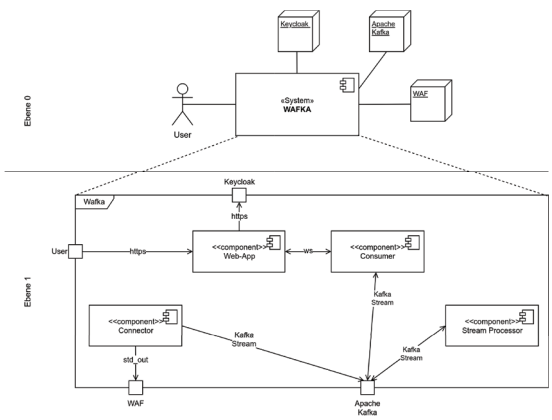
Zielsetzung

Mit dieser Master-Thesis sollte ein Software-Produkt entwickelt werden, das aggregierte Log-Einträge und gegebenenfalls weitere Daten der WAFs in «near realtime» darstellt und eine nachvollziehbare, effiziente Behandlung ermöglicht. Für die Verarbeitung und Persistierung dieser Daten soll der bestehende Apache-Kafka-Cluster von Puzzle ITC verwendet werden.

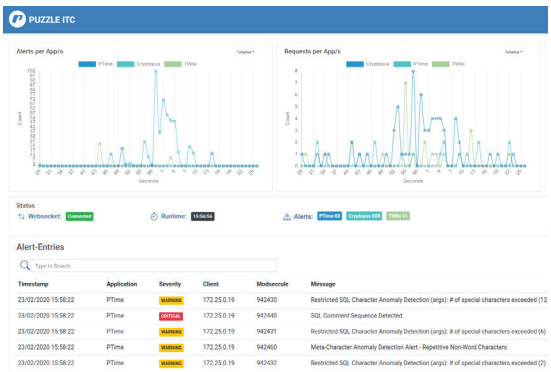
Ergebnis

Das Software-Produkt setzt sich aus verschiedenen JAVA-Komponenten zusammen, welche über den Apache-Kafka-Cluster interagieren. Im ersten Schritt werden die WAF-Logdaten mit Hilfe des Connectors in einem Kafka Topic persistiert. Mit Kafka Streams prozessiert die StreamProcessor-Komponente die unterschiedlichen Meldungstypen der WAFs und erstellt gleichzeitig eine zeitbasierte Aggregation (Windowing) als Datenbasis für die Diagrammdarstellung. Der Consumer bezieht die prozessierten Daten und stellt sie schliesslich der VueJS-Web-Applikation über Websockets bereit. Mit der neuen Software erhält der Benutzer ein praktisches Instrument, um sich einen schnellen Überblick über die aktuelle Situation der WAFs zu verschaffen. Neben den Diagrammen mit den wichtigsten Kennzahlen werden ihm alle Meldungen in einer Tabellenkomponente zur Weiterverarbeitung aufgeführt.

Stephan Girod



Architektur Bausteinsicht



Screenshot Webapplikation