Mit Riverbed AppResponse die Reaktion auf Vorfälle automatisieren

Sicherheitswarnungen, z. B. von Angriffserkennungssystemen oder protokollbasierten Alarmsystemen, wird nicht immer sofort mit der Priorität eines Vorfalls begegnet. Die Warnungen werden meistens gespeichert und bleiben dann für spätere Untersuchungen abrufbar, wenn weitere Nachforschungen erforderlich sind. Leider dauert es bei Sicherheitsvorfällen oft Wochen oder gar Monate, bis sie ihre ganze Kraft entfalten. Diese „Stillstandszeit“ bei Angriffen ist in den letzten Jahrzehnten immer länger geworden. Riverbed AppResponse APIs ermöglichen die automatische Erstellung relevanter PCAP-Dateien (Pocket Capture) zu allen betreffenden Ereignissen. Sicherheitsverantwortliche können so auf alle relevanten Pakete für alle Ereignisse zugreifen, falls weitere Untersuchungen erforderlich sind – auch, wenn das Ereignis bereits Monate zurückliegt.

Hintergrund

Ein weltweit tätiges, innovatives Biopharma-Unternehmen nutzt die gesamte Riverbed Lösung für einheitliches Network-Performance-Management (NPM) – hochpräzise Flow-Überwachung, Paketerfassung und Endpunktüberwachung. Sie wissen: *Man kann nicht verwalten, was man nicht messen kann*. Und genauso gilt: *Man kann nicht schützen, was man nicht sehen kann*. Das wollen wir uns heute genauer ansehen.

Die Paketerfassung und -analyse von Riverbed AppResponse liefert wertvolle Telemetrie für Netzwerk- und Sicherheitsbetriebsteams. Das Netzwerkbetriebsteam kann z. B. die TCP-Kennzahlen und die grafische Darstellung der Antwortzeiten nutzen, um Berichten über Probleme mit der Anwendungs-Performance nachzugehen. Das Sicherheitsbetriebsteam kann Paketdaten auswerten, die AppResponse zur Unterstützung einer Sicherheitsuntersuchung gespeichert hat.

Reaktion auf Vorfälle erfordert Paketdaten

Der Biopharma-Kunde verfolgt bei der Implementierung von AppResponse das Ziel, für jede AppResponse Appliance 24 Stunden an Paketdaten zu speichern. Das Sicherheitsteam benötigt unter Umständen einen

deutlich längeren Verlauf, insbesondere, wenn Pakete Bestandteile von IDS-/IPS-/NDR-Erkennungen sind. Manchmal sind die relevanten Pakete jedoch bereits aus dem Erfassungspuffer von AppResponse herausgefallen.

Für welche Zeiträume eine Paketerfassungslösung Pakete speichern kann, hängt von der erfassten Datenmenge und vom verfügbaren Paketspeicher der Appliance ab. AppResponse bietet eine differenzierte Kontrolle darüber, welche Pakete in den Paketspeicher geschrieben werden. Dennoch kann es sein, dass Pakete nicht verfügbar sind, wenn sie aufgrund eines Performanceproblems oder für eine Sicherheitsuntersuchung benötigt werden. Durch das Hinzufügen von mehr Paketspeicher verlängert sich zwar die Paketspeicherdauer. Die Paketdatenmenge, die gespeichert werden kann, ist jedoch immer begrenzt. Riverbed Professional Services fand eine kreative und erfolgreiche Lösung, die es dem Kunden ermöglichte, den verfügbaren Paketspeicher optimal auszunutzen.

API automatisiert Paketspeicher

Riverbed Professional Services stellte dem Sicherheitsteam des Kunden einen zweistufigen Prozess zur Paketerfassung für die Vorfallsreaktion bereit:

1. Eine neu entwickelte API ermöglicht dem Team das automatisierte Anfordern von Paketerfassungen für angegebene IP-Adressen, Ports und Zeiträume, basierend auf Ereignissen, die von den Sicherheitstools erkannt wurden. Eine Anforderung an die API liefert eine Liste von AppResponse Appliances mit Paketen, die der Anforderung zugeordnet sind.
2. Eine zweite API führt daraufhin die Anforderung an die ermittelten AppResponse Appliances durch, um die relevanten Pakete abzurufen. Dann speichert sie die Pakete zur späteren Analyse auf einem sicheren FTP-Server.

Nachdem das API-Framework installiert war, konnte der Kunde auch ein Web-Front-End für das Sicherheitsteam und andere Stakeholder erstellen. Darüber werden Paketerfassungen für angegebene IP-Adressen, Ports und Anfangs-/Endzeiten angefordert. Wenn die Anforderung geplant wurde und abgeschlossen ist, erhält der Benutzer eine E-Mail. Sie informiert ihn über den Abschluss der Anforderung und enthält einen sicheren Link zum Speicherort der angeforderten Pakete.

Vorteile für Stakeholder

Diese innovative Lösung verbessert die Agilität und die Forensik-Fähigkeiten des Sicherheitsteams durch einen automatisierten Prozess, der die Speicherung paketbasierter Evidenz für Sicherheitsereignisse und die Unterstützung weiterer Sicherheitsuntersuchungen ermöglicht. Die Lösung sorgt auch für einen höheren ROI von AppResponse für das Tools-Team: Indem die Paketspeicherdauer verlängert wird, ohne dass notwendigerweise in zusätzliche Speichereinheiten investiert werden muss, werden die Anforderungen weiterer Stakeholder erfüllt.