SCHNELLE REAKTION UND UNTERSTÜTZUNG AUF DIE ALS KRITISCH EINGESTUFTE SICHERHEITSLÜCKE LOG4J

IT-Abteilungen rund um den Globus wurden durch Bekanntwerden der Log4j-Schwachstelle in den Ausnahmezustand versetzt. Diese Sicherheitslücke in der weit verbreiteten Protokollierungsbibliothek für Java-Anwendungen wurde als extrem kritisch eingestuft.

Seit der Entdeckung gibt es eine Flut von Cyberkriminellen, die versuchen, Instanzen zu entdecken, in denen diese Schwachstelle noch existiert, um sie auszunutzen. Auch Kunden der ENTIRETEC waren von dieser Bedrohungslage betroffen und fürchteten mögliche Angriffe durch Schadsoftware oder Daten-Exfiltration.

Ein innerhalb kürzester Zeit entwickelter ENTIRETEC Service auf Basis von Infobox BloxOne Threat Defence schaffte Abhilfe und sichert fortan proaktiv die Infrastrukturen unserer Kunden.

HERAUSFORDERUNG

- Identifizieren von kritischen Log4j-Aktivitäten
- Schnellstmögliches Beheben der Schwachstelle
- Unterbindung nachgelagerter Aktivitäten eines Angriffs
- Überwachung des Sicherheitsstatus von Log4j

LÖSUNG

- ENTIRETEC Service auf Basis von Infoblox BloxOne Threat Defence

ERGEBNIS

- 24x7 Überwachung des Log4j-Sicherheitsstatus durch Experten als zusätzliche Absicherungsschicht
- Tiefe Einblicke zu den Netzwerkaktivitäten auf DNS-Ebene
- Schnelle Reaktion und Eindämmung bei möglichen Angriffen

DIE HERAUSFORDERUNG

Nach Bekanntwerden der kritischen Sicherheitslücke in der Java-Bibliothek Log4j wurde ENTIRETEC von Kunden angefragt, ob wir sie mit einer wirksamen Sicherheitslösung zur Bewältigung der Log4j-Sicherheitsverletzung unterstützen könnten.

Ziel war es, die IT-Teams unserer Kunden beim Erkennen von Log4j-Aktivitäten zu unterstützen, eventuelle Angriffe zu verhindern und auch nachgelagerte Aktivitäten eines Angriffs zu unterbinden z.B. das Aktivieren von Malware oder Exfiltration von Daten.

DIE LÖSUNG

ENTIRETEC hat umgehend mit der Entwicklung einer möglichen Lösung begonnen. Innerhalb von 4 Tagen konnten wir unseren Kunden einen Service auf Basis von Infoblox BloxOne Threat Defense anbieten, diesen ohne Verzögerung installieren und 24x7 betreiben.

Erfahrene Experten des ENTIRETEC Security Teams prüfen seitdem regelmäßig und rund um die Uhr den aktuellen Sicherheitsstatus von Log4j. Verdächtige DNS-Verbindungen werden frühzeitig erkannt und unmittelbar geblockt, so dass Angreifer keinen Zugriff auf sensible Kundendaten erlangen. Auf diese Weise wird das Risiko von Data Exfiltration oder Data Infiltration von Schadsoftware via DNS minimiert. Die Lösung integriert sich nahtlos in die bestehende Kunden-Infrastruktur. Eine proaktive Information der Kunden über den aktuellen Sicherheitsstatus schafft absolute Transparenz. Im Bedarfsfall ist eine lückenlose Eskalationskette zum Security-Team des Kunden etabliert.

DAS ERGEBNIS

Der ENTIRETEC Service auf Basis von Infoblox BloxOne Threat Defence ermöglicht unseren Kunden eine kontrollierte Situation im Umgang mit der Log4j-Sicherheitslücke, die uns, wie Experten* voraussagen, noch über Wochen und Monate hinweg beschäftigen wird.

Technisch gewährt die Lösung tiefe Einblicke zu den Netzwerkaktivitäten auf DNS-Ebene. Im Fall eines erkannten Log4j-Vorfalls erfolgt eine 24x7 eine schnelle Reaktion und Eskalation.

Die Integration der Sicherheitslösung in ein Security Information and Event Management (SIEM) sowie die Einbindung der Serviceprozesse zu einem Security Operation Center (SOC) Provider verstärken darüber hinaus das Sicherheitsszenario.

> "Die Infoblox-Lösung kombiniert mit unserer 24x7 Überwachung bietet unseren Kunden eine zusätzliche Absicherungsschicht und lässt IT-Verantwortliche nachts wieder ruhiger schlafen.
>
> René Schiller, Teamlead Solution Architecture & Service Portfolio Management, ENTIRETEC AG

* heise online „Schutz vor schwerwiegender Log4j-Lücke", 13.12.2021

ENTIRETEC ist ein weltweit agierender Managed Services Anbieter und Spezialist für Netzwerk- und Security-Technologien. Branchenübergreifend unterstützen wir globale Geschäftsstrategien unserer Kunden mit hochverfügbaren und sicheren IT-Lösungen und kombinieren diese maßgeschneidert zu zukunftsfähigen Antworten für Digitalisierung, Mobilität, Cloud und IoT.

® ENTIRETEC | www.entiretec.com | mail@entiretec.com | +49.351.41355.0