DREIFACH ABGESICHERT GEGEN ATTACKEN MIT MANAGED DETECTION AND RESPONSE, MICROSOFT SENTINEL UND SASE

Mit mehr als 100 Jahren Erfahrung in der Entwicklung und Herstellung von Automatisierungslösungen, Fertigungssystemen und Zerspanungswerkzeuge für Kunden auf der ganzen Welt ist das Schweizer Unternehmen Mikron für seine hochpräzisen Produkte bekannt, die eng mit der Schweizer Innovationskultur verbunden sind.

> Die SASE Sensoren beobachteten die Malware, so konnten wir eine Verbreitung quasi sofort unterbinden. Wären wir nicht durch die Open Systems Solution benachrichtigt worden, hätte der Angriff ein katastrophales Ausmass annehmen können.

Rolando Galeazzi, Mikron CISO

DIE HERAUSFORDERUNG

- Zu viele Cybersecurity Anbieter im Markt
- Nicht genügend Security Fachkräfte
- Alert-Flut schwer zu handhaben
- Angriffsrisiko zu hoch

DIE LÖSUNG

- Einheitliche Lösung: SASE SD-WAN + Microsoft Azure Sentinel + MDR
- 24x7 SOC

DAS RESULTAT

- Fokus auf reale Bedrohungen
- Verwertbare Angriffsinformationen
- Unmittelbare und effiziente Reaktion durch das SOC von Open Systems
- Massive Reduktion des Angriffsrisikos und der -verbreitung von Malware bei Mikron

Für eine Sache will das Unternehmen aber natürlich nicht stehen: Anfälligkeit für Cyber-Attacken. Gelingt ein solcher Angriff, könnten IT-Systeme lahmgelegt, Kundendaten und geistiges Eigentum gestohlen oder die Produktion beeinträchtigt werden.

Um Bedrohungen wie diese zu bekämpfen „bauen wir seit zwei Jahren unsere Sicherheitsinfrastruktur auf und sind von mehreren Drittanbietern zu einem einzigen Anbieter gewechselt“, sagt CISO Rolando Galeazzi.

Dieser Anbieter war Microsoft. Wie viele Unternehmen setzte Mikron auf das Microsoft Azure Sentinel SIEM (Security Information and Event Management), als Teil seiner Microsoft 365 E5-Lizenz. Galeazzi sah sich allerdings bald einer Flut von Alerts gegenüber, wodurch es ihm immer schwerer fiel, ernstzunehmende Bedrohungen unter den vielen nichtigen Meldungen zu erkennen. Da so viele Warnungen eingingen, war es unmöglich, rund um die Uhr mitzuhalten, geschweige denn effizient auf Bedrohungen zu reagieren.

WAS FEHLTE: MANAGED DETECTION AND RESPONSE

Mikron arbeitete bereits mit der SASE-Plattform von Open Systems für ein sicheres, cloudbasiertes SD-WAN. Galeazzi erfuhr, dass der Managed Detection and Response (MDR) Service von Open Systems auf Sentinel aufbaut. Dadurch konnte er Mikrons Microsoft-Investition weiterhin nutzen, und so mit aufeinander abgestimmten Anbietern eine nahtlose Integration zwischen Sentinel und SASE ermöglichen.

Diese dreifache Integration bedeutet, dass die SOC-Analysten von Open Systems die Ermittlungsarbeit leisten und auf Bedrohungen reagieren, obwohl sie ausserhalb des Netzwerks agieren. Ihr Zugang zum Netzwerk und ihr unmittelbares Eingreifen tragen dazu bei, die Ausbreitungszeit der Angriffe zu minimieren und so den potenziellen Schaden zu mindern.

„In Sachen Sicherheit bin ich auf mich allein gestellt. Mein IT-Team besteht aus unseren Infrastruktur Leuten; ihre Hauptaufgabe besteht nicht darin, Alerts zu sortieren. Der Zweck dieser Integration ist ein 24x7 Security Operations Center (SOC), da eine einzelne Person nicht 24 Stunden am Tag verfügbar sein kann“, sagt Galeazzi.

ERKENNUNG UND REAKTION IM ERNSTFALL

Galeazzi stellt fest, dass er durch die Anreicherung der Sentinel-Daten der Open Systems SOC-Ingenieure eine bessere Übersicht über mögliche Bedrohungen erhält. Galeazzi sagt: „Sentinel ist der Mittelpunkt des Gesamtbildes, Open Systems macht die Nutzung möglich.“

Open Systems ist in der Lage, die False-Positive Raten durch Anreicherung, Korrelation und weitere Untersuchungen zu reduzieren, um die „Alert-Fatigue“ zu verhindern und wertvolle Zeit für die Kunden zu sparen.

„Die Benachrichtigungen vom Defender enthalten reine Informationen. Open Systems ist in der Lage, Alerts mit zusätzlichen, von Fachkräften gesammelten Daten anzureichern und in einen Kontext zu stellen. Am Ende kann man so viel künstliche Intelligenz einsetzen wie man will, aber man braucht immer noch die menschliche Komponente“, sagt Galeazzi.

WENN ES SCHNELL GEHEN MUSS

72 Stunden: Mikrons durchschnittliche Zeit für Security Change Requests vor dem Wechsel zu Open Systems.

15–30 Minuten: Mikrons durchschnittliche Zeit für Security Change Requests nach dem Wechsel zu Open Systems.

Der Wechsel zu einem einheitlichen Managed Detection and Response ist Teil eines grösseren Trends, weg von der „Best of Breed“-Ära der Sicherheit, die im Cloud-Zeitalter nicht mehr funktioniert.

„In naher Zukunft wird diese Integration Standard sein“, sagt Galeazzi. „Es ist nutzlos, wenn die Protokolle zwischen Standort und Cloud hin- und her fliessen. Es ist am besten, sie nur an einem Ort aufzubewahren. Managed Security Provider werden sich der Verlagerung zu cloudbasierten SIEMs stellen müssen – oder den Anschluss verlieren“.

Mikron muss sich dank einer vorausschauenden und integrierten Lösung nun keine Gedanken mehr um Cybersecurity machen.