KUNDENSTORY **MIKRON**

ABGESICHERT GEGEN ATTACKEN **MIT SASE**

open-systems.com

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

- Nicht genügend Security Fachkräfte
- Alert-Flut schwer zu handhaben
- Angriffsrisiko zu hoch

DIE LÖSUNG

- Einheitliche Lösung: SASE SD-WAN + Microsoft Sentinel
- 24x7 Operations

DAS RESULTAT

- Fokus auf reale Bedrohungen
- Verwertbare Angriffsinformationen
- Unmittelbare und effiziente Reaktion durch Open Systems

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“, sagt CISO Rolando Galeazzi.

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.

EINE EINZELNE PERSON KANN NICHT 24 STUNDEN AM TAG VERFÜGBAR SEIN

Mikron arbeitete bereits mit der SASE-Plattform von Open Systems für ein sicheres, cloudbasiertes SD-WAN. Galeazzi erfuhr, dass er Mikrons Microsoft-Investition weiterhin nutzen, und so mit aufeinander abgestimmten Anbietern eine nahtlose Integration zwischen Sentinel und SASE ermöglichen.

Die Analysten von Open Systems leisten die Ermittlungsarbeit leisten, 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. Eine einzelne Person kann nicht 24 Stunden am Tag verfügbar sein“, sagt Galeazzi.

„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.

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

> **Mein IT-Team besteht aus unseren Infrastruktur Leuten; ihre Hauptaufgabe besteht nicht darin, Alerts zu sortieren.**
>
> **Rolando Galeazzi,** Mikron CISO