Vier Fragen entscheiden über mehr Cyber-Resilienz

Plattform-Endpoint-Schutz wird zur strategischen Weichenstellung

Die Mehrheit der Unternehmen weltweit setzt inzwischen Lösungen zum Schutz ihrer Endpunkte ein. Branchenweit wird dafür mit ähnlichen Attributen wie „KI-gestützt“, „Next-Gen“ oder „integriert“ kommuniziert. Doch es bestehen erhebliche Unterschiede, insbesondere, wenn Unternehmen von reiner Prävention zu strategischer und ganzheitlicher Detection & Response übergehen, um die Resilienz zu stärken.

Dass Resilienz ein Top-Thema in jedem Unternehmen sein sollte, belegen die aktuellen Studienergebnisse von Sophos: Laut dem Sophos State of Ransomware Report 2025 lag die durchschnittliche Lösegeldsumme nach einem Ransomware-Angriff bei rund einer Million US-Dollar und bei weiteren 1,5 Millionen Wiederherstellungskosten on-top. Zudem zeigt der Sophos Threat Report 2025, dass Ransomware etwa 70 Prozent der Sophos Incident Response-Fälle bei kleinen Unternehmenskunden ausmachte. Bei mittelständischen Unternehmen von 500 bis 5000 Mitarbeitern lag dieser Wert sogar bei über 90 Prozent.
Diese Zahlen unterstreichen: Der Schutz von Endpunkten ist kein reines IT-Thema mehr, sondern eine strategische Architekturfrage, die über die Cyber-Resilienz eines Unternehmens entscheidet.

Plattformdenken statt Features
Moderne Endpoint Protection geht weit über die bloße Abwehr einzelner Bedrohungen hinaus. Entscheidende Differenzierungsmerkmale liegen in der Datenqualität der Telemetrie, der Architektur und der Integrationsfähigkeit der Sicherheitsplattform.
Moderne Sicherheitsplattformen wie Sophos XDR (Extended Detection and Response) nutzen KI-gestützte Workflows, umfassende Integrationen und eine einheitliche Sicht auf die gesamte IT-Infrastruktur, um Bedrohungen effizient zu identifizieren und darauf zu reagieren.

„Die Zeiten, in denen einzelne Sicherheitsprodukte ausgereicht haben, sind vorbei. Cyber-Resilienz entsteht heute durch eine ganzheitliche, lernfähige Plattformarchitektur, die Prävention, Erkennung und Reaktion intelligent verbindet“, sagt Michael Veit, Security-Experte bei Sophos. „Unternehmen, die ihre Sicherheit dynamisch orchestrieren, reagieren schneller und können Angriffe stoppen, bevor sie Schaden anrichten.“

Wichtige Fragen zur Entscheidung für eine moderne Sicherheitsplattform sind:
- **Volumen:** Wie viel Telemetrie wird erfasst? Erkennen Sie reales Angreiferverhalten im globalen Maßstab, das heißt neben Malware auch „Hands-on-Keyboard“-Angriffe, Toolmissbrauch oder persistente Techniken?
- **Vielfalt:** Sieht die Plattform nur Endpoints oder hat sie auch E-Mails, Netzwerke, Cloud-Dienste und Identitäten im Blick? Kommen die Daten aus unterschiedlichen Regionen, Branchen und Sicherheitsreifegraden?
- **Geschwindigkeit:** Wie schnell werden Daten verarbeitet und aktualisiert? Lernen Ihre Modelle aus neuen Bedrohungen in Stunden oder erst nach Tagen?
- **Verlässlichkeit:** Können Sie den Daten vertrauen? Werden sie mit Threat Intelligence angereichert und durch reale Vorfälle verifiziert?

Von Prävention zur Resilienz
Der Endpoint ist oft die erste und beste Gelegenheit, Angriffe zu stoppen. Eine moderne Sicherheitsarchitektur ermöglicht es, diesen Schutz auf E-Mail, Netzwerk, Cloud und Identität

auszuweiten. So entsteht eine durchgängige Detection & Response-Strategie, die eine Ausbreitung verhindert und kritische Systeme schützt.
Damit sinken Risiken, verkürzen sich Erkennungszeiten und werden Reaktionen schneller. Und falls im Unternehmen die Expertise oder das Personal fehlt, lassen sich rund um die Uhr verfügbare Managed Detection and Response Services (MDR) direkt in die Plattform integrieren.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, Senior PR-Manager EMEA Central
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de