Fünf Grundlagen für das Cybersicherheitsprogramm der Zukunft

Mit wenigen fundamentalen Grundsätzen können Organisationen ihre Cyberrresilienz in einer sich ständig ändernden Bedrohungslandschaft maßgeblich stärken.

Knapp zwei Tage – so lange ist die durchschnittliche Dauer, die Cyberkriminelle benötigen, um eine Schwachstelle auszunutzen. Um mit diesen äußerst agilen Bedrohungsakteuren Schritt zu halten, bestimmen die heute getroffenen Entscheidungen die Fähigkeit eines Unternehmens, auf aktuelle und künftige Bedrohungen zu reagieren.

Damit Unternehmen aller Branchen und Größen bestmöglich gegen Cybergefahren gewappnet sind, hat Sophos fünf grundlegende Bausteine für eine Cybersicherheitsstrategie aufgestellt. Sie bilden die Grundlage für einen Cyberschutz, der den Anforderungen an die Security standhält.

1. Die Bedrohungslandschaft verstehen
Von der organisierten Kriminalität über Hacktivisten bis hin zu staatlich gesponserten Akteuren – die heutige Bedrohungslandschaft ist komplex und schnelllebig. Der Ausgangspunkt für eine erfolgreiche Cybersicherheitsstrategie ist ein tiefes Verständnis der sich verändernden Bedrohungslandschaft, um die spezifischen Sicherheitslücken des eigenen Unternehmens zu erkennen und geeignete Maßnahmen dagegen zu ergreifen.
Das Verständnis der Bedrohungslandschaft ist eine 24x7-Aufgabe, die eine kontinuierliche Überwachung und Analyse der Aktivitäten von potenziellen Bedrohungsakteuren erfordert. Das klingt nach viel Aufwand, doch Unternehmen müssen dies glücklicherweise nicht alleine stemmen. Erfahrene und vertrauenswürdige Sicherheitspartner können das Fachwissen, die Prozesse und die Technologie bereitstellen, damit Unternehmen ein besseres Verständnis für gängige Angriffsvektoren, -techniken und -taktiken entwickeln und erkennen.
Um die Risiken im Kontext zu verstehen und sie im Laufe ihrer Entwicklung anzugehen, benötigen Unternehmen umfassende Transparenz über die gesamte Angriffsfläche. Eine offene XDR-Plattform (Extended Detection and Response) bietet dafür den ganzheitlichen Überblick über die Systeme, Daten und Prozesse, um das Risiko der Bedrohungen zu minimieren.
Darüber hinaus sind umfassende Informationen für eine dynamische und widerstandsfähige Sicherheitslage entscheidend. Effektive Threat Intelligence-Systeme nutzen menschliches Fachwissen, KI und Analysen, um Angriffsmuster zu analysieren und die Security-Strategie kontinuierlich zu verfeinern.

2. Angriffe im Kontext verstehen
Der Kontext eines Angriffs ist der Schlüssel zum besseren Verständnis und zur Anwendung des gewonnenen Wissens über Bedrohungen. Selten treten Bedrohungen isoliert auf. Sie wirken sich übergreifend auf das Umfeld des Unternehmens aus. Dazu gehören Prioritäten für das Business, Abhängigkeiten in der Lieferkette und IT-Systeme ebenso wie gesetzliche Vorschriften und sozioökonomische Aspekte. Die Kontextualisierung von Bedrohungen mit Erkenntnissen über interne und externe Faktoren verbessert die Fähigkeit eines Unternehmens, Angriffe zu antizipieren und zu entschärfen.

3. Raum für Veränderung
Um ihre Ziele zu erreichen, erfinden sich Cyberkriminelle ständig neu und ändern ihre Strategie kontinuierlich. Um hier Schritt zu halten – oder im Idealfall einen Schritt voraus zu sein – müssen Unternehmen die Cyberkriminellen mit einer Cybersicherheitsstrategie schlagen, die ebenso flexibel und anpassungsfähig wie die Bedrohungen selbst ist. Ein

Sicherheitsprogramm mit hoher Flexibilität und Skalierbarkeit wächst nahtlos mit dem Unternehmen mit und passt sich ständig an die sich ändernden Bedingungen an.

4. Bedeutung des menschlichen Faktors
Zusätzlich zur technischen und KI-gestützten Sicherheit ergänzt das menschliche Fachwissen die Verteidigung des Unternehmens um eine wichtige Sicherheitsebene. In diesem Zusammenhang gilt es zu beachten, dass Mitarbeiter bei mangelnder Schulung und Sensibilisierung schnell zu einem Einfallstor für Cyberangriffe werden können. Laut dem Sophos State of Ransomware Report 2025 sind 63 Prozent der Unternehmen Opfer von Ransomware geworden, weil es ihnen an Fachwissen/ Mitarbeitern mangelt.

5. Verbesserte Geschwindigkeit und Agilität
Geschwindigkeit und Agilität sind in der heutigen Bedrohungslandschaft nicht verhandelbar, da die Verweilzeiten der Cyberkriminellen immer kürzer werden und sie immer kreativer vorgehen. Zudem haben auch die Bedrohungsakteure KI, die ihnen beim schnellen Skalieren und beim raschen Zuschlagen hilft. Darüber hinaus verfügen auch sie über die Technologie, Infrastruktur und Ressourcen, um sich kontinuierlich anzupassen und zu verändern.

Die Zukunft wird nicht unbedingt unsicher sein. Unternehmen können den Cyberkriminellen dann einen Schritt voraus sein, wenn sie Technologie, Intelligenz und Fachwissen sinnvoll kombinieren und in eine Cybersicherheitsstrategie einbetten.

Ausführlicher lassen sich diese Grundlagen zur Cyber-Resilienz hier noch einmal nachlesen.

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