Welche Rolle spielt der Mensch für moderne Cybersecurity?

In einer sich ständig verändernden Bedrohungslandschaft spielt auch das menschliche Verhalten eine bedeutende Rolle – einerseits positiv als Verstärkung in der Abwehr, andererseits negativ als Türöffner für Cyberkriminelle. Ein schwieriger Balanceakt, für den es allerdings effektive Lösungen gibt.

Sicherheitstechnologien entwickeln sich stetig weiter – und mit ihnen die Taktiken von Cyberkriminellen, die Schwachstellen bei Maschinen und Menschen ausnutzten, um unerlaubten Zugang zu Systemen zu bekommen. In der ersten Hälfte von 2023 stellte sich im Sophos Cybersecurity Report heraus, dass kompromittierte Zugangsdaten die Hauptursache für 50 Prozent aller Attacken waren. Für Unternehmen bedeutet das, jenseits der Implementierung von Sicherheitslösungen einen Schritt weiter in Richtung Datensicherheit zu gehen.

Neben den gängigen Maßnahmen wie Nutzung von Multi-Faktor-Authentifizierungen (MFA), regelmäßigem Überwachen von Schwachstellen und Updates plus Schulungen sollten Unternehmen auch folgende Bereiche auf dem Radar haben: innovative Lösungen für das Identitätsmanagement, Monitoring des Nutzerverhaltens und Datenverlust-Prävention (DLP). Auch die Einbindung von KI-gestützten Verhaltensanalysen gehört genauso dazu wie moderne Verschlüsselungstechniken, denn sie können im Wettlauf mit Cyberkriminellen der entscheidende Schritt voraus sein.

Eine gründliche Sicherheitsstrategie verlangt einen kooperativen Ansatz, bei dem Einzelpersonen, Unternehmen und Gemeinschaften zusammenarbeiten, um eine widerstandsfähige Cybersicherheitskultur zu gewährleisten. Zwar ist es wichtig, über die richtigen Instrumente für die Cybersicherheit zu verfügen, doch war es noch nie so wichtig wie heute, den menschlichen Aspekt des Cyberrisikos zu berücksichtigen. Die Betonung von Training, Bewusstsein und technologischen Innovationen bildet den Mittelpunkt des Schutzschildes gegen Cyberbedrohungen. Durch die Ausbildung einer aufmerksamen und informierten Belegschaft können Unternehmen Risiken erheblich reduzieren und Vermögenswerte schützen.

Den menschlichen Faktor verstehen

Technischer Vorsprung und die wachsende Einführung von CSaaS (Cybersecurity-as-a-Service) zeigen: Die erfolgreichsten Angriffe erfordern eine Bedrohungsjagd, Untersuchung und Reaktion, die von Menschen geführt wird. Sie befinden sich im Zentrum von Cybersicherheit, sei es im IT-Team, bei einem Managed Service Provider (MSP) oder auch bei den Mitarbeitern. Unternehmen müssen diese Punkte bedenken und sich gegen jegliche Art von Risiko durch Personen schützen, die die Tür für Cyberkriminelle öffnen könnten.

Ein Musterbeispiel ist der kürzliche Angriff auf die Hotelgruppe MGM Resorts International. Die Cyberkriminelle-Gruppe „Scattered Spider“ war in der Lage, mithilfe gefälschter Telefonanrufe Mitarbeiter zu täuschen, um in den Besitz von Login-Daten zu gelangen und anschließend Ransomware einzusetzen, die den Betrieb unterbricht. Durch Social Engineering konnte die Gruppe das Personal im Informationsbereich dazu bringen, alle MFA-Technologien zurückzusetzen und sich als Benutzer des Unternehmens auszugeben.

Cyberkriminelle nutzen zunehmend das Vertrauen der Menschen aus, besonders angesichts der rapiden Entwicklung von künstlicher Intelligenz (KI) und maschinellem Lernen. KI-

betriebene, personalisierte Scams sind weitaus schwerer zu erkennen, selbst für die am besten vorbereiteten Angestellten.

Schutz vor Bedrohungen

Nutzer-Training ist weiterhin ein wichtiges Element der Cyberabwehr eines Unternehmens. Und es liegt in der Verantwortung jedes Einzelnen zu gewährleisten, dass sie den Kriminellen nicht zufällig doch Eintritt verschaffen. Unternehmen sollte ihre Belegschaft mit Basiskenntnissen und Fähigkeiten zum Entdecken und Verhindern von Angreifer-Taktiken, -Techniken und -Prozeduren (TTPs) ausstatten.

Es ist keine Überraschung, dass die Technologie immer mehr in den Mittelpunkt der Unternehmenstätigkeit rückt, wenn es um die Datensicherheit im Betrieb geht, allerdings muss diese verantwortlich von einem kompetenten Anwender eingesetzt werden. Angesichts der zunehmenden Gefahren für Organisationen, wenden sich viel an Managed Service Provider (MSP) zur Stärkung ihrer Sicherheitsstrategie. In der heutigen Bedrohungslandschaft ist die „Ein Schritt voraus“-Taktik immer schwieriger für interne Teams zu handhaben, so dass gegenwärtig 93 Prozent der Organisationen schon grundlegende Sicherheitsmaßnahmen für eine Herausforderung halten. Bei der Zusammenarbeit mit einem MSP können Unternehmen nicht nur von den Vorteilen der Next-Gen Lösungen profitieren, sondern auch eine Fülle an Kenntnissen und Expertise nutzen, die für den entscheidenden Vorsprung gegenüber den Angreifern unerlässlich ist. Sie können sich darauf verlassen, dass für sie engagierte Bedrohungsjäger und Sicherheitsspezialisten rund um die Uhr auf Bedrohungen achten.

Aktuelle Bedrohungen erfordern einen kollaborativen Ansatz
Der menschliche Faktor in der Cybersicherheit ist entsprechend weiterhin eine wichtige Komponente, die die Sicherheitsposition eines Unternehmens stärken oder schwächen kann. Für eine effektivere und vollständigere Abwehr aktueller Gefahren ist ein proaktiver Ansatz nötig, der technologische Lösungen und menschliches Verständnis kombiniert. Einzelne Organisationen und Gemeinschaften müssen zusammenarbeiten, um bewährte Verfahren zu fördern und sicherzustellen, dass sie über die erforderlichen Fähigkeiten und Kenntnisse verfügen, die zur allgemeinen Sicherheitshygiene der Organisation beträgt.

Eine proaktive Sicherheitsstrategie gewährleistet, dass Unternehmen für die Risiken, die ihnen durch unbedachtes Fehlverhalten Einzelner entstehen können, vorbereitet sind. Einfache Fehler zu vermeiden wird entscheidend sein, denn diese zu übersehen, kann in einer Katastrophe enden.

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

Über Sophos

Sophos ist ein weltweit führender und innovativer Anbieter von fortschrittlichen Cybersecurity-Lösungen, darunter Managed Detection and Response (MDR)- und Incident-Response-Dienste. Das Unternehmen bietet ein breites Portfolio an Endpoint-, Netzwerk-, E-Mail- und Cloud-Sicherheitstechnologien, das bei der Abwehr von Cyberangriffen unterstützt. Als einer der größten auf Cybersecurity spezialisierten Anbieter schützt Sophos mehr als 500.000 Unternehmen und mehr als 100 Millionen Anwender weltweit vor aktiven Angriffen, Ransomware, Phishing, Malware und vielem mehr.
Die Dienste und Produkte von Sophos werden über die cloudbasierte Management-Konsole Sophos Central verbunden und vom bereichsübergreifenden Threat-Intelligence-Expertenteam Sophos X-Ops unterstützt. Die Erkenntnisse von Sophos X-Ops erweitern das gesamte Sophos Adaptive Cybersecurity Ecosystem. Dazu gehört auch ein zentraler Datenspeicher, der eine Vielzahl offener APIs nutzt, die Kunden, Partnern, Entwicklern und anderen Anbietern von Cybersecurity und Informationstechnologie zur Verfügung stehen.
Sophos bietet Cybersecurity-as-a-Service für Unternehmen an, die vollständig verwaltete, schlüsselfertige Sicherheitslösungen benötigen. Kunden können ihre Cybersecurity auch direkt mit der Security Operations Platform von Sophos verwalten oder einen hybriden Ansatz verfolgen, indem sie ihre internen Teams mit Sophos Services ergänzen, einschließlich Threat Hunting und Systemwiederherstellung.
Sophos vertreibt seine Produkte über Reseller und Managed Service Provider (MSPs) weltweit. Der Hauptsitz von Sophos befindet sich in Oxford, U.K.
Weitere Informationen unter: www.sophos.de

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
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