Sophos härtet Active-Adversary-Sicherheit mit 3 neuen Lösungen

Sophos stellt neue Lösungen und Optionen für die Sophos Firewall, Sophos NDR sowie Sophos XDR vor.

Wiesbaden, 14. November 2023 – Sophos stellt drei neue Produkte und Erweiterungen vor, die sich gezielt gegen Active Adversaries und damit insbesondere gegen aktive, persönliche und menschlich getriebene Attacken von Cyberkriminellen richten. Die drei Neuheiten umfassen eine neue Version der Sophos Firewall, neue Sophos Network Detection and Response (NDR)-Optionen sowie das erweiterte Sophos Extended Detection and Response (XDR).

„Angesichts schnell agierender Angreifer, die ihre Taktiken, Techniken und Vorgehensweisen (TTPs) ständig weiterentwickeln und oft legitime Tools für ihre mehrstufigen Angriffe einsetzen, muss die Cybersecurity-Abwehr dynamisch und vorausschauend sein“, sagt Raja Patel, Chief Product Officer bei Sophos. „Sophos verfolgt einen proaktiven Schutzansatz, um Bedrohungen bereits am Einfallstor zu stoppen, noch bevor sie sich verbreiten und ausweiten. Wir entwickeln Produkte mit branchenweit einzigartigen Sicherheitsfunktionen, die auf den detaillierten Bedrohungsdaten der Sophos X-Ops von mehr als einer halben Million Unternehmen weltweit basieren. Damit können wir Bedrohungen schnell und umfassend erkennen und abwehren."

Zu den Sophos Neuheiten gehören:

Sophos Firewall v20
Die neue Sophos Firewall v20 Software mit Active Threat Response eliminiert Angriffe automatisch, ohne dass Firewall-Regeln hinzugefügt werden müssen. Sie verhindert damit, dass Cyberkriminelle unerkannt in Netzwerke eindringen können. Wenn Administratoren beispielsweise auf einen Cobalt Strike Beacon aufmerksam gemacht werden, können sie das Ziel zur Ad-hoc-Blockierungsliste hinzufügen, wodurch das komplette Netzwerk am Zugriff auf diese IP-Adresse, Domain oder URL gehindert wird. Die neue Version der Sophos Firewall Software enthält außerdem ein integriertes Zero Trust Network Access (ZTNA)-Gateway. ZTNA erleichtert es Unternehmen, einen modernen und sicheren Remote-Zugriff auf Anwendungen hinter der Firewall zu ermöglichen. Gleichzeitig bietet ZTNA deutliche Verbesserungen für die Netzwerkskalierbarkeit verteilter Unternehmen sowie für die Benutzerfreundlichkeit bei der Verwaltung.

Sophos Network Detection and Response (NDR)
Sophos Network Detection and Response (NDR) ist jetzt für Kunden von Sophos Extended Detection and Response (XDR) und Sophos Managed Detection and Response (MDR) verfügbar, um die Threat-Detection-Funktionen auf das Netzwerk auszuweiten. Sophos NDR überwacht die Aktivitäten innerhalb des Netzwerks auf verdächtige und schädliche Datenverkehrsmuster, die auf einen Angriff hindeuten könnten. Es erkennt eine Vielzahl von Sicherheitsrisiken, darunter fehlerhafte und ungeschützte Geräte, Insider-Bedrohungen, unentdeckte Zero-Day-Attacken und Bedrohungen, die auf das Internet der Dinge (IoT) und Betriebstechnologie (OT) abzielen.

Sophos Extended Detection and Response (XDR)
Sophos XDR verbindet Sicherheitsdaten aus unterschiedlichen Quellen, um Bedrohungen schneller zu erkennen und Active Adversaries früher zu stoppen. Die jetzt erweiterte Reihe von Drittanbieter-Integrationen erleichtert das Sammeln, Anreichern und Kombinieren von Telemetriedaten über Endpoint-, Firewall-, Cloud-, Identitäts-, Netzwerk- und E-Mail-Lösungen

hinweg. Das verbesserte Workflow- und Case-Management für Sicherheitsteams und -analysten ermöglichen es außerdem, sich ständig wiederholende und redundante Warnmeldungen herauszufiltern. Das Management erfolgt von einer einzigen Konsole aus und bietet einen vollständigen Überblick, um den Arbeitsaufwand durch automatisierte Reaktionsmaßnahmen zu reduzieren.

„Da Angriffszeiten sich immer weiter verkürzen, ist es für Unternehmen wichtig, den potenziellen Aufwand für Angreifer so weit wie möglich zu erhöhen. Mit anderen Worten: Wenn Systeme gut gewartet sind, müssen Angreifer mehr tun, um sie zu unterwandern. Das kostet Zeit und vergrößert das Erkennungsfenster“, sagt John Shier, Field Chief Technology Officer bei Sophos. „Robuste, mehrschichtige Verteidigungssysteme bieten mehr Widerstand und fordern mehr Fähigkeiten, die ein Angreifer einsetzen muss. Viele Cyberkriminelle haben einfach nicht die Kompetenz, diese Hürden zu überwinden und werden zu einfacheren Zielen weiterziehen.“

Schnelle Reaktion mit dem Cybersecurity-Ökosystem von Sophos
Anwender können Sophos-Lösungen ganz einfach in der Cloud-nativen Sophos Central Plattform verwalten, in der die Sophos Sicherheitsprodukte und Managed Services Informationen austauschen, um automatisch auf Bedrohungen zu reagieren. Unter anderem werden infizierte Endpoints automatisch isoliert und getarnte Angreiferbewegungen blockiert. Unternehmen können zudem die MDR-Services von Sophos für das Erkennen und die Reaktion auf Bedrohungen nutzen. Als weltweit meistgenutztes MDR-Angebot mit mehr als 19.000 Kunden bietet Sophos MDR rund um die Uhr Bedrohungssuche, -erkennung und -reaktion mit den branchenweit ersten Integrationen von Drittanbietern und einer zusätzlichen Breach Warranty zum Schutz vor Sicherheitsverletzungen in Höhe von 1 Million US-Dollar.

Zitat von IDC
„Bei vielen Unternehmen wächst der Wunsch nach Konsolidierung. Wir haben festgestellt, dass vor allem kleine und mittelständische Unternehmen eine höhere Bereitschaft zeigen, ihre Endpoint-Sicherheitslösungen von mehreren Anbietern zu konsolidieren“, sagt Chris Kissel, Research Vice President, Security and Trust Products, bei IDC. „Der Hauptgrund für die Konsolidierung der Anbieter ist nicht finanzieller Natur, sondern die Effizienz der Sicherheitsabläufe. Unternehmen können bessere Sicherheitsergebnisse mit Tools erzielen, die verschiedene Facetten des Sicherheitsökosystems abdecken, die aufeinander abgestimmt sind und von einer XDR-Plattform zentral verwaltet werden.“

Verfügbarkeit
Die neue Sophos Firewall-Software ist ab sofort über den weltweiten Sophos Channel bei Partnern und Managed Service Providern (MSPs) sowie als kostenloses Upgrade für alle lizenzierten Firewall-Kunden erhältlich. Die neuen Sophos NDR- und XDR-Integrationen werden ab Ende November erhältlich sein.

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