



Sophos führt Incident Response Retainer ein

Neuer Pauschalvertrag reduziert den bürokratischen Aufwand und ermöglicht es dem Sophos Incident Response Team so, aktive Angriffe schnell zu untersuchen und zu beseitigen

Kürzere Verweildauer von Angreifern erfordert schnellere Reaktion, wie der neue Active Adversary Report von Sophos zeigt

Wiesbaden, 29. August 2023 – [Sophos](#) bietet ab sofort über sein weltweites Partnernetzwerk den neuen Dienst „Sophos Incident Response Retainer“ an. Dieser bietet Unternehmen einen schnellen Zugang zum branchenweit ersten Incident Response Service zum Festpreis, der 45 Tage 24/7 Sophos MDR (Managed Detection and Response) umfasst. Der Sophos Incident Response Retainer reduziert für Unternehmen den bürokratischen Aufwand und ermöglicht es dem Sophos-Expertenteam, auf aktive Cyberattacken besonders schnell zu reagieren sowie diese zu untersuchen und zu beheben. Externe Schwachstellen-Scans und Anleitungen zur Vorbereitung auf kritische Cybersecurity-Situationen sind ebenfalls in der Pauschale enthalten. Unternehmen können damit ihre bestehende Sicherheit proaktiv verbessern, indem sie Probleme rechtzeitig erkennen und beheben und so die Wahrscheinlichkeit eines Angriffs verringern.

Verweildauer der Angreifer deutlich kürzer

Dass eine schnelle Reaktionszeit immer wichtiger wird, zeigt der aktuelle Sophos [Active Adversary Report 2023 for Tech Leaders](#) von August 2023, der aufdeckt, dass die Verweildauer von Angreifern immer kürzer wird. Die Zeit, in der Angreifer aufgespürt und vertrieben werden können, ist entscheidend für die Schadensbegrenzung und die Bekämpfung von Datenverletzungen und [Ransomware](#). Der Active Adversary Report belegt, dass die durchschnittliche Verweildauer von Angreifern (Zeit vom Beginn eines Angriffs bis zu seiner Entdeckung) [weiter sinkt](#), und zwar von 10 Tagen im Jahr 2022 auf acht Tage in der ersten Hälfte des Jahres 2023. Insbesondere bei Ransomware sank die Verweildauer rapide von neun auf nur fünf Tage. Außerdem zeigt der Report, dass die Angriffe bevorzugt nachts und am Wochenende erfolgen. Nur 9,6 Prozent der Ransomware-Vorfälle finden während der Geschäftszeiten des Zielunternehmens statt. Die häufigste Angriffszeit ist freitags zwischen 23 Uhr und Mitternacht in den lokalen Zeitzonen der Zielunternehmen.



„Der Sophos Incident Response Retainer hilft Unternehmen, die schnellstmögliche Reaktion auf aktive Cyberangriffe zu realisieren. Angesichts der heutigen komplexen und herstellerübergreifenden Computerumgebungen, des Fachkräftemangels, des sich verändernden Verhaltens von Angreifern und der Anforderungen an Cyber-Versicherungen ist es von entscheidender Bedeutung, dass alle Unternehmen im Voraus festgelegte Reaktionspläne für Vorfälle haben. Vorbereitet zu sein ist eine Schlüsselkomponente für Cyber-Resilienz“, sagt Rob Harrison, Vice President, Product Management bei Sophos. „Angreifer nutzen oft dieselbe Schwachstelle in einem einzigen System aus und es ist nicht ungewöhnlich, dass [mehrere, unterschiedliche Angreifer dasselbe Ziel ins Visier nehmen](#). Das Ziel von Sophos ist es, aktive Angriffe sofort zu stoppen und sicherzustellen, dass eine vollständige Beseitigung erreicht wird. Der Retainer sorgt dabei für Planungssicherheit, da der Service unabhängig davon, wie viele Stunden die Bereinigung dauert, gleistet wird. Wir sind der einzige Sicherheitsanbieter, der diese Art von Retainer-Services für dringende Sicherheitsvorfälle anbietet.“

„Fünfundsechzig Prozent der Unternehmen hatten trotz erheblicher Investitionen in Cybersecurity-Tools¹ in den letzten zwölf Monaten mit einem signifikanten Sicherheitsverstoß zu kämpfen“, sagt Chris Kissel, Research Vice President, Security and Trust Products, IDC. „Der Umgang mit unerwarteten Cyberangriffen ist zeitaufwändig, beschwerlich und stellt eine große finanzielle Belastung dar. Die einzige Möglichkeit, Zeit zu sparen, Kosten zu senken und die Auswirkungen eines Angriffs abzumildern, besteht darin, ein erfahrenes und einsatzbereites Incident-Response-Team zu haben, bevor die Angreifer zuschlagen.“

Der Sophos Incident Response Retainer ist weltweit für alle Kunden, die bereits das Sophos-Portfolio mit Endpoint-, Netzwerk-, E-Mail- und anderen Sicherheitsprodukten oder Sophos MDR Essentials nutzen, in drei Stufen über [Sophos Partner](#) erhältlich. Dank der einzigartigen Fähigkeit von Sophos, Angriffe in Umgebungen mit mehreren Anbietern zu erkennen, darauf zu reagieren und sie zu beheben, ist der Sophos Incident Response Retainer auch für Nicht-Sophos-Kunden verfügbar. Für bestehende Sophos-Kunden sind ebenfalls Endpoint-Konfigurationsüberprüfungen und Geräte-Audits in dem Angebot enthalten. Unternehmen, die umfassendere Leistungen in einem Paket bevorzugen, können Sophos MDR Complete einsetzen, das automatisch einen umfassenden Incident Response Service beinhaltet.

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

¹ IDC, Ransomware Winter 2023: Focus on Prevention ... Backups or Paying the Ransom Won't Save You, Doc# US50727822, June 2023.

Pressekontakt:

Sophos

Jörg Schindler, PR-Manager Central & Eastern Europe

joerg.schindler@sophos.com, +49-721-25516-263

TC Communications

Arno Lucht, +49-8081-954619

Thilo Christ, +49-8081-954617

Ulrike Masztalerz, +49-30-55248198

Ariane Wendt +49-172-4536839

sophos@tc-communications.de