Sophos lanciert Managed Threat Response (MTR)

Machine Learning verleiht der neuen Threat Hunting-, Detection- und Response-Lösung mehr Leistung im Kampf gegen komplexe Bedrohungen der Cybersicherheit.

Wiesbaden, 9. Oktober 2019 – Sophos hat seine Managed Threat Response (MTR)-Funktion weiterentwickelt. Der wiederverkäufliche Service bietet Organisationen ein 24/7 verfügbares Sicherheitsteam, um auch hochentwickelte und komplexe Bedrohungen zu neutralisieren.

Diese Art der Attacken umfasst aktive Angriffe, die dateifreie Attacken und Administrator-Werkzeuge wie die PowerShell nutzen, um Privilegien zu erhöhen, Daten zu exfiltrieren und seitlich zu verteilen. Der Artikel Lemon_Duck PowerShell Malware aus den SophosLabs erläutert diesen Vorgang genauer. Derartige Angriffe sind schwer zu entdecken, da sie aktive Gegner einbinden, indem sie legitime Werkzeuge für bösartige Zwecke nutzen. MTR hilft dabei, derartige Bedrohungen zu eliminieren.

„Cyberkriminelle passen ihre Methoden an und setzen immer mehr hybride Angriffe ein, die Automation mit interaktivem menschlichem Erfindungsreichtum kombinieren“, erklärt Joe Levy, Chief Technology Officer bei Sophos. „Haben die Angreifer einmal Fuß gefasst, werden sie irreführende Techniken anwenden, die menschliche Intelligenz benötigen, um Attacken aufzuspüren und zu unterbinden. Größtenteils benachrichtigen andere MDR-Services einfach nur ihre Kunden über potenzielle Gefahren und überlassen es dann ihnen, wie sie damit umgehen wollen. Das MTR von Sophos geht darüber aber hinaus: mit zusätzlicher Intelligenz, um Bedrohungen aufzuspüren, beispielloser Produktexpertise und ununterbrochener Abdeckung. Zusätzlich erhalten die Kunden die Möglichkeit, dass ein hoch trainiertes Team von Response-Sachkundigen auf ihre Veranlassung hin gezielte Maßnahmen ergreift, um sogar die kompliziertesten Bedrohungen zu neutralisieren.“

Aufbauend auf Intercept X Advanced mit Endpoint Detection und Reaktion (EDR) fusioniert das Sophos MTR maschinelles Lernen mit Experten-Analyse, um das Auffinden von Bedrohungen zu verbessern, Warnmeldungen gründlicher zu untersuchen und gezielter bei der Eliminierung von Gefahren zu agieren. Diese innovativen Leistungsmöglichkeiten basieren auf den Technologien der jüngsten Sophos-Zukäufe von Rook Security und DarkBytes.

Die technischen Details beinhalten:

- **Expertensuche nach Bedrohungen**: Sophos MTR sieht attackierendes Verhalten voraus und identifiziert neue Indikatoren von Angriffen. Die Gefahrenjäger scannen proaktiv, wägen potenzielle Bedrohungen und Vorfälle ab und untersuchen zufällige und angrenzende Ereignisse, die vorab nicht entdeckt werden konnten.

- **Weiterentwickelte kontradiktorische Erkennung**: MTR verwendet eine bewährte Untersuchungstechnik, um legitimes Verhalten von Taktik, Technik und Prozedur (TTPs) der Angreifer zu unterscheiden. Gekoppelt an die verbesserte Telemetrie von Sophos Central – mit einem detaillierten Bild gegnerischer Aktivitäten als Extraservice – lassen sich Umfang und Schweregrad der Bedrohung feststellen, um schnell reagieren zu können.

- **Maschinell-beschleunigte menschliche Reaktion auf Gefahren**: Ein geschultes Team globaler Spezialisten erzeugt und verwendet Bedrohungsintelligenz für die Bestätigung von Gefahren und agiert aus der Ferne schnell und präzise, um die Bedrohung zu stören, einzudämmern und zu neutralisieren.

- **Vermögensermittlung und vorschriftsmäßige Sicherheitsrichtlinien**: Sophos MTR liefert wertvolle Erkenntnisse in verwaltete und nicht-verwaltete Vermögenswerte, Schwachstellen für besser fundierte Folgenabschätzung und Bedrohungsfahndung. Vorschriftsmäßige und umsetzbare Leitlinien, um Konfigurations- und Architektur-Schwächen zu lösen, ermöglichen es Unternehmen, proaktiv ihren Sicherheitsstatus mit härterer Abwehr zu verbessern.

Die MTR-Funktion lässt sich mit verschiedenen Service-Stufen und Reaktionsmodi individualisieren, um die speziellen Bedürfnisse jeder Organisation zu berücksichtigen. Im Gegensatz zu vielen MDR-Services, die sich auf Monitoring und Warnmeldungen fokussieren, setzt das neue MTR auf schnelle Eskalation und Maßnahmen gegen Bedrohungen, die auf den Präferenzen der Organisation beruhen.

Sophos MTR ist ab sofort weltweit bei registrierten Sophos Partnern erhältlich. Mehr Informationen auf Sophos News und Sophos.com.

Über Sophos
Als ein weltweit führender Anbieter von Next-Generation-Cybersicherheit schützt Sophos fast 400.000 Unternehmen jeder Größe in mehr als 150 Ländern vor den neuesten Cyberbedrohungen. Mit den SophosLabs und seinem globalen Team für Bedrohungs- und Datenanalyse schützen die Cloud- und KI-gestützten Sophos-Lösungen Endpoints (Laptops, Server und mobile Geräte) sowie Netzwerke vor kontinuierlich neu entwickelten Cybertaktiken und -techniken, einschließlich automatisierter Attacken, Ransomware, Malware, Exploits, Datenexfiltration, Phishing und mehr. Die preisgekrönte, Cloud-basierte Plattform Sophos Central integriert das gesamte Sophos-Produktportfolio, von der Intercept X Endpoint-Lösung bis zur XG Firewall, in einem einzigen Synchronized Security System. Die Lösungen von Sophos sind exklusiv über den globalen Channel mit mehr als 47.000 Partnern und Managed Service Providern (MSPs) erhältlich. Sophos stellt seine Technologien für Unternehmen auch Privatanwendern mit Sophos Home zur Verfügung. Das Unternehmen hat seinen Hauptsitz in Oxford, Großbritannien, und ist an der Londoner Börse unter dem Symbol "SOPH" notiert. Weitere Informationen unter www.sophos.de.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
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