Sophos baut Endpoint Detection and Response (EDR) mit neuer Version aus

Sophos Intercept X with EDR bietet branchenweit erstmals Live-Erkennungs- und Reaktionsfähigkeiten für Securtiy-Analysten und IT-Administratoren.

Die SophosLabs erkannten, dass das Kingminer Botnet jetzt auch den EternalBlue Exploit für die Verbreitung von Malware nutz – die neue EDR-Engine erkennt Anzeichen einer Kompromittierung.

Wiesbaden, 9. Juni 2020 – Sophos stellt die aktualisierte Version seiner Endpoint Detection and Response (EDR)-Lösung vor. Sophos EDR richtet sich an Security-Analysten und IT-Administratoren und ist ab sofort in Sophos Intercept X Advanced with EDR und Intercept X Advanced for Server with EDR integriert. Bedeutende Weiterentwicklungen und neue Funktionen ermöglichen es Security-Analysten, Bedrohungen schneller und einfacher zu identifizieren und zu neutralisieren. So kann aktiv ein sicherer IT-Betrieb aufrechterhalten und das Risiko reduziert werden.

Sophos Studie bestätigt Notwendigkeit von Threat Intelligence
Zudem hat Sophos die neue Studie „An Insider View into the Increasingly Complex Kingminer Botnet“ veröffentlicht. Die Studie bestätigt das Einbeziehen von Servern bei Angriffen und die Bedeutung von Threat Intelligence bei der Erkennung solcher Aktivitäten. Das Kingminer-Botnet versucht in Server einzudringen, indem es Anmeldedaten via Brute-Forcing identifiziert. Sophos hat nun herausgefunden, dass das Botnet den EternalBlue Exploit nutzt, um neben anderen Angriffsmechanismen auch Malware zu verbreiten. Die neue Version von Sophos EDR bietet eine benutzerdefinierte Query Engine und ermöglicht damit das Erkennen von Anzeichen einer Kompromittierung.

„Während Unternehmen zunehmend in die Cloud wechseln und das Remote-Arbeiten ermöglichen, erhöhen Cyberkriminelle den Einsatz und schrecken vor nichts zurück, um aus den erweiterten Angriffsflächen Kapital zu schlagen. Server und andere Endpoints sind oft unzureichend geschützt, wodurch Schlupflöcher entstehen, die von Angreifern ausgenutzt werden“, sagt Dan Schiappa, Chief Product Officer bei Sophos. „Sophos EDR identifiziert diese Angriffe, verhindert Attacken und bringt Licht in ansonsten dunkle Bereiche. Live-Abfragen, die nur in Sophos Intercept X with EDR verfügbar sind, ermöglichen es, nach Indikatoren einer Kompromittierung zu suchen und den aktuellen Systemstatus zu ermitteln. Dieses Maß an Information ist entscheidend, um das wechselnde Verhalten der Angreifer zu verstehen und die Verweildauer zu verkürzen.“

Neue EDR Kernfunktionen
Sophos EDR bietet jetzt einen Überblick über das gesamte Unternehmen. Es ermöglicht Security- und IT-Experten, Fragen in Bezug auf kritische Bedrohungen und auf den sicheren IT-Betrieb schnell und einfach zu beantworten. Zu den neuen Funktionen gehören:

Live Discover: Erkennt vergangene und aktuelle Aktivitäten und speichert die Daten bis zu 90 Tage. Sofort einsatzbereite SQL-Abfragen ermöglichen es Fragen zur Bedrohungssuche und IT zu beantworten. Sie können aus einer Bibliothek mit vordefinierten Optionen ausgewählt und von Benutzern vollständig angepasst werden. Diese flexible Query Engine

bietet Zugriff auf hoch detaillierte Aufzeichnungen über Endpoint-Aktivitäten, die mit der Sophos Deep-Learning-Technologie kontinuierlich aktualisiert werden.

Live Response: Remote-Reaktion und Fernzugriff auf Endpunkte und Server über eine Command-Line-Schnittstelle, um weitere Untersuchungen durchzuführen und Probleme zu beheben. Dazu gehören einfaches Neustarten von Geräten, Installieren und Deinstallieren von Software, Beenden aktiver Prozesse, Ausführen von Skripts, Bearbeiten von Konfigurationsdateien, Ausführen forensischer Tools, Isolieren von Rechnern und mehr.

Sophos EDR basiert auf dem neuronalen Deep-Learning-Netzwerk von Sophos, das anhand von Hunderten von Millionen Beispielen und Bedrohungsindikatoren geschult ist. Security-Analysten und IT-Administratoren erhalten außerdem On-Demand-Zugriff auf Bedrohungsinformationen aus den SophosLabs, die täglich mehr als 400.000 Malware-Samples verfolgen, zerlegen und analysieren.

Verfügbarkeit
Sophos Intercept X Advanced with EDR und Intercept X Advanced for Server mit EDR steht ab sofort und ohne zusätzliche Kosten zur Verfügung. Sophos EDR unterstützt Windows, MacOS und Linux. Die neuen Funktionen Live Discover und Live Response lassen sich einfach im Threat-Analysecenter auf der Cloud-basierten Plattform Sophos Central verwalten, um Informationen in Echtzeit mit dem gesamten Portfolio an Next Generation Cyber-Sicherheitslösungen von Sophos über den Synchronized Security-Ansatz auszutauschen. In Kombination mit Sophos Managed Threat Response (MTR), einem Dienst zur Bedrohungssuche, -erkennung und -bewältigung, können Unternehmen ihre Schutz durch Analysen von Experten erweitern und damit eine zusätzliche proaktive Schutzstrategie verfolgen.

Über Sophos
Als ein weltweit führender Anbieter von Next-Generation-Cybersicherheit schützt Sophos mehr als 400.000 Unternehmen jeder Größe in über 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 sich ständig verändernden Cyberangriffen, einschließlich Ransomware, Malware, Exploits, Datenexfiltration, individuellen Hackervorstößen, Phishing und mehr. Die cloud-basierte Plattform Sophos Central integriert über APIs das gesamte Next Generation Sophos-Portfolio, von der Intercept X Endpoint-Lösung bis zur XG Firewall, in einem einzigen Synchronized-Security-System. Sophos treibt die Entwicklung zur Next Generation Cybersicherheit voran und setzt fortschrittliche Technologien, beispielsweise aus den Bereichen Cloud, Machine Learning, APIs, Automatisierung oder Managed Threat Response ein, um Unternehmen jeder Größe Schutz der Enterprise-Klasse zu bieten. Sophos vertreibt Produkte und Services exklusiv über einen globalen Channel mit mehr als 47.000 Partnern und Managed Service Providern (MSP). Sophos stellt seine innovativen, gewerblichen Technologien auch Privatanwendern via 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