Sophos präsentiert XG Firewall mit neuer Xstream“-Architektur

Untersuchungen der SophosLabs zeigen, dass 44 Prozent der Informationsdiebe Verschlüsselung verwenden, um gestohlene Daten zu verstecken.

Wiesbaden, 18. Februar 2020 – Sophos stellt heute seine neue „Xstream“-Architektur für die Sophos XG Firewall vor. Die Firewall ist nun zusätzlich mit hochleistungsfähigen TLS-Entschlüsselungsfunktionen (Transport Layer Security) für den Datenverkehr ausgestattet. Dies eliminiert erhebliche Sicherheitsrisiken im Zusammenhang mit verschlüsseltem Netzwerkverkehr, die von Sicherheitsteams aufgrund von Bedenken hinsichtlich Leistung und Komplexität oft unbeachtet bleiben. Die XG Firewall bietet zudem eine verbesserte KI-Bedrohungsanalyse aus den SophosLabs und eine höhere Leistung der Applikation insgesamt.

Im Zusammenhang mit der TLS-Entschlüsselung veröffentlichen die SophosLabs zudem einen neuen Report mit dem Titel „Nearly a Quarter of Malware now Communicates Using TLS“. Hier wird zum Beispiel erläutert, wie 23 Prozent der Malware-Familien verschlüsselte Kommunikation für Command and Control (C2) oder die Installation verwenden. Der Artikel beschreibt drei häufige Trojaner – Trickbot, IcedID und Dridex –, die TLS im Verlauf ihrer Angriffe nutzen. Cyberkriminelle nutzen TLS auch, um ihre Exploits, Nutzlasten und gestohlenen Inhalte zu verstecken und einer Entdeckung zu entgehen. Tatsächlich verwenden 44 Prozent der Informationsdiebe Verschlüsselung, um entführte Daten, einschließlich der Passwörter von Bank- und Finanzkonten und anderer sensibler Anmeldedaten, aus Organisationen herauszuschmuggeln.

„Wie die Untersuchungen der SophosLabs zeigen, machen sich Cyberkriminelle Verschlüsselung zu eigen, um Sicherheitsprodukte zu umgehen. Leider verfügen die meisten Firewalls nicht über skalierbare TLS-Kryptofunktionen und können den verschlüsselten Datenverkehr nicht überprüfen, ohne dass Anwendungen unterbrochen werden oder die Netzwerkleistung beeinträchtigt wird“, sagt Dan Schiappa, Chief Product Officer bei Sophos. „Mit der neuen Xstream-Architektur in der XG Firewall bietet Sophos einen entscheidenden Einblick in einen großen und bisher toten Winkel und beseitigt gleichzeitig Latenz- und Kompatibilitätsprobleme durch die vollständige Unterstützung des neuesten TLS 1.3-Standards. Die internen Benchmark-Tests von Sophos haben eine zweifache Leistungssteigerung der neuen XG TLS Inspection Engine im Vergleich zu früheren XG-Versionen ergeben. Dies ist ein entscheidender Schritt nach vorn.“

Eine Sophos-Umfrage unter 3.100 IT-Managern in zwölf Ländern ergab, dass IT-Administratoren oft von einer Entschlüsselung absehen, um Latenz zu vermeiden. Im White Paper der Umfrage „The Achilles Heel of Next-Gen Firewalls“ wird zudem berichtet, dass 82 Prozent der Befragten ein TLS-Inspektion befürworten, aber nur 3,5 Prozent der Unternehmen ihren Datenverkehr für eine ordnungsgemäße Inspektion.

Die wichtigsten neuen Funktionen der Sophos XG Firewall im Überblick:

- Inspektion von TLS 1.3 zur Erkennung getarnter Malware: Die neue Port-agnostische TLS-Engine verdoppelt die Leistung der Kryptographie im Vergleich zu früheren XG-Versionen.
- Optimierte Leistung kritischer Anwendungen: Neue FastPath-Richtlinien steigern die Leistung von SD-WAN-Anwendungen und den Datenverkehr, einschließlich Voice over IP, SaaS und andere, auf bis zu Leitungsgeschwindigkeit.
- Adaptives Traffic Scanning: Die neu verbesserte Deep Packet Inspection (DPI)-Engine nimmt eine dynamische Risikobewertung des Traffic vor und passt sie an die entsprechende Stufe des Bedrohungs-Scans an. Damit wird der Durchsatz in den meisten Netzwerkumgebungen um bis zu 33 Prozent erhöht.
- Bedrohungsanalyse mit den SophosLabs: Dies bietet Netzwerkadministratoren im Zusammenspiel mit den SophosLabs eine verbesserte KI-Analyse, um Abwehrmechanismen zu verstehen und anzupassen und um sich vor der Bedrohungslandschaft, die sich ständig verändert, zu schützen.
- Umfassendes Cloud-Management und Reporting in Sophos Central: Die zentralisierten Verwaltungs- und Reporting-Funktionen in Sophos Central bieten Kunden ein Gruppen-Firewall-Management und flexibles Cloud-Reporting über die gesamte Firmengruppe hinweg ohne zusätzliche Kosten.
- Integration mit dem Sophos Managed Threat Response (MTR)-Dienst: Kunden, die eine XG Firewall im Einsatz haben und auch den Sophos MTR Advanced-Dienst abonnieren, erhalten durch die Integration detailliertere Informationen, um Angriffe zu verhindern, zu erkennen oder darauf zu reagieren.

Neben dem gesamten Sophos Portfolio an Next Generation Sicherheitslösungen ist auch die Sophos XG Firewall in der Cloud-basierten Sophos Central-Plattform verfügbar. Der Synchronized Security-Ansatz von Sophos ermöglicht die Interaktion aller Sophos Lösungen für den Informationsaustausch und die Reaktion auf Bedrohungen in Echtzeit.

Zusätzliche Informationen

- SophosLabs Report zum Thema TLS-Entschlüsselung „Nearly a Quarter of Malware now Communicates Using TLS“: https://news.sophos.com/en-us/2020/02/18/nearly-a-quarter-of-malware-now-communicates-using-tls

- Video „TLS Encryption Explained“ über Angreifer, die TLS-Verschlüsselung für die Cyber-Kriminalität nutzen: https://vimeo.com/392040023

- Sophos White Paper “Has Encryption Made Your Firewall Irrelevant?”: https://secure2.sophos.com/en-us/security-news-trends/whitepapers/encryption-firewall.aspx

- Der „Threat Report 2020“ von den SophosLabs: https://www.sophos.com/en-us/labs/security-threat-report.aspx

- Sophos-Report „Sophos Snatch Ransomware report“: https://news.sophos.com/en-us/2019/12/09/snatch-ransomware-reboots-pcs-into-safe-mode-to-bypass-protection/

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