Auf der Suche nach dem einen (ungeschützten) Gerät: Remote Ransomware-Angriffe steigen um 62 Prozent

Erfolgreiche Ransomware-Gruppierungen wechseln immer häufiger auf Remote-Verschlüsselung, laut Sophos' neuestem CrypoGuard-Report. Das Problem: traditioneller Anti-Ransomwareschutz „sieht" das Unheil nicht kommen und greift ins Leere.

Wiesbaden, 29. Dezember 2023 – Sophos veröffentlichte vor kurzem seinen neuen Report „CryptoGuard: An Asymmetric Approach to the Ransomware Battle" mit den Auswertungen seiner CryptoGuard-Abwehrtechnologie. Die erfolgreichsten und aktivsten Ransomware-Gruppierungen wie Akira, ALPHV/ BlackCat, LockBit, Royal oder Black Basta wechseln demnach bewusst auf Fernverschlüsselung für ihre Angriffe. Bei dieser sogenannten „Remote Ransomware" nutzen Cyberkriminelle ein kompromittiertes und oft schlecht geschütztes Endgerät, um Daten auf anderen Geräten zu verschlüsseln, die mit dem gleichen Netzwerk verbunden sind.

Die CryptoGuard-Technologie gegen Ransomware überwacht schadhafte Verschlüsselung von Dateien und bietet unmittelbar Schutz plus eine Reset-Funktion, sogar wenn die Ransomware selbst gar nicht auf einem geschützten Host erscheint. Diese Technologie ist die letzte Linie im mehrstufigen Endpoint-Schutz von Sophos. Seit 2022 wurde hier für Remote-Angriffe ein Wachstum von 62 Prozent verzeichnet.

Mark Loman, Vice President Threat Research bei Sophos: „Unternehmen können heutzutage tausende gut gesicherte Computer betreiben, aber mit Remote Ransomware genügt schon ein ungeschütztes Gerät, um das gesamte Netzwerk zu kompromittieren. Angreifer wissen darum und suchen gezielt nach dieser einen Schwachstelle – und bei den meisten Firmen findet sich mindestens eine. Remote-Verschlüsselung wird ein dauerhaftes Problem bleiben und in Anbetracht der Warnmeldungen lässt sich sagen, dass diese Angriffsmethode stetig wächst."

Traditionelle Anti-Ransomware-Maßnahmen erkennen die Remote-Aktivitäten nicht

Das Problem bei dieser Fernverschlüsselung ist, dass die traditionellen Anti-Ransomware Schutzmaßnahmen, die auf den Remote-Geräten laufen, diese schadhaften Dateien oder ihre Aktivitäten nicht erkennen und damit auch nicht vor Verschlüsselung oder Datenverlust schützen können. Die CryptoGuard-Technologie setzt auf einen neuartigen Ansatz: sie analysiert die Inhalte der Dateien, um zu prüfen, ob irgendwelche Daten verschlüsselt wurden. Damit entdeckt sie Ransomware-Aktivitäten auf jedem Gerät im gesamten Netzwerk – auch wenn sich keine Schadsoftware auf dem Gerät befindet.

CryptoLocker gilt als die erste erfolgreiche Ransomware, die 2013 für Remote-Verschlüsselung mit asymmetrischer Verschlüsselung (auch Public-Key Kryptographie bekannt) genutzt wurde. Seitdem waren die Angreifer in der Lage, den Gebrauch von Ransomware zu eskalieren. Grund: ständige, allgegenwärtige Sicherheitslücken in Organisationen weltweit und das Aufkommen von Kryptowährungen.

Moderne Ransomware-Verteidigung setzt auf asymmetrische Abwehr

„Als wir das erste Mal sahen, wie CryptoLocker vor zehn Jahren die Remote-Verschlüsselung ausnutzte, wussten wir: diese Taktik wird in den nächsten Jahren eine Herausforderung für die Verteidigung. Viele Lösungen fokussieren sich auf das Aufspüren schadhafter Binärprogramme oder deren Ausführung. Im Fall von Fernverschlüsselung aber erfolgen diese Schritte auf einem anderen (ungeschützten) Computer als auf dem, dessen Dateien

verschlüsselt werden. Der einzige Weg das zu stoppen, ist die genaue Beobachtung und Schutz der Dateien.
Deswegen haben wir CryptoGuard entwickelt. Diese Lösung sucht nicht nur nach Ransomware, sondern sie konzentriert sich auf die primären Ziele – die Dateien. Es setzt eine mathematische Prüfung bei Dokumenten ein, um Anzeichen von Manipulation oder Verschlüsselung aufzuspüren. Bemerkenswert ist, dass diese autonome Strategie bewusst nicht auf Indikatoren für Verstöße, Bedrohungssignaturen, künstliche Intelligenz, Cloud-Lookups oder Vorwissen angewiesen ist, um wirksam zu sein. Durch den Fokus auf die Dateien beeinflussen wir das Machtverhältnis zwischen Angriff und Verteidigung. Wir erhöhen für die Angreifer Kosten und Komplexität einer erfolgreichen Datenverschlüsselung, so dass sie ihr Ziel aufgeben. Das ist ein Teil unseres asymmetrischen Abwehransatzes“, erläutert Loman.

Eine effektive Verteidigung stoppt Fernattacke plus Teildatenverschlüsselung
„Remote Ransomware ist ein bekanntes Problem für Organisationen und trägt generell zur Langlebigkeit von Ransomware bei. Da das Lesen von Daten über eine Netzwerkverbindung langsamer ist als von der lokalen Festplatte, haben wir gesehen, dass Angreifer wie LockBit oder Akira strategisch nur einen Teil einer Datei verschlüsseln. Dieses Prinzip strebt nach maximalem Effekt in minimaler Zeit, zudem reduziert es das Fenster für die Verteidiger, um die Attacke zu bemerken und zu reagieren. Der Sophos-Ansatz zur Anti-Ransomware-Technologie stoppt sowohl die Fernattacke als auch die Teilverschlüsselung der Dateien“, so Loman.

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