Sophos Active Adversary Report deckt die neuen Tricks der Cyberkriminellen auf

Die detaillierte Analyse tatsächlicher Angriffe auf Unternehmen deckt eine neue Masche der Cyberkriminellen auf, um ihre Verweildauer zu vertuschen und damit auch eine rasche Abwehrreaktion zu vereiteln: Sie machen die Telemetrie-Protokolle unbrauchbar. Sophos Field CTO John Shier ordnet die Ergebnisse ein und gibt Empfehlungen.

Wiesbaden, 16. November 2023 – Sophos hat seinen neuen Active Adversary Report veröffentlicht. Besonders auffallend: in 42 Prozent der analysierten Angriffe fehlten die telemetrischen Protokolle und in 82 Prozent dieser Fälle deaktivierten oder löschten die Kriminellen Telemetriedaten aktiv, um ihre Angriffe zu verstecken. Zudem nimmt die Aufenthaltsdauer im gekaperten System weiter ab und setzt damit den Trend vom letzten Report weiter fort.

„Active Adversary" beschreibt als Fachbegriff die Art der Angriffsstrategie auf ein System. Im Gegensatz zur rein technischen und automatisierten Attacke kommt bei dieser Art der menschliche Faktor ins Spiel: Cyberkriminelle sitzen aktiv am Keyboard und reagieren individuell auf die Gegebenheiten in einem infiltrierten System. Diese Schleichfahrten werden durch Lücken in der Telemetrie nochmals unterstützt, da sie die notwendige Sichtbarkeit in den Netzwerken und Systemen verringern. Ein großes Problem, besonders seit sich die Verweildauer der Angreifer – vom initialen Zugang bis zur Aufdeckung – kontinuierlich verringert und somit auch die Zeit für die Verteidigungsreaktion kürzer ist.

John Shier, Field CTO von Sophos, zum Telemetrieproblem
„Zeit ist der kritische Faktor bei der Reaktion auf eine aktive Bedrohung. Die Phase zwischen der Entdeckung eines initialen Zugriffs bis zur kompletten Entschärfung der Situation sollte so kurz wie möglich sein. Je weiter die Kriminellen in der Angriffskette kommen, desto mehr Probleme sehen wir im Abwehrzentrum. Fehlende Telemetriedaten erhöhen die Wiederherstellungszeit, etwas das die meisten Organisationen sich nicht leisten können. Deswegen ist ein komplettes und präzises Protokollieren sehr wichtig. Wir sehen aber, dass Organisationen viel zu oft nicht über die Daten verfügen, die sie eigentlich benötigen."

Unter fünf Tage im System – schnelle Ransomware-Angriffe liegen bei 38 Prozent
Im Active Adversary Report klassifiziert Sophos Ransomware-Angriffe mit einer Verweildauer von bis zu fünf Tagen als „schnelle Attacken". Davon gab es 38 Prozent in den untersuchten Fällen. „Langsame Attacken" gelten als solche, die teilweise eine weitaus größere Verweildauer als fünf Tage haben. Davon gab es 62 Prozent. Auch wenn die „schnellen" Attacken damit noch weniger oft vertreten sind, nimmt deren Anteil im Gesamtbild ständig zu – und das mit Gründen: Angreifer reagieren damit auf die besseren Erkennungsmethoden in Unternehmen, die ihnen weniger Zeit lassen und zudem sind die Cyberkriminellen mittlerweile auch einfach sehr geübt. „Wie bei jedem Prozess führen Wiederholung und Übung tendenziell zu besseren Ergebnissen", so John Shier. „Moderne Ransomware wird in diesem Jahr zehn Jahre alt, ein lange Zeit mit vielen Beispielen, um immer mehr Kriminelle zu Experten zu machen. Eine umso gefährlichere Entwicklung, wenn viele Verteidigungsstrategien nicht mithalten konnten."

Bei der Prüfung der schnellen und langsamen Typen ergaben sich wenig Variationen hinsichtlich der Werkzeuge, Techniken und LOLBins (living-off-the-land Binärprogramme), die die Angreifer einsetzen. Dies deutet darauf hin, dass die Verteidiger des angegriffenen

Systems ihre Abwehrstrategien nicht neu erfinden müssen, wenn die Verweildauer sinkt. Allerdings müssen sich Unternehmen darüber im Klaren sein, dass schnelle Angriffe und fehlende Telemetrie schnelle Reaktionszeiten behindern und in der Folge zu einer erheblich umfangreicheren Störung des Geschäftsbetriebs führen können.

Neue Abwehrmaßnahmen nicht zwingend nötig
„Cyberkriminelle sind faul, sie nehmen nur Veränderungen vor, wenn sie dadurch besser ihr Ziel erreichen. Was läuft, ändern Angreifer nicht, selbst wenn sie dadurch nach der Infiltration schneller entdeckt werden. Das sind gute Nachrichten für Organisationen, da sie ihre Defensivstrategie nicht radikal ändern müssen, nur weil die Angreifer den Turbo einlegen. Defensivmaßnahmen, die schnelle Attacken aufspüren, greifen bei allen Attacken, zeitunabhängig. Das beinhaltet auch die komplette Telemetrie, den robusten Schutz für alle Bereiche und eine allgegenwärtige Überwachung“, gibt Shier zu bedenken. „Der Schlüssel liegt in der Erhöhung der Widerstände. Macht man es den Angreifern schwerer und zieht jede Phase des Angriffs in die Länge, bleibt mehr Zeit, um zu reagieren.

Der Sophos Active Adversary Report basiert auf 232 Incident-Response-Fälle vom 1. Januar 2022 bis 30. Juni 2023 über 25 Branchen hinweg. Betroffene Organisationen ließen sich in 34 verschiedenen Ländern auf sechs Kontinenten lokalisieren. 83 Prozent der Fälle betrafen Unternehmen mit weniger als 1.000 Mitarbeitern. Der Report liefert verwertbare Informationen, wie Sicherheitsexperten ihre Defensivstrategien optimal gestalten können.

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