SOPHOS

Remote-Ransomware

Unbefugte Remote-Verschlüsselung ist eine beliebte Ransomware-Technik, die bei rund 60 % der manuell gesteuerten Ransomware-Angriffe zum Einsatz kommt[1]. Die meisten führenden Endpoint-Security-Lösungen sind mit der Bekämpfung von Remote-Ransomware überfordert. In diesem Guide erfahren Sie mehr über die Risiken von Remote-Ransomware, warum die meisten Endpoint-Security-Lösungen keinen Schutz bieten und welche branchenführenden Anti-Ransomware-Lösungen von Sophos Remote-Verschlüsselung effektiv stoppen.

Sophos-Whitepaper. Dezember 2023

Was ist Remote-Ransomware?

Bei Remote-Ransomware-Angriffen nutzen Cyberkriminelle einen kompromittierten Endpoint und verschlüsseln so Daten auf anderen Geräten im gleichen Netzwerk.

Angreifer versuchen in der Regel, Ransomware direkt auf den Geräten bereitzustellen, die sie verschlüsseln möchten. Wird der erste Versuch blockiert (z.B. von Sicherheits-Software), geben die Angreifer nur selten auf. Stattdessen versuchen sie, mit anderen Methoden ihr Ziel zu erreichen.

Sobald es den Cyberkriminellen gelingt, ein Gerät zu kompromittieren, können sie die Domänenarchitektur des Unternehmens/der Organisation nutzen, um Daten auf zur Domäne hinzugefügten, verwalteten Geräten zu verschlüsseln. Die schädlichen Aktivitäten (Eindringen, Payload-Ausführung und Verschlüsselung) erfolgen auf dem bereits kompromittierten Gerät und werden daher selbst von modernen Sicherheitslösungen nicht erkannt. Einzig die Übertragung von Dokumenten von einem Gerät auf ein anderes weist auf eine Kompromittierung hin.

80 % aller Remote-Verschlüsselungsangriffe starten auf nicht verwalteten Geräten im Netzwerk[2]. Manche beginnen jedoch auf nicht ausreichend geschützten Geräten, deren Abwehr nicht verhindert, dass Cyberkriminelle sich Zugriff verschaffen.

Warum ist Remote-Ransomware so weit verbreitet?

Remote-Ransomware zeichnet sich vor allem durch ihre Skalierbarkeit aus: Ein einziger nicht verwalteter oder unzureichend geschützter Endpoint macht die gesamte Unternehmensumgebung anfällig für Remote-Verschlüsselung, auch wenn auf allen anderen Endpoints Next-Gen-Endpoint-Security läuft.

Erschwerend kommt hinzu, dass zahlreiche Ransomware-Varianten diese Remote-Verschlüsselung unterstützen. Hierzu zählen unter anderem Akira, BitPaymer, BlackCat, BlackMatter, Conti, Crytox, DarkSide, Dharma, LockBit, MedusaLocker, Phobos, Royal, Ryuk und WannaCry.

Ein weiterer entscheidender Grund für die Verbreitung von Remote-Ransomware: Die meisten Endpoint-Security-Lösungen sind hier machtlos, denn sie konzentieren sich auf die Erkennung von schädlichen Ransomware-Dateien und -Prozessen auf geschützten Endpoints. Bei Remote-Verschlüsselungsangriffen laufen die schädlichen Aktivitäten jedoch auf dem kompromittierten Gerät ab und bleiben so unerkannt.

Sophos Endpoint beinhaltet robusten Schutz vor unbefugter Remote-Verschlüsselung, durch unsere branchenführende Schutztechnologie CryptoGuard.

Sophos CryptoGuard: Branchenführender, universeller Schutz vor Ransomware

Sophos Endpoint bietet mehrschichtigen Schutz vor Ransomware und umfasst unter anderem CryptoGuard, unsere einzigartige Anti-Ransomware-Technologie, die in allen Sophos Endpoint Subscriptions enthalten ist.

Endpoint-Security-Lösungen anderer Anbieter suchen lediglich nach schädlichen Dateien und Prozessen. CryptoGuard analysiert Datendateien dagegen auf Anzeichen schädlicher Verschlüsselung – unabhängig vom Ausführungsort der Prozesse. Auf diese Weise bietet unsere Lösung hocheffektiven Schutz vor Ransomware aller Art, einschließlich unbefugter Remote-Verschlüsselung. Erkennt CryptoGuard eine schädliche Verschlüsselung, wird die Aktivität blockiert und Dateien werden automatisch in den unverschlüsselten Ursprungszustand zurückversetzt.

CryptoGuard prüft den Inhalt aller Dokumente aktiv beim Lese- und Schreibzugriff auf Dateien und stellt anhand mathematischer Analysen fest, ob sie verschlüsselt wurden. Dieser universelle Ansatz ist branchenweit einzigartig. Sophos Endpoint stoppt Ransomware-Angriffe, Remote-Ransomware und komplett neue Ransomware, die Lösungen anderer Anbieter übersehen.

CryptoGuard, eine der leistungsstarken Schutztechnologien in Sophos Endpoint, ist in allen Subscriptions von Sophos Intercept X Advanced, Sophos XDR und Sophos MDR enthalten. Die Funktion ist standardmäßig automatisch aktiviert. So werden Unternehmen und Einrichtungen sofort und ohne Feinabstimmung oder Konfiguration umfassend vor lokaler und Remote-Ransomware geschützt.

- **Analysiert Datei-Inhalte und erkennt so unbefugte Verschlüsselungen**

  Andere Lösungen betrachten Ransomware aus einer Anti-Malware-Perspektive und konzentrieren sich auf die Erkennung von schädlichem Code. CryptoGuard analysiert Datei-Inhalte mithilfe mathematischer Algorithmen und ermittelt so schnelle Massenverschlüsselungen von Dateien.

- **Blockiert lokale und Remote-Ransomware**

  CryptoGuard konzentriert sich auf Datei-Inhalte und kann deshalb Ransomware-Verschlüsselungs-Versuche auch dann erkennen, wenn der schädliche Prozess nicht auf dem Gerät des Opfers ausgeführt wird.

- **Setzt schädliche Verschlüsselungen automatisch zurück**

  CryptoGuard erstellt temporäre Sicherungen modifizierter Dateien und setzt Änderungen automatisch zurück, wenn Massenverschlüsselungen erkannt werden. Lösungen anderer Anbieter verwenden den Volume-Schattenkopie-Dienst von Windows, den Angreifer überlisten können. Sophos setzt hingegen auf proprietäre Technologie. Verschlüsselte Dateien werden unabhängig von Größe oder Dateityp wiederhergestellt. So lassen sich Betriebsstörungen auf ein Minimum reduzieren.

- **Blockiert Remote-Geräte automatisch**

  Bei einem Ransomware-Angriff blockiert CryptoGuard automatisch IP-Adressen von Remote-Geräten, die versuchen, Dateien auf den Geräten der Opfer zu verschlüsseln.

- **Schützt den Master Boot Record (MBR)**

  CryptoGuard schützt das Gerät auch vor Ransomware, die den Master Boot Record verschlüsselt (und somit das Hochfahren verhindert), sowie vor Angriffen, bei denen die Festplatte gelöscht wird.

Ermitteln Sie ungeschützte Geräte

Ein einziger ungeschützter Endpoint kann Ihr Unternehmen/Ihre Organisation anfällig für Remote-Verschlüsselung machen. Sophos Endpoint bietet robusten, universellen Ransomware-Schutz vor unbefugter Verschlüsselung. Aber wie erkennen Sie ungeschützte Geräte in Ihrem Netzwerk?

Hier hilft Sophos Network Detection and Response (NDR). Sophos NDR überwacht den Netzwerkverkehr auf verdächtige Verkehrsflüsse und ermittelt so ungeschützte Geräte und nicht autorisierte Assets in der Umgebung.

Um den bestmöglichen Schutz vor Remote-Ransomware zu gewährleisten, empfehlen wir, Sophos Endpoint auf allen Systemen in der Umgebung zu installieren und gleichzeitig Sophos NDR zur Ermittlung ungeschützter Geräte im Netzwerk bereitzustellen.

Verbessern Sie jetzt Ihren Schutz vor Remote-Ransomware

Schädliche Remote-Verschlüsselung ist eine beliebte Ransomware-Technik und kann von den meisten führenden Endpoint-Security-Lösungen nur schwer gestoppt werden. Wenn Sie eine andere Lösung als Sophos Endpoint nutzen, sind Sie mit hoher Wahrscheinlichkeit gefährdet.

Sie möchten mehr zu Sophos Endpoint wissen und verstehen, wie Sie sich besser vor modernen Angriffen wie Remote-Ransomware schützen können?

> Kontaktieren Sie uns, wir beraten Sie gerne!

Oder testen Sie Sophos Endpoint 30 Tage lang kostenlos und unverbindlich in Ihrer eigenen Umgebung.

1 Microsoft Digital Defense Report. https://www.microsoft.com/de-de/security/security-insider/microsoft-digital-defense-report-2023

2 Burt, T. (5. Oktober 2023). Spionage treibt Cyberangriffe auf globaler Ebene an. Microsoft. https://blogs.microsoft.com/on-the-issues/2023/10/05/microsoft-digital-defense-report-2023-global-cyberattacks/

Sophos bietet branchenführende Cybersecurity-Lösungen für Unternehmen jeder Größe und schützt Kunden in Echtzeit vor komplexen Bedrohungen wie Malware, Ransomware und Phishing. Bewährte Next-Gen-Funktionen mit der Power von Machine Learning und künstlicher Intelligenz sichern Unternehmensdaten effektiv.

2023-12-06 (WP-DD)