SOPHOS

Ungepatchte Schwachstellen: Der verheerendste Angriffsvektor bei Ransomware

Einfluss der Angriffsursache auf die Auswirkungen von Ransomware-Angriffen, basierend auf den Erkenntnissen von 2.974 Unternehmen, die im vergangenen Jahr von Ransomware betroffen waren.

Sophos-Whitepaper, April 2024

Einführung

Um einen Ransomware-Angriff auszuführen, müssen sich Angreifer zunächst Zugang zur IT-Umgebung, den Geräten und Daten des ins Visier genommenen Unternehmens verschaffen. Bedrohungsakteure greifen dabei hauptsächlich auf zwei Angriffsvektoren zurück: Sie melden sich mit **kompromittierten Zugangsdaten** (d. h. mit legitimen, gestohlenen Anmeldedaten) an und sie nutzen **Schwachstellen** in Unternehmensanwendungen und -Tools aus. Andere, weniger verbreitete Angriffswege sind Brute-Force-Angriffe, Supply-Chain-Angriffe, schädliche E-Mails/Dokumente und Adware. Phishing spielt bei Ransomware-Angriffen eine große Rolle, dient aber in erster Linie dem Diebstahl von Zugangsdaten, mit denen sich Cyberkriminelle dann im Unternehmen anmelden können.

Der Report zeigt Unterschiede in den Auswirkungen von Ransomware je nach Angriffsursache. Dabei beleuchtet er den Schweregrad, die finanziellen Folgen sowie die betrieblichen Auswirkungen von Angriffen, die von ausgenutzten Schwachstellen ausgehen, im Vergleich zu Angriffen über kompromittierte Zugangsdaten. Außerdem geht der Report auf die am stärksten und am wenigsten betroffenen Branchen ein.

Sophos hat eine unabhängige Befragung von 2.974 IT-/Cybersecurity-Entscheidern in kleinen und mittelständischen Unternehmen mit 100 bis 5.000 Mitarbeitern in Auftrag gegeben. Alle beteiligten Unternehmen waren im vergangenen Jahr von Ransomware betroffen. Die Umfrage wurde Anfang 2024 vom Marktforschungsinstitut Vanson Bourne durchgeführt und bezieht sich auf die Erfahrungen der Umfrageteilnehmer in den letzten 12 Monaten.

Kurzfassung

Ransomware-Angriffe haben immer negative Folgen. Angriffe, die von ungepatchten Schwachstellen ausgehen, sind jedoch besonders gravierend. So meldeten Unternehmen, die von diesen Angriffen betroffen waren, erheblich schwerwiegendere Auswirkungen als Unternehmen, bei denen kompromittierte Zugangsdaten als Einfallstor dienten. Zudem zeichneten sich die folgenden Tendenzen ab:

- Backups wurden kompromittiert
  (Erfolgsquote 75 % ggü. 54 % bei kompromittierten Anmeldedaten)
- Daten wurden verschlüsselt
  (Verschlüsselungsrate 67 % ggü. 43 % bei kompromittierten Anmeldedaten)
- Unternehmen zahlten das Lösegeld
  (71 % Zahlungsrate ggü. 45 % bei kompromittierten Anmeldedaten)
- Unternehmen trugen die Lösegeldkosten selbst
  (31 % ggü 2 % bei kompromittierten Anmeldedaten)

Sie berichteten auch über:

- 4 Mal höhere Bereinigungskosten nach einem Angriff
  (3 Mio. USD ggü. 750.000 USD bei kompromittierten Anmeldedaten)
- Längere Ausfallzeiten
  (45 % benötigen mehr als einen Monat zur Wiederherstellung ggü. 37 % bei kompromittierten Anmeldedaten)

Der Report konzentriert sich auf die Korrelation. Die Gründe für diese Ergebnisse müssen jedoch noch weiter analysiert werden, denn nicht alle Ransomware-Angriffe sind gleich. Einerseits werden Angriffe von raffinierten, gut finanzierten Cyberbanden mit innovativen Methoden ausgeführt. Andererseits nimmt der Einsatz von einfacher, billiger Ransomware durch weniger versierte Bedrohungsakteure zu. Möglicherweise verfügen Cyberkriminelle, die ungepatchte Software-Schwachstellen ausnutzen können, über mehr Know-how und sind so eher in der Lage, Backups zu kompromittieren und Daten zu verschlüsseln als Angreifer, die gestohlene Anmeldedaten (z. B. im Dark Web) kaufen.

Erkenntnis 1: Ein Drittel der Ransomware-Angriffe beginnt mit der Ausnutzung einer ungepatchten Schwachstelle

32 % der Ransomware-Angriffe, mit denen die Umfrageteilnehmer im vergangenen Jahr konfrontiert waren, ließen sich auf ausgenutzte Schwachstellen zurückführen. Bei genauerer Betrachtung zeigt sich, dass der Anteil dieser Ransomware-Angriffe je nach Branche stark variiert:

- Höchster Anteil: Energie, Öl/Gas und Versorgungsunternehmen – 49 % der Angriffe
- Niedrigster Anteil: Bauwesen und Immobilien – 21 % der Angriffe

Wahrscheinlich lässt sich diese Diskrepanz zum Teil auf unterschiedliche Technologielösungen und die damit verbundenen Patching-Probleme zurückführen. Branchen wie Energie, Öl/Gas und Versorgungsunternehmen haben in der Regel einen höheren Anteil älterer Technologien im Einsatz, die anfälliger für Schwachstellen sind. Zudem sind für veraltete und nicht mehr unterstützte Lösungen möglicherweise keine Patches verfügbar.

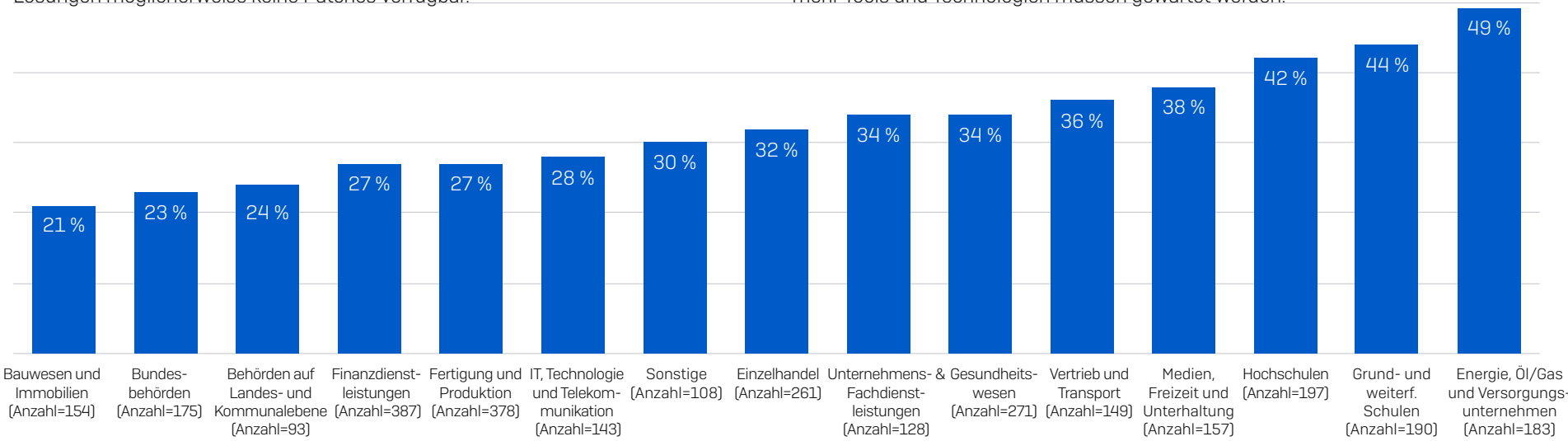
Prozentualer Anteil der Angriffe, bei denen Schwachstellen ausgenutzt wurden

Tatsächlich sind in vielen Fällen Patches durchaus vorhanden, sie wurden jedoch nicht rechtzeitig installiert. Von den Angriffen, zu deren Behebung Sophos-Incident-Responder im Jahr 2022 hinzugezogen wurden und die auf ausgenutzten Schwachstellen basierten, wurden über die Hälfte (55 %) durch ProxyShell und Log4Shell verursacht. Für beide gab es zum Zeitpunkt der Kompromittierung bereits Patches. Auch 30 Monate nach der Veröffentlichung des Patches liegen Sophos noch Belege dafür vor, dass ProxyShell weiterhin ausgenutzt wird. Mehr erfahren.

Die Analyse ergab auch, dass die Wahrscheinlichkeit eines durch einen Exploit ausgelösten Angriffs je nach Unternehmensgröße unterschiedlich hoch ist:

- 26 % der Ransomware-Angriffe in kleinen Unternehmen (Jahresumsatz unter 50 Mio. USD)
- 30 % der Ransomware-Angriffe in mittleren Unternehmen (50 Mio.–1 Mrd. USD)
- 37 % der Ransomware-Angriffe in großen Unternehmen (ab 1 Mrd. USD)

Wenn Unternehmen wachsen, wächst auch ihre IT-Infrastruktur. Je größer die Umgebung, desto schwieriger lässt sich die Angriffsfläche nachvollziehen und desto mehr Tools und Technologien müssen gewartet werden.



Erkenntnis 2: Die Auswirkungen von Ransomware sind schwerwiegender, wenn der Angriff von einer ausgenutzten Schwachstelle ausgeht

Das eigentliche Ziel von Ransomware-Akteuren besteht darin, die Daten eines Unternehmens zu verschlüsseln und im Gegenzug Lösegeld für den Entschlüsselungsschlüssel zu fordern. Auf dem Weg dorthin versuchen sie fast immer, die Backups der betroffenen Unternehmen zu kompromittieren, um deren Möglichkeiten zur Wiederherstellung von Daten ohne Lösegeldzahlung einzuschränken.

Die Analyse zeigt, dass die Auswirkungen bei allen drei Aspekten – Kompromittierung von Backups, Datenverschlüsselung und Lösegeldzahlung – am gravierendsten sind, wenn der Angriff von einer ausgenutzten Schwachstelle herrührt.

Kompromittierung von Backups

Die Angriffsursache hat keinen Einfluss auf die Wahrscheinlichkeit, dass Backups kompromittiert werden. Bei 96 % der Angriffe, die von ausgenutzten Schwachstellen und kompromittierten Anmeldedaten ausgingen, versuchten die Angreifer, Backups zu kompromittieren. Erhebliche Unterschiede lassen sich dagegen bei der Erfolgsquote verzeichnen:

- 75 % der Angriffe, die von ausgenutzten Schwachstellen ausgingen, waren erfolgreich
- 54 % der auf kompromittierten Anmeldedaten basierten Angriffe waren erfolgreich

Dies könnte darauf zurückzuführen sein, dass Angreifer, die ungepatchte Schwachstellen ausnutzen, eher dazu fähig sind, Backups zu beeinträchtigen. Möglicherweise verfügen Unternehmen mit einer ungeschützten Angriffsfläche jedoch auch über einen schwächeren Backup-Schutz. Von der Angriffsursache einmal abgesehen: Wenn Ihre Backups kompromittiert werden, verringert sich Ihre Resilienz gegen die vollen Auswirkungen des Angriffs.

Datenverschlüsselung

Wenn ein Angriff von einer ausgenutzten Schwachstelle und nicht von kompromittierten Anmeldedaten ausgeht, ist die Datenverschlüsselungsrate um mehr als 50 % höher:

- 67 % der Angriffe, die von ausgenutzten Schwachstellen ausgingen, führten zu Datenverschlüsselung
- 43 % der Angriffe, die durch kompromittierte Anmeldedaten verursacht wurden, führten zu Datenverschlüsselung

Wie bei der Kompromittierung von Backups lassen sich die Diskrepanzen bei den Ergebnissen je nach Ursache möglicherweise auf Unterschiede bei den Kompetenzen der Angreifer sowie Ungleichheiten bei der Cyberabwehr der Unternehmen zurückführen.

Lösegeldzahlungsquote

Angesichts der höheren Rate an kompromittierten Backups bei Angriffen, die von ausgenutzten Schwachstellen ausgingen, überrascht es wohl kaum, dass die Bereitschaft zur Zahlung des Lösegelds hier auch entsprechend höher ausfiel:

- 71 % der Unternehmen, deren Daten verschlüsselt wurden, zahlten das Lösegeld, wenn der Angriff von ausgenutzten Schwachstellen verursacht wurde
- 45 % der Unternehmen, deren Daten verschlüsselt wurden, zahlten das Lösegeld, wenn der Angriff von kompromittierten Anmeldedaten ausging

Ohne wiederherstellbare Backups sind Ransomware-Opfer häufiger auf den Entschlüsselungsschlüssel angewiesen und sind eher geneigt, mit den Angreifern zusammenzuarbeiten, um die Daten wiederherzustellen.

Erkenntnis 3: Ungepatchte Schwachstellen haben geschäftskritische Konsequenzen

Ransomware-Angriffe, die von ausgenutzten Schwachstellen ausgehen, haben wesentlich größere finanzielle und betriebliche Auswirkungen als solche, die mit kompromittierten Anmeldedaten beginnen.

Lösegeldzahlung

Zwar wirkt sich die Angriffsursache nur unwesentlich auf die Höhe der Lösegeldzahlung aus (durchschnittlich 1,988 Mio. USD bei ausgenutzten Schwachstellen ggü. 2 Mio. USD bei kompromittierten Zugangsdaten), bei der Finanzierung des Lösegelds spielt sie aber eine entscheidende Rolle:

- 31 % der betroffenen Unternehmen finanzierten das volle Lösegeld selbst, wenn der Angriff über ausgenutzte Schwachstellen erfolgte
- 2 % der betroffenen Unternehmen finanzierten das gesamte Lösegeld selbst, wenn sich die Angreifer über kompromittierte Zugangsdaten Zugriff verschafften

Muttergesellschaften und Cyberversicherungen beteiligen sich eher an der Lösegeldsumme, wenn der Angriff von kompromittierten Anmeldedaten und nicht von ausgenutzten Schwachstellen ausgeht.

Mit Hinblick auf die Bereitschaft der Versicherungsträger, Schäden zu übernehmen, lässt sich Folgendes feststellen: Ein Viertel (25 %) der abgelehnten Ansprüche in Unternehmen, die von einer ausgenutzten Schwachstelle betroffen waren, war darauf zurückzuführen, dass sie nicht über die vom Versicherer vorausgesetzten Cyberschutzmaßnahmen verfügten. Bei Cyberangriffen, die auf kompromittierte Zugangsdaten zurückgingen, belief sich der prozentuale Anteil auf 12 % der Ansprüche.

Bereinigungskosten

Neben der Begleichung des Lösegelds kommen jedoch noch viele weitere Kosten auf die betroffenen Unternehmen zu. Abgesehen von gezahlten Lösegeldsummen belaufen sich die durchschnittlichen Bereinigungskosten bei Ransomware-Angriffen, die auf ausgenutzte Schwachstellen zurückzuführen sind, im Schnitt auf 3 Mio. USD. Sie sind damit viermal höher als bei Angriffen, die durch kompromittierte Zugangsdaten verursacht werden (750.000 USD).

Ausfallzeiten

Auch die Wiederherstellung nach Angriffen, bei denen Schwachstellen als Einfallstor ausgenutzt wurden, gestaltet sich wesentlich langwieriger als beim Angriffsvektor „kompromittierte Zugangsdaten".

- 45 % der Unternehmen, die über eine ausgenutzte Schwachstelle angegriffen wurden, benötigten mehr als einen Monat für die Wiederherstellung
- 37 % der Unternehmen, die über kompromittierte Zugangsdaten angegriffen wurden, benötigten mehr als einen Monat für die Wiederherstellung

Dieses Ergebnis spiegelt wahrscheinlich die unterschiedlichen Abhilfemaßnahmen wider, die die betroffenen Unternehmen je nach Ursache ergreifen müssen, sowie den damit verbundenen Mehraufwand. Das Patchen eines Systems oder das Upgrade eines End-of-Life-Produkts auf eine unterstützte Version kann mitunter mehr Zeit in Anspruch nehmen als das Zurücksetzen der Zugangsdaten. Eine weitere mögliche Erklärung ist der größere Schaden, der durch Angriffe verursacht wird, bei denen Schwachstellen als Einfallstor ausgenutzt werden. Hinzu kommt eine höhere Wahrscheinlichkeit, dass Backups kompromittiert und Daten verschlüsselt werden.

Empfehlungen

Patches sind ein wichtiger erster Schritt zur Minimierung des Risikos, Opfer eines Ransomware-Angriffs (oder einer anderen Sicherheitsverletzung) zu werden, der von Schwachstellen ausgeht. Wenn Sie die Sicherheitslücke schließen, können Angreifer sie nicht ausnutzen. Idealerweise sollte Patching Teil einer umfassenderen Risikomanagement-Strategie zur Exploit-Abwehr sein.

Reduzieren Sie Ihre Angriffsfläche

- Verschaffen Sie sich einen umfassenden Überblick über Ihre externen Assets. So können Sie blinde Flecken vermeiden.
- Setzen Sie beim Patchen auf risikobasierte Priorisierung. Da neue Schwachstellen schneller entdeckt werden, als die meisten Unternehmen sie beheben können, sollten Sie sich auf besonders anfällige Bereiche konzentrieren. Dabei gilt es, Patches für Schwachstellen mit hohem Risiko zu identifizieren und zu priorisieren.
- Installieren Sie Updates regelmäßig. Durch die Verwendung der neuesten Version einer Anwendung oder eines Tools profitieren Sie von den neuesten Sicherheitsverbesserungen des Anbieters.

Stellen Sie Anti-Exploit-Schutz bereit

Auch wenn die Zahl der ausnutzbaren Schwachstellen weiterhin rapide ansteigt, können Angreifer nur auf eine begrenzte Anzahl an Exploit-Techniken zurückgreifen. Integrierter Anti-Exploit-Schutz in Endpoint-Sicherheitslösungen stoppt die bei diesen Angriffen verwendeten Verhaltensweisen. Dies gilt auch für Zero-Day-Schwachstellen, für die noch kein Patch veröffentlicht wurde.

Erkennen und stoppen Sie verdächtige Aktivitäten

Technologie-Lösungen allein können nicht jeden Angriff stoppen. Cyberkriminelle nutzen legitime IT-Tools und gestohlene Zugangsdaten aus und passen ihre Methoden kontinuierlich an, um unerkannt zu bleiben. Um komplexe, manuelle Ransomware-Angriffe und Sicherheitsverletzungen zu stoppen, ist 24/7 Detection and Response in Ihrer gesamten Umgebung durch einen spezialisierten Anbieter oder ein hochqualifiziertes internes Team erforderlich.

Wie Sophos helfen kann

Sophos Managed Risk

Sophos Managed Risk ist ein Service zum Management von Schwachstellen und Angriffsflächen, der auf branchenführender Tenable-Technologie basiert und von einem Expertenteam für Threat Exposure und Threat Remediation bereitgestellt wird. Damit lassen sich vier wichtige Anwendungsfälle abdecken: Einblick in Angriffsflächen, kontinuierliches Risiko-Monitoring, Schwachstellen-Priorisierung und schnelle Identifizierung neuer Risiken.

Sophos Managed Risk ist verfügbar über Sophos MDR, einen Fully Managed 24/7 Cybersecurity-Service, der von den Bedrohungsexperten von Sophos bereitgestellt wird. Ein dediziertes Team von Managed-Risk-Experten, das auf Schwachstellen und Threat Exposure spezialisiert ist, arbeitet rund um die Uhr eng mit den Sophos MDR-Analysten zusammen. Mehr erfahren.

Sophos Endpoint

Sophos Endpoint umfasst mehr als 60 Anti-Exploit-Funktionen, die Verhaltensweisen blockieren, mit denen Angreifer ungepatchte Schwachstellen ausnutzen, und so sowohl bekannte Sicherheitslücken als auch Zero-Day-Bedrohungen stoppen. Die Anti-Exploit-Funktionen werden automatisch bereitgestellt – ganz ohne Konfiguration.

Sophos Endpoint nutzt einen umfassenden Schutz-Ansatz und verlässt sich nicht auf eine einzelne Sicherheitstechnologie. Web, Anwendungs- und Peripherie-Kontrollen reduzieren Ihre Angriffsfläche und blockieren gängige Angriffsvektoren. KI, Verhaltensanalysen, Anti-Ransomware und weitere hochmoderne Technologien stoppen Bedrohungen schnell, bevor diese sich ausweiten. Mehr erfahren.

2024-03-27 (WP-PC)

SOPHOS