SOPHOS

Die Auswirkungen kompromittierter Backups auf Ransomware-Angriffe

Erkenntnisse von 2.974 Unternehmen und Organisationen, die im letzten Jahr von Ransomware-Angriffen betroffen waren

Sophos-Whitepaper, März 2024

Einführung

Bei einem Ransomware-Angriff gibt es im Wesentlichen zwei Optionen zur Wiederherstellung verschlüsselter Daten: Zurückspielen der Daten aus Backups und Zahlung des Lösegelds. Indem Ransomware-Akteure die Datensicherung ihrer Opfer kompromittieren, vereiteln sie die Wiederherstellung verschlüsselter Daten aus Backups und erhöhen so den Druck, das Lösegeld zu zahlen.

Dieser Report bietet Ihnen einen umfassenden Einblick in die Auswirkungen der Backup-Kompromittierung auf Ransomware-Angriffe. Zudem erfahren Sie mehr darüber, wie häufig Backups im Rahmen von Ransomware-Angriffen beeinträchtigt werden.

Hintergrund

Sophos hat eine unabhängige Befragung von 2.974 IT-/Cybersecurity-Entscheidern in Unternehmen und Organisationen aus 14 Ländern in Auftrag gegeben. Alle beteiligten Unternehmen und Organisationen waren im vergangenen Jahr von Ransomware betroffen. Die Umfrage wurde vom Marktforschungsinstitut Vanson Bourne zwischen Januar und Februar 2024 durchgeführt und bezieht sich auf die Erfahrungen der Umfrageteilnehmer in den letzten 12 Monaten. Weitere Informationen zu den Umfrageteilnehmern entnehmen Sie bitte dem Anhang am Ende des Reports.

Kurzfassung

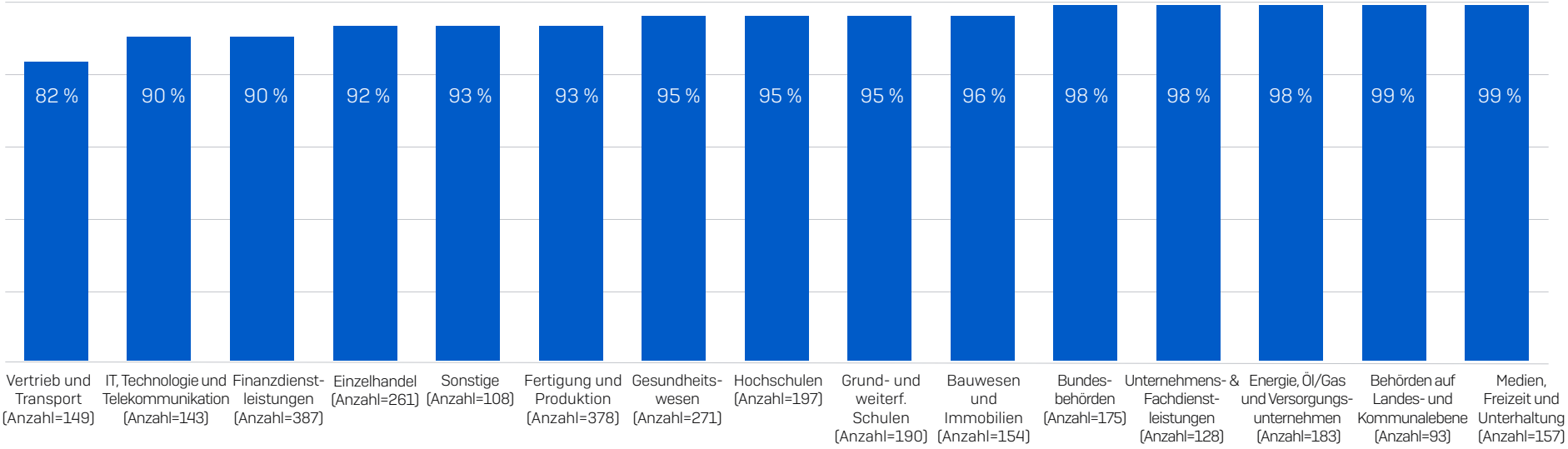
Die finanziellen und betrieblichen Auswirkungen eines Ransomware-Angriffs, bei dem Backups kompromittiert werden, sind immens. Gelingt es Cyberkriminellen, Backups zu schädigen, ist die Wahrscheinlichkeit, dass ein Unternehmen/eine Organisation das Lösegeld zahlen muss, fast doppelt so hoch. Darüber hinaus fallen die Gesamtkosten für die Wiederherstellung achtmal höher aus als bei Unternehmen/Organisationen, deren Backups nicht betroffen sind.

Wenn Sie böswillige Akteure erkennen und stoppen, bevor Ihre Datensicherung kompromittiert wird, können Sie die Folgen eines Ransomware-Angriffs für Ihr Unternehmen/Ihre Organisation minimieren. So bietet Ihnen eine Investition in Präventivmaßnahmen nicht nur mehr Schutz vor Ransomware, sondern senkt auch die Gesamtausgaben für Ihre Cybersicherheit.

Erkenntnis 1: Ransomware-Akteure versuchen in der Regel, Ihre Backups zu kompromittieren

Bei 94 % der Befragten, die im vergangenen Jahr von Ransomware betroffen waren, haben Cyberkriminelle im Rahmen des Angriffs versucht, auch die Backups zu schädigen. Bei Behörden auf Landes- und Kommunalebene sowie im Medien-, Freizeit- und Unterhaltungssektor lag der prozentuale Anteil sogar bei 99 %. Im Bereich Vertrieb und Transport wurden die wenigsten Kompromittierungsversuche gemeldet. Doch selbst in dieser Branche bestätigten mehr als acht von zehn (82 %) der von Ransomware betroffenen Unternehmen und Organisationen, dass die Angreifer versucht hatten, auf ihre Backups zuzugreifen.

Prozentualer Anteil der Ransomware-Angriffe, bei denen die Angreifer versuchten, Backups zu kompromittieren



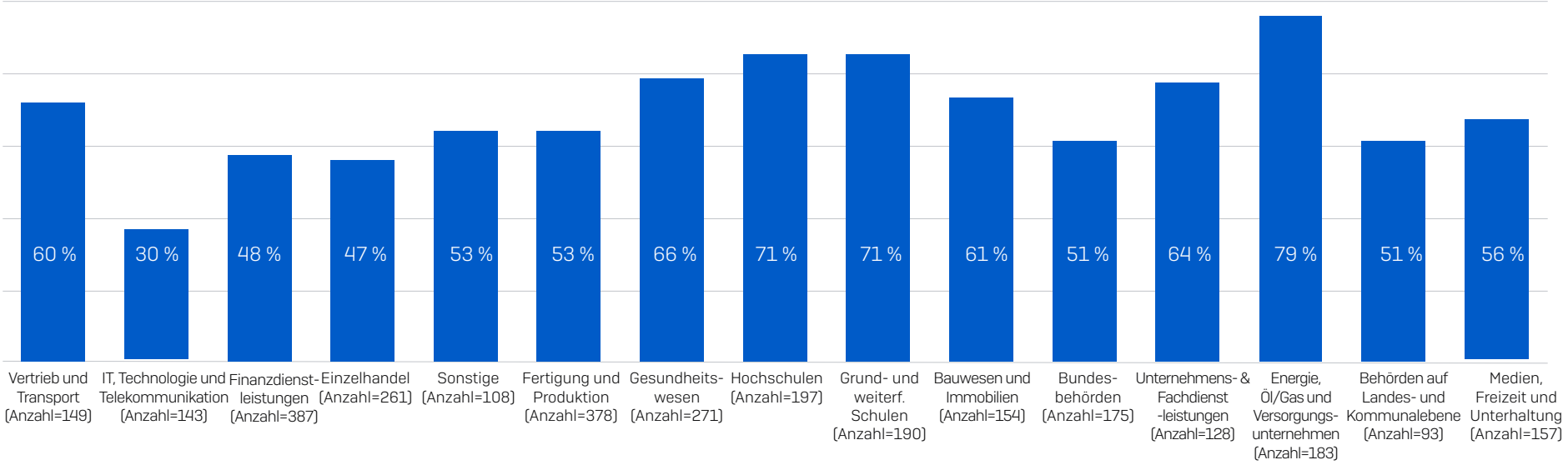
Erkenntnis 2: Die Erfolgsquote bei Kompromittierungen variiert stark nach Branche

In allen Branchen waren 57 % der Versuche, Backups zu kompromittieren, erfolgreich. Somit konnten Cyberkriminelle die Wiederherstellung nach einem Ransomware-Angriff bei mehr als der Hälfte ihrer Opfer beeinträchtigen. Interessanterweise zeichneten sich im Branchenvergleich signifikante Unterschiede bei der Erfolgsquote der Angreifer ab:

- In den Bereichen Energie, Öl/Gas und bei den Versorgungsunternehmen (Erfolgsquote: 79 %) sowie im Bildungswesen (Erfolgsquote: 71 %) gelang es Angreifern am häufigsten, die Backups ihrer Opfer zu schädigen.
- In der IT, Technologie und Telekommunikation (Erfolgsquote: 30 %) sowie im Einzelhandel (Erfolgsquote: 47 %) wurden Backups dagegen am seltensten kompromittiert.

Die unterschiedlichen Erfolgsquoten lassen sich auf mehrere mögliche Gründe zurückführen. Vermutlich verfügten Unternehmen und Organisationen aus den Bereichen IT, Telekommunikation und Technologie über einen stärkeren Backup-Schutz und waren so besser gegen den Angriff gewappnet. Möglicherweise waren sie auch besser in der Lage, Kompromittierungsversuche rechtzeitig zu erkennen und zu stoppen. Es kann auch sein, dass Energie-, Öl-/Gas- und Versorgungsunternehmen von besonders komplexen Angriffen betroffen waren. Doch von der Ursache ganz abgesehen: Die Folgen können in allen Fällen verheerend sein.

Erfolgsquote von Versuchen, Backups zu kompromittieren



Erkenntnis 3:
Lösegeldforderungen und -zahlungen verdoppeln sich bei kompromittierten Backups

Datenverschlüsselung

In Unternehmen und Organisationen, deren Backups kompromittiert wurden, wurden 63 % häufiger Daten im Zuge eines Ransomware-Angriffs verschlüsselt als bei Unternehmen und Organisationen mit intakten Backups: Bei 85 % der Unternehmen und Organisationen mit kompromittierten Backups gelang es den Angreifern, die Daten ihrer Opfer zu verschlüsseln. In Unternehmen und Organisationen, deren Backups nicht betroffen waren, lag der prozentuale Anteil dagegen bei 52 %. Möglicherweise deutet die höhere Verschlüsselungsrate auf eine insgesamt schwächere Cyber-Resilienz hin, d. h. Unternehmen und Organisationen sind weniger in der Lage, sich gegen alle Phasen eines Ransomware-Angriffs zu verteidigen.

Lösegeldforderungen

Bei Ransomware-Angriffen mit kompromittierten Backups fielen Lösegeldforderungen im Schnitt mehr als doppelt so hoch aus: So betrug die geforderte Summe durchschnittlich 2,3 Mio. US-Dollar (Backups kompromittiert) ggü. 1 Mio. US-Dollar (Backups intakt). Vermutlich schätzen Cyberkriminelle ihre Verhandlungsbasis als stärker ein, wenn sie Backups beeinträchtigen, und fordern entsprechend höhere Summen.

Lösegeld-Zahlungsquote

Unternehmen und Organisationen, deren Backups beeinträchtigt wurden, zahlten fast doppelt so häufig Lösegeld, um ihre verschlüsselten Daten wiederherstellen zu können, als Unternehmen und Organisationen, deren Backups nicht betroffen waren (67 % ggü. 36 %).

Höhe der Lösegeldzahlungen

Im Schnitt beliefen sich Lösegeldzahlungen von Unternehmen und Organisationen, deren Backups kompromittiert wurden, auf 2 Mio. US-Dollar und fielen damit fast doppelt so hoch aus als bei Unternehmen und Organisationen, deren Backups intakt blieben (1,062 Mio. US-Dollar). Zudem waren Unternehmen und Organisationen mit kompromittierten Backups auch seltener in der Lage, das Lösegeld herunterzuhandeln und zahlten im Schnitt 98 % der geforderten Summe. Dagegen konnten Ransomware-Opfer mit unversehrten Backups das Lösegeld auf 82 % der Forderung reduzieren.

Datenverschlüsselungsrate

89 %
bei kompromittierten Backups

52 %
bei intakten Backups

Lösegeldforderung (Durchschnitt)

$2,3 Mio. bei kompromittierten Backups

$1 Mio. bei intakten Backups

Zahlten Lösegeld zur Datenwiederherstellung

67 %
bei kompromittierten Backups

36 %
bei intakten Backups

Lösegeldzahlung (Durchschnitt)

$2,3 Mio. bei kompromittierten Backups

$1,062 Mio. bei intakten Backups

Erkenntnis 4: Die Bereinigungskosten fallen achtmal höher aus, wenn Backups kompromittiert werden

Nicht bei allen Ransomware-Angriffen wird Lösegeld gezahlt. Doch unabhängig davon, ob eine Zahlung erfolgt oder nicht, führt ein Ransomware-Angriff zu erheblichen Bereinigungskosten. Häufig haben Ausfälle aufgrund von Ransomware signifikante Auswirkungen auf das Tagesgeschäft. Darüber hinaus erweist sich die Wiederherstellung von IT-Systemen oft als komplexes und kostspieliges Unterfangen.

Die durchschnittlichen Bereinigungskosten nach Ransomware-Angriffen waren in Unternehmen und Organisationen, deren Backups kompromittiert wurden, mit 3 Mio. US-Dollar achtmal höher als in Unternehmen und Organisationen, deren Backups nicht betroffen waren (375.000 US-Dollar). Diese Diskrepanz ist vermutlich auf mehrere Gründe zurückzuführen, wie etwa den zusätzlichen Aufwand, der in der Regel mit der Wiederherstellung von entschlüsselten Daten ohne intakte Backups einhergeht. Möglicherweise weist ein schwächerer Backup-Schutz zudem auf eine weniger robuste Cyberabwehr und einen damit verbundenen erhöhten Wiederherstellungsaufwand hin.

Bei Unternehmen und Organisationen, deren Backups kompromittiert wurden, nahm die Wiederherstellung wesentlich mehr Zeit in Anspruch: Nur 26 % der Daten wurden innerhalb einer Woche vollständig wiederhergestellt, verglichen mit 46 % in Unternehmen und Organisationen mit intakten Backups.

Gesamt-Bereinigungskosten (Durchschnitt)

$ 3 Mio.	bei kompromittierten Backups
$ 0,375 Mio.	bei intakten Backups

Empfehlungen

Backups sind ein zentraler Bestandteil einer ganzheitlichen Cyberabwehr-Strategie. Wenn Ihre Backups online zugänglich sind, können Sie davon ausgehen, dass Angreifer sie finden. Empfehlungen für Unternehmen und Organisationen:

- Erstellen Sie regelmäßig Backups und speichern Sie diese an mehreren Orten. Sichern Sie Ihre Backup-Konten in der Cloud durch mehrstufige Authentifizierung, um den Zugriff durch Cyberkriminelle zu verhindern.
- Proben Sie die Wiederherstellung aus Backups. Je vertrauter Sie mit dem Wiederherstellungsprozess sind, desto schneller und einfacher können Sie sich von einem Vorfall erholen.
- Schützen Sie Ihre Backups. Überwachen Sie verdächtige Aktivitäten in Zusammenhang mit Ihren Backups und reagieren Sie darauf, denn möglicherweise versuchen Angreifer, Ihre Backups zu kompromittieren.

So kann Sophos helfen

Sophos MDR: Unsere Experten schützen Ihre Backups

Sophos MDR ist ein 24/7 Managed Detection and Response Service, der durch ein Team von Sicherheitsexperten bereitgestellt wird. Diese sind auf das Erkennen und Bekämpfen komplexer Cyberangriffe spezialisiert, gegen die reine Technologie-Lösungen machtlos sind. Der Service erweitert Ihr IT-/Sicherheitsteam um über 500 Spezialisten, die Ihre Umgebung überwachen, verdächtige Aktivitäten und Warnhinweise erkennen, analysieren und darauf reagieren.

Sophos MDR-Analysten nutzen Telemetriedaten Ihrer Backup- und Wiederherstellungslösung, um Kompromittierungsversuche zu erkennen und zu stoppen, bevor größerer Schaden entsteht. Außerdem werten sie Signale Ihrer vorhandenen Sicherheitstools aus, einschließlich Ihrer Endpoint-, E-Mail- und Firewall-Lösungen, und erkennen so Ransomware und Sicherheitsverletzungen. Im Schnitt beheben die MDR-Experten von Sophos Vorfälle in nur 38 Minuten – so bleiben Sie Angreifern stets einen Schritt voraus.

Sophos XDR: Transparenz und Tools zur Abwehr von Angreifern

Sophos XDR liefert internen IT-Teams die nötige Transparenz und Tools, um in kürzester Zeit mehrphasige Bedrohungen an allen wichtigen Angriffsflächen zu analysieren und zu bekämpfen. Mit Sophos XDR können Sie Telemetriedaten von Ihrer Backup- und Wiederherstellungslösung und Ihren IT-Security-Tools nutzen, um Angriffe schnell zu erkennen und umgehend zu reagieren.

Anhang

An der Umfrage nahmen IT-Experten aus kleinen und mittelgroßen Unternehmen und Organisationen mit 100 bis 5.000 Mitarbeitern in 14 Ländern teil: Australien, Österreich, Brasilien, Frankreich, Deutschland, Indien, Italien, Japan, Singapur, Südafrika, Spanien, Schweiz, Vereinigtes Königreich, USA.

2024-03-18 (WP-NP)

SOPHOS