World Backup Day 2024:
Warum Cyberkriminelle gezielt Backups ins Visier nehmen und wie Security die Datensicherung schützen kann

Es gibt im Wesentlichen zwei Möglichkeiten, verschlüsselte Daten nach einem Ransomware-Angriff wiederherzustellen: die Wiederherstellung aus Backups und die Zahlung des Lösegelds. Zwei Probleme, gleiche Ursache: Die vollständige Wiederherstellung der Daten nach einer Lösegeldzahlung ist höchst ungewiss, denn auf ein Versprechen von Cyberkriminellen kann man sich im Zweifel nicht verlassen. Und das Rückspielen der Daten aus den Backups funktioniert in vielen Fällen deshalb nicht, weil die Cyberkriminellen oft auch diese verschlüsselt haben, um den Druck auf die Opfer, das Lösegeld zu bezahlen, dramatisch zu erhöhen. Unternehmen, die kein geschütztes Backup in der Hinterhand haben, sitzen in der Klemme. Daher ist es ratsam, die Security und die Datensicherung zu kombinieren, um den Schutz der Backups zu maximieren sowie zudem auf unveränderliche Backups zu setzen.

Harte Fakten belegen das Risiko
In einer Umfrage unter knapp 3.000 IT- und Cybersicherheitsexperten weltweit, die das Marktforschungsinstitut Vanson Bourne Anfang 2024 im Auftrag von Sophos durchführte, wurde deutlich, dass die finanziellen und betrieblichen Auswirkungen einer Kompromittierung von Backups durch einen Ransomware-Angriff immens sind. Insgesamt stechen vier Haupterkenntnisse aus der Umfrage ins Auge:

Erkenntnis 1: Ransomware-Angreifer versuchen fast immer, Ihre Backups zu kompromittieren. Bei 94 Prozent der Unternehmen, die im vergangenen Jahr von Ransomware betroffen waren, haben die Cyberkriminellen während des Angriffs versucht, auch die Backups zu kompromittieren.

Erkenntnis 2: Die Erfolgsquote bei Kompromittierungen variiert stark je nach Branche. Uber allen Branchen hinweg waren durchschnittlich 57 Prozent der Backup-Kompromittierungsversuche erfolgreich. Interessanterweise gibt es aber große Unterschiede in den unterschiedlichen Branchen, von 79 Prozent in den Sektoren Energie, Öl/Gas und Versorgung bis 30 Prozent für die Bereiche IT, Technologie und Telekommunikation.

Erkenntnis 3: Lösegeldforderungen verdoppeln sich, wenn Backups kompromittiert werden. Opfer, deren Backups kompromittiert wurden, erhielten im Durchschnitt mehr als doppelt so hohe Lösegeldforderungen wie diejenigen, deren Backups nicht betroffen waren. Die durchschnittlichen Lösegeldforderungen lagen bei 2,3 Millionen US-Dollar (Backups kompromittiert) und 1 Million US-Dollar (Backups nicht kompromittiert).

Erkenntnis 4: Die Kosten für die Wiederherstellung nach einem Ransomware-Angriff sind achtmal höher, wenn Backups kompromittiert sind. Durch Ransomware verursachte Ausfälle haben, neben potenziellen Lösegeldzahlungen, häufig erhebliche Auswirkungen auf den täglichen Geschäftsbetrieb. Zudem ist die Wiederherstellung von IT-Systemen komplex und teuer. Die durchschnittlichen Gesamtkosten für die Wiederherstellung nach einer Ransomware-Attacke betrugen bei Organisationen, deren Backups kompromittiert wurden, durchschnittlich 3 Millionen US-Dollar. Das entspricht der achtfachen Summe im Vergleich zu Organisationen, deren Backups nicht betroffen waren und die durchschnittlich 375.000 US-Dollar aufwenden mussten.

Alle Details zu der Backup-Umfrage können im englischen Blogartikel „The impact of compromised backups on ransomware outcomes“ nachgelesen werden.

Wichtige Tipps für den Schutz von Backups vor Ransomware
Unternehmen können mit Hilfe von Security-Services, wie Managed Detection and Response, böswillige Akteure in der kompletten IT-Infrastruktur rund um die Uhr erkennen und stoppen – noch bevor Systeme und damit auch die Backups kompromittiert werden. Dies hilft insbesondere solchen Unternehmen, die kein eigenes Security Operations Center (SOC) betreiben können oder keine eigenen Security-Spezialisten mit Forensikerfahrung und 24x7-Verfügbarkeit im Team haben.
Zudem ist es sinnvoll, das Backup mit dem Security-Ökosystem zu integrieren. Die Backup-Systeme sollten ähnlich wie alle Endpoints kontinuierlich und aktiv vor Ransomware und anderen böswilligen Beschädigungen geschützt sein. Besonders wirkungsvoll ist der Schutz dann, wenn die Security oder die Security-Services ein fester Bestandteil der Backup-Lösungen sind, wie es beispielsweise Sophos in Kooperation mit Arcserve und Veeam realisiert.

Darüber hinaus können die folgenden drei Tipps die Gefahren eines Ransomware-Angriffs erheblich reduzieren:

- Regelmäßig Erstellen von Backups und das Speichern an mehreren Orten, beispielsweise nach der 3-2-1-Regel.
- Aktivierung einer MFA (Multi-Faktor-Authentifizierung), insbesondere bei Cloud-Backup-Konten, um zu verhindern, dass Angreifer Zugriff erhalten.
- Regelmäßiges Testen und Üben der Daten-Wiederherstellung aus den Backups. Je fließender der Wiederherstellungsprozess beherrscht wird, desto schneller und einfacher können sich Unternehmen von einem Angriff erholen.
- Security-Monitoring und Überwachung der Backups, um rechtzeitig verdächtige Aktivitäten von potenziellen Angreifern zu erkennen und darauf zu reagieren.

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

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