Wenn das Backup beim Ransomware-Angriff zum Problem wird

Cyberkriminelle richten ihre Verschlüsselungstaten auch auf Backups aus. Warum? Weil so noch mehr Erpressungsdruck entsteht und sich die Lösegeldsummen verdoppeln.

Die finanziellen und betrieblichen Auswirkungen eines Ransomware-Angriffs sind schon schlimm genug. Wenn es den Cyberkriminellen allerdings zusätzlich gelingt, die Backups zu schädigen oder zu verschlüsseln, ist die Wahrscheinlichkeit hoch, dass ein Unternehmen rund das doppelte an Lösegeld zahlen muss. Laut einer Studie von Sophos bei 2.974 IT-/Cybersecurity-Entscheidern in 14 Ländern fallen die Gesamtkosten für die Wiederherstellung sogar achtmal höher aus als bei Organisationen, deren Backups nicht betroffen sind.

Backup-Verschlüsselung gehört zum kriminellen Standard
In der Cyberkriminalität geht es um Geld, sehr viel Geld. Und daher versuchen mittlerweile alle Ransomware-Gruppen auch die Backups zu kompromittieren, um den Erpressungsdruck maßgeblich zu erhöhen. Die aktuelle Studie von Sophos bestätigt dies: Bei durchschnittlich 94 Prozent der Befragten, die von Ransomware betroffen waren, haben Cyberkriminelle versucht, auch die Backups zu verschlüsseln. Dieser Prozentsatz variiert in den untersuchten Branchen auf hohem Niveau. Bei Behörden auf Landes- und Kommunalebene sowie im Medien-, Freizeit- und Unterhaltungssektor lag der prozentuale Anteil sogar bei 99 Prozent. Im Bereich Vertrieb und Transport wurden mit immerhin noch 82 Prozent die wenigsten Backup-Kompromittierungsversuche ermittelt.

Erfolg bestätigt bekanntlich die eingesetzte Taktik
Der Versuch, Backups zu kompromittieren, um noch höhere Summen zu erpressen, ist nicht gleich ein Erfolg. Denn bei längst nicht allen Angriffen erreichen die Cyberkriminellen ihr Ziel. Besonders deutlich zeigt dies die Studie von Sophos im Vergleich der unterschiedlichen Branchen. Im Durchschnitt über alle Branchen hinweg waren 57 Prozent der Cyberkriminellen erfolgreich bei der Schädigung oder Verschlüsselung der Backups.

In den Branchen Energie, Öl/Gas und bei den Versorgungsunternehmen lag die Erfolgsquote bei 79 Prozent, im Bildungswesen bei 71 Prozent. Hingegen in der IT, Technologie und Telekommunikation beträgt die Erfolgsquote lediglich 30 Prozent und im Einzelhandel 47 Prozent. Damit liegt die Vermutung nahe, dass Unternehmen und Organisationen aus den Bereichen IT, Telekommunikation und Technologie über einen stärkeren Backup-Schutz verfügen oder sie waren möglicherweise in der Lage, Kompromittierungsversuche rechtzeitig zu erkennen und zu stoppen.

Die Kompromittierung von Backups kommt Organisationen teuer zu stehen
Im internationalen Schnitt beliefen sich Lösegeldzahlungen von Unternehmen, deren Backups kompromittiert wurden, auf 2 Mio. US-Dollar und fielen damit fast doppelt so hoch aus als bei Organisationen, deren Backups intakt blieben (1,062 Mio. US-Dollar). Zudem waren Unternehmen und Organisationen mit kompromittierten Backups viel weniger in der Lage, das Lösegeld zu verhandeln. Sie zahlten im Schnitt 98 Prozent der geforderten Summe. Im Gegensatz dazu konnten Ransomware-Betroffenen mit unversehrten Backups das Lösegeld auf 82 Prozent der Forderung reduzieren.

Weitere, detaillierte Informationen stehen im Sophos Whitepaper „Die Auswirkungen kompromittierter Backups auf Ransomware-Angriffe“ zur Verfügung.

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, Senior PR-Manager EMEA Central
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