COHESITY

HINWEISE UND TIPPS

5 Arten von Ransomware-Angriffen auf Ihre Backups ...und wie Sie diese verhindern können

Backup- und Wiederherstellungslösungen sollen Ihr Unternehmen schützen. Hochentwickelte Malware wie Locky und Crypto haben es allerdings nun auf Ihre Backup-Daten abgesehen. Das ist angesichts der steigenden Häufigkeit und Breite von Ransomware-Angriffen nicht verwunderlich. Die erste Ransomware-Zahlung – um 1989 – schuf die Voraussetzungen für Hacker weltweit, die Daten ahnungsloser Opfer zu sperren und zurückzuhalten, bis deren Besitzer dafür bezahlen. Analysten schätzen, dass heute alle 14 Sekunden ein Ransomware-Angriff auf Unternehmen stattfindet – das kostet Unternehmen weltweit Milliarden. Daher ist es so wichtig, diese fünf Überlegungen anzustellen, damit Sie Ransomware-Angriffe auf Ihre Backups verhindern, ermitteln und schnell darauf reagieren können.

1 Sichern Sie Ihre Backups gegen hochentwickelte Ransomware-Angriffe

Cyberkriminelle zielen heute aggressiv auf Schattenkopie-Backups ab. Ziel ist es, das zu kontrollieren oder sogar zu zerstören, was lange als Versicherung für Ihre Unternehmenskontinuität galt. Mit ausgefeilten Angriffen gelangen Sie von einem Endpunkt aus in eine primäre Umgebung und steuern direkt auf Ihre Backups zu, wo 80 % Ihrer Unternehmensdaten gespeichert sind. Von dort aus löschen oder beschädigen Sie alles und übernehmen anschließend die Produktivumgebung. Zum Schutz Ihres Backups vor Ransomware benötigen Sie eine mehrschichtige Verteidigung. Die ursprünglichen Backup-Aufträge müssen in einem unveränderlichen Zustand gehalten werden und dürfen keinesfalls zugänglich gemacht werden, um zu verhindern, dass sie von einem externen System angegriffen werden. Außerdem sind eine Multi-Faktor-Authentifizierung (MFA) und Write-Once-Read-Many-Funktionen (WORM) für einen Snapshot unerlässlich.

Ransomware in Zahlen

- Ransomware-Angriffe alle 14 Sekunden
- 700 % Anstieg seit 2016
- 35 % der Erpressungen werden bezahlt
- 2 Mrd. USD an finanziellen Verlusten
- 11 Mrd. USD an Verlusten bei Finanzen, Produktivität und Ausfallzeiten!

„Ransomware-Entwickler sind sich bewusst, dass Backups eine effiziente Abwehr darstellen und passen ihre Malware an, sodass diese Backups suchen und eliminieren können."

- CSO MAGAZINE

2 Mit der Erweiterung der Angriffsflächen werden Backups Ransomware-Angriffen ausgesetzt

Ein explodierendes Datenwachstum (die IDC schätzt, dass bis 2025 mehr als 175 Zettabytes an Daten vorhanden sein werden) und die Massenfragmentierung von Daten – d. h. die zunehmende Verbreitung von Backup-Daten über verschiedene, weitläufige Silos hinweg – vergrößern die Angriffsfläche Ihres Unternehmens. Infolgedessen sind Ihre Daten für Cyberkriminelle zugänglicher geworden. Wenn Sie verhindern möchten, dass Ransomware überhaupt erfolgreich ist, müssen Sie die Angriffsfläche Ihres Unternehmens zunächst reduzieren und wissen, welche Daten sich wo befinden. Mit einer einheitlichen Lösung zur Verbindung von Infrastruktur, Workloads und Backup-Standorten beseitigen Sie die Massenfragmentierung von Daten und schützen Ihr Unternehmen somit vor Ransomware.

3 Angriffe auf Backups werden einfacher durch intermittierende Überwachung

Cyber-Bedrohungen kommen nicht immer von außerhalb eines Unternehmens, sondern können auch unternehmensintern gestartet werden. Stellen Sie sich beispielsweise einen verärgerten Mitarbeiter vor, der einen großen Datensatz verändert oder löscht. Es reicht nicht aus, sich ausschließlich auf kleinste Änderungsraten von Backup-Daten zu verlassen, um ein derartiges Verhalten zu erkennen. Daher muss Ihr Unternehmen in der Lage sein, einen Angriff in Echtzeit zu erkennen. Sie benötigen eine Lösung, die durch die Analyse von Dateien und Auditprotokollen kontinuierlich kleinere Änderungsraten überwacht und erkennt – auch wenn Sie nicht genau aufpassen. Mit der richtigen Backup-Lösung schützen Sie Ihr Unternehmen Sekunde für Sekunde vor Cyber-Angriffen.

4 Öffentliche Cloud dient als Einstiegspunkt für Kriminelle durch Ransomware

Die Cloud wird schnell zu einem Einstiegspunkt für Cyber-Angriffe – was Ihre Backup-Daten einem hohen Risiko aussetzt. McAfee schätzt, dass heute einer von vier Public-Cloud-Nutzern schon einmal Opfer von Datendiebstahl war. Das heißt also: Daten in der Cloud sind nicht vor Ransomware geschützt. Die öffentliche Cloud mag eine kostengünstige Lösung für Backups sein, sorgt aber auch für erhöhte Datensichtbarkeit. Um der Ransomware stets einen Schritt voraus zu sein, ist eine Backup- und Wiederherstellungslösung erforderlich, die über ein einziges Dashboard verfügt. Mit der Möglichkeit, Ihre Backup-Daten schnell und umfassend anzuzeigen und zu verwalten – unabhängig davon, ob sie sich vor Ort oder in öffentlichen Clouds befinden – sind Sie in der Lage schnell die richtigen Maßnahmen zu ergreifen und ihr Unternehmen vor Ransomware-Angriffen zu schützen.

5 Lange Backup- und Wiederherstellungszyklen kommen zur Ransomware-Bedrohung hinzu.

Wenn Ihr Unternehmen auf ältere Backup-Lösungen angewiesen ist, die Synthetic-Full-Backup erfordern und dann Opfer eines Ransomware-Angriffs werden, kann es passieren, dass Ihr IT-Team Tage (oder sogar Wochen!) im Wiederherstellungsmodus verbringt. In einem kürzlich veröffentlichten Bericht des Ponemon Institute werden die durchschnittlichen Kosten eines einzelnen Ransomware-Angriffs auf 5 Millionen US-Dollar beziffert. Diese sind hauptsächlich auf Produktivitätsverluste, Systemausfälle und Informationsdiebstahl zurückzuführen. Sie benötigen eine Backup- und Wiederherstellungslösung, die schnell auf Ransomware-Angriffe reagiert und es Ihnen ermöglicht, infizierte Dateien in Ihrem globalen Datenfußabdruck – einschließlich öffentlicher Clouds – schnell zu finden und zu löschen. Des Weiteren sind sofortige Massenwiederherstellungsfunktionen erforderlich, die die Wiederherstellung von Hunderten von virtuellen Maschinen sofort, auf skalierbare Weise und zu jedem Zeitpunkt ermöglichen.

Verhinderung, Ermittlung und schnelle Reaktion auf Ransomware-Bedrohungen

Kein Unternehmen will Datenverluste durch Cyber-Angriffe erleiden, allerdings in der Lage sein, Forderungen nach einer Ransomware-Zahlung abzulehnen. Schützen Sie Ihre Daten mit einem umfassenden Ansatz für Sicherheit, Erkennung und schnelle Reaktion auf Ransomware-Angriffe.

Laden Sie das E-Book hier herunter, um mehr über die Sicherheit Ihrer Daten zu erfahren