COHESITY

MERKBLATT

5 Wege, wie Ransomware die Datensicherung unbrauchbar macht

Überblick

Ihre Datensicherungs- und Wiederherstellungslösung sollte Ihr Unternehmen schützen, aber raffinierte Malware wie Locky und Crypto hat es jetzt auf Backup-Daten abgesehen. Ransomware-Angriffe nehmen aktuell nicht nur in Anzahl und Ausmaß zu, sondern werden auch immer ausgefeilter und beschränken sich längst nicht mehr nur darauf, Ihre Daten unzugänglich zu machen und so lange zu blockieren, bis Sie Lösegeld zahlen. Mittlerweile gehen sie dazu über, das System zu kompromittieren, das Ihre Daten schützen soll. Laut Cybersecurity Ventures wird Ransomware bis Ende 2021 voraussichtlich alle 11 Sekunden ein Unternehmen angreifen. Deshalb sollten Sie die folgenden fünf Punkte beachten, wenn Sie überlegen, wie Sie Ihre Datensicherung am besten schützen können, damit Sie im Fall des Falles schnell auf einen Ransomware-Angriff reagieren können.

Ransomware in Zahlen

- Alle 11 Sekunden gibt es Ransomware-Angriffe[1]
- 10,5 Billionen US-Dollar weltweiter Schaden bis 2025[1]
- 1.070 % Anstieg gegenüber dem Vorjahr zwischen Juli 2020 und Juni 2021[2]
- 10- bis 15-fach höherer finanzieller Schaden als die eigentliche Lösegeldforderung[3]

1. Aufgrund ausgefeilter Ransomware-Angriffe werden Ihre Datensicherungen zu potenziellen Schwachstellen

Cyber-Kriminelle haben es jetzt auf die Daten der Datensicherung abgesehen, um die volle Kontrolle zu erlangen oder, schlimmer noch, das zu zerstören, was lange Zeit als Versicherungspolice für die Geschäftskontinuität galt. Ihre raffinierteren Angriffe dringen von einem Endpunkt aus in eine primäre Umgebung ein und steuern direkt auf Ihre Datensicherungen zu – wo 80 % der Unternehmensdaten gespeichert sind – und löschen oder kompromittieren dort alles, bevor sie die Produktionsumgebung übernehmen. Um zu vermeiden, dass Ransomware Ihre Datensicherung angreift, ist eine mehrschichtige Verteidigung erforderlich. Die originalen Backup-Daten sollten in einem unveränderlichen Zustand gehalten werden, und die goldene Kopie der Daten sollte nie von einem externen System verwendet werden. Regeln wie Write Once Read Many (WORM), Datenverschlüsselung, integrierte Fehlertoleranz und moderne Datenisolierung bieten als Teil Ihrer Datensicherungslösung einen zusätzlichen Schutz vor einem Ransomware-Angriff.

> "Ransomware-Entwickler sind sich bewusst, dass Backups eine effiziente Abwehr darstellen und passen ihre Malware an, sodass diese Backups suchen und ausschalten können.
>
> **CSO Magazine**

2. Je größer die Angriffsflächen, desto größer das Risiko gezielter Ransomware-Angriffe auf Backup-Daten

IDC berichtet, dass im Jahr 2020 64,2 Zettabyte an Daten erstellt oder repliziert wurden, und schätzt, dass im Jahr 2025 mehr als 175 Zettabyte an Daten existieren werden. In der Vergangenheit haben sich Unternehmen beim Schutz ihrer wachsenden Datenmengen auf mehrere Einzelprodukte (z. B. Medien- und Master-Server, Zielspeicher usw.) für die Datensicherung verlassen. Da diese Produkte ausufernde Silos bilden, die sich über die On-Premises-Umgebung und mehrere Clouds erstrecken, vergrößern sie die Angriffsfläche Ihres Unternehmens. Doch damit haben Cyber-Kriminelle leichtes Spiel, wenn sie auf Ihre Backup-Daten zugreifen wollen. Der erste Schritt gegen das Eindringen von Ransomware beginnt mit der Reduzierung der Angriffsfläche Ihres Unternehmens und dem Einschreiten gegen Massendatenfragmentierung. Doch dafür müssen Sie wissen, welche Daten Sie haben und wo sie sich befinden. Eine einheitliche Lösung, die den Überblick über Infrastruktur, Workloads und Standorte der Datensicherung verbessert, schützt Ihre Daten besser vor Ransomware.

[1] Cybersecurity Ventures
[2] Fortinet 2021 Ransomware-Umfragebericht
[3] Gartner: Wie man sich auf Ransomware-Angriffe vorbereitet, November 2020

3. Kompromittierte Anmeldeinformationen sind ein Geschenk, an dem Ransomware-Angreifer lange Freude haben

Gestohlene Zugangsdaten sind für Ransomware-Angreifer der heilige Gral, da sie ununterbrochenen Zugang zu verschiedenen Teilen der IT-Umgebung, einschließlich Datensicherungen, bieten und es Cyberkriminellen ermöglichen, Daten für größeren Profit zu exfiltrieren. Laut dem Verizon Data Breach Investigations Report 2021 waren kompromittierte Anmeldedaten die häufigste Datenform bei vorsätzlichen Sicherheitsverletzungen in diesem Jahr, und zwar bei sage und schreibe 61 % der Verstöße. Unternehmen, die eine moderne Datensicherung mit strengen Kontrollen des Benutzerzugriffs – einschließlich rollenbasierter Zugriffskontrollen (RBAC), Multifaktor-Authentifizierung (MFA) und kontinuierlicher Überwachungsfunktionen – einsetzen, können Ransomware-Angriffe effektiver abwehren und die damit verbundenen Ausfallzeiten und negativen Auswirkungen auf die Produktivität verhindern.

4. Mangelnde Sichtbarkeit und Früherkennung verschaffen Angreifern einen Vorsprung

Ransomware-Angreifer haben bei dunklen Daten leichtes Spiel. Sie können Datensicherungen unzugänglich machen und auf Produktionssysteme verlagern, um Ihre Daten heimlich zu entfernen und im Dark Web zu verkaufen. Die frühzeitige Erkennung mit einer zuverlässigen Backup- und Datenmanagementlösung der nächsten Generation ist ein guter Anfang, um bösartige Akteure zu bremsen. Um jedoch Ransomware-Exfiltrationsangriffe zu entdecken, ist eine Erkennung in nahezu Echtzeit erforderlich, die durch künstliche Intelligenz und maschinelles Lernen (AI/ML) unterstützt wird. Automatisierte Informationen, einschließlich Warnmeldungen, sorgen für eine schnellere Entdeckung von Angriffen und ersparen Ihren IT-Mitarbeitern Nächte und Wochenenden an Arbeit.

5. Lange Wiederherstellungszyklen verschlimmern Ihr Ransomware-Problem

Wenn Ihr Unternehmen sich auf ältere Produkte verlässt, die eine synthetische Vollsicherung erfordern und Opfer eines Ransomware-Angriffs wird, kann die Wiederherstellung Ihr IT-Team Tage (oder sogar Wochen!) kosten. 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. Deshalb benötigen Sie eine Datensicherung und -wiederherstellungslösung, die schnell auf Ransomware-Angriffe reagiert und es Ihnen ermöglicht, in Ihrem globalen Datenbestand – einschließlich Public Clouds – schnell eine saubere Kopie der Daten ausfindig zu machen. Außerdem benötigen Sie eine Funktion zur sofortigen Massenwiederherstellung, da Sie damit Hunderte von virtuellen Maschinen (VMs), Datenbanken und große Mengen unstrukturierter Daten sofort und zu jedem beliebigen Zeitpunkt wiederherstellen können.

Stoppen Sie erpresserische Cyber-Angriffe und schützen Sie Ihre Daten vor Ransomware

Wenn Sie Ihr Cyber-Risiko verringern und Ransomware-Zahlungsforderungen ablehnen möchten, sollten Sie sicherstellen, dass Ihre Sicherungs- und Datenmanagementlösungen cyber-resistent sind. Nur ein umfassender Ansatz zur Abwehr von Ransomware-Angriffen schützt Ihre Datensicherung davor, zum Angriffsziel zu werden, stoppt das Eindringen durch vollständige Transparenz und frühzeitige Erkennung und reduziert Ausfallzeiten und Datenverluste durch schnelle und saubere Wiederherstellung in großem Umfang.

Laden Sie das E-Book hier herunter, um mehr über den Schutz Ihrer Daten zu erfahren.

COHESITY

Cohesity.com | +1 855 926 4374 | 300 Park Ave., Suite 1700, San Jose, CA 95110, USA

9100003-006-DE 1-2022