Data Protection

Moderne Workloads treffen auf Cybercrime und veraltete Backup-Ansätze – ein grausiger, aber vermeidbarer Mix.

WIEN/COLUMBUS. Unternehmen sind mit immer komplexeren hybriden IT-Umgebungen konfrontiert und müssen ihre Budgets erhöhen, um Cyberangriffe abzuwehren und mit der zunehmenden Diversifizierung von Produktionsumgebungen über verschiedene Clouds hinweg Schritt halten zu können – IT-Führungskräfte haben zudem das Gefühl, nicht ausreichend geschützt zu sein.

Die Ergebnisse des vierten jährlichen Data Protection Trends Reports vom Datensicherheitsexperten Veeam Software zeigten deutlich, dass eine der obersten Prioritäten der Unternehmen in diesem Jahr die Verbesserung der Zuverlässigkeit und des Erfolgs von Backups sei, meint Mario Zimmermann, Regional Director Austria bei Veeam. Außerdem auf der Agenda: der Schutz von Infrastructure as a Service (IaaS) und Software as a Service (SaaS).

© Panthermedia.net/Toppercussion

Teure Daten
„Weltweit rechnen Unternehmen damit, ihr Budget für Datensicherung im Jahr 2023 um 6,5 Prozent zu erhöhen“, sagt Mario Zimmermann, Regional Director Austria bei Veeam.


© Anna Stöcher

Der Klassiker: Lösegeld

Ransomware ist neben Naturkatastrophen (Feuer, Überschwemmung, usw.) und Benutzerfehlern (Überschreiben, Löschen, usw.) die häufigste und folgenreichste Ursache von Ausfällen, kurz: das Worst-Case-Scenario. Dem Bericht zufolge verursachten Cyberangriffe die folgenschwersten Ausfälle für Unternehmen in den Jahren 2020, 2021 und 2022. 85% der Unternehmen wurden in den letzten zwölf Monaten mindestens einmal angegriffen, ein Anstieg von 76% gegenüber dem letztjährigen Bericht.

Insbesondere die Wiederherstellung sei das Hauptproblem; die Befragten gaben an, dass nur 55% ihrer verschlüsselten oder zerstörten Daten nach Angriffen wiederhergestellt werden konnten. Nur 19% konnten ihre Daten selber wiederherstellen und zahlten kein Lösegeld. 33% zahlten, bekamen ihre Daten aber dennoch nicht zurück.

Laut der Umfrage ist der wichtigste Aspekt, nach dem Unternehmen bei einer modernen Datenschutzlösung suchen, die „Integration der Datensicherung in eine Strategie der Cyberbereitschaft“. Unternehmen sollten daher Sicherungs- und Wiederherstellungslösungen implementieren, die einen umfassenden Ansatz für die Datensicherheit bieten und mit anderen Technologien zur Erkennung und Behebung von Cyberangriffen integriert werden können, um eine umfassende Cyberresilienz zu gewährleisten, raten die Spezialisten bei Veeam.

Wolkige Heilsbringer

Zuverlässigkeit und Konsistenz (beim Schutz von IaaS- und SaaS-Servern sowie Servern im Rechenzentrum) seien laut Veeam die wichtigsten Faktoren für die Verbesserung der Datensicherung im Jahr 2023. Unternehmen, die Schwierigkeiten haben, in der Cloud gespeicherte Daten mit herkömmlichen Backup-Lösungen zu schützen, werden ihre Backup-Lösung für das Rechenzentrum wahrscheinlich durch IaaS/PaaS- und/oder SaaS-Funktionen ergänzen.

Cloud-basierte Dienste scheinen für Unternehmen aller Größenordnungen nahezu unvermeidlich zu sein. Aber so wie es nicht nur eine Art von Produktions-Cloud gibt, gibt es auch nicht nur ein einziges Cloudsicherungs-Szenario. Unternehmen sollten Cloud-Tiers für die Aufbewahrung, Backup as a Service (BaaS) und schließlich Disaster Recovery as a Service (DRaaS) in Betracht ziehen.

Cyberresilienz

Unternehmen würden immer komplexere hybride Umgebungen aufbauen, während das Volumen und die Raffinesse von Cyberattacken zunehmen, beschreibt Zimmermann den Ist-Zustand.

Veraltete Backup-Ansätze würden modernen Workloads – von IaaS und SaaS bis hin zu Containern – nicht gerecht und, wenn Schnelligkeit gefragt wäre, nur zu einer unzuverlässigen und langsamen Wiederherstellung im Unternehmen führen. Das sei es, was IT-Führungskräfte bei der Planung ihrer Cyberresilienz in den Mittelpunkt stellen, so Zimmermann. *(hk)*

Archivierung
Mit Cloud-Tiering werden weniger häufig verwendete Daten von teuren lokalen Dateispeichern auf billigere Speicherebenen in der Cloud ausgelagert.


© APA/AFP/Alain Jocard