7 Schritte zur wirksamen **Backup-Strategie**

In Zeiten steigender Datenmengen und Ransomware-Angriffen müssen Unternehmen ihre Cyberresilienz spürbar erhöhen. Eine wirkungsvolle Data-Protection-Strategie ist dafür die Grundlage. Dell Technologies nennt sieben Schritte, mit denen Unternehmen sie praktisch umsetzen … | VON CHRISTIAN WINTERFELDT

Nicht nur die zunehmende Menge an Daten, sondern vor allem auch deren Verteilung auf unterschiedlichste Speicherorte steigert die Komplexität des Datenmanagements. Eine hohe Anzahl von Cyberattacken, überlastete Teams und schmale Budgets verschärfen die Lage für Betrieb und Unternehmen zusätzlich. Sie benötigen daher eine ebenso effektive wie effiziente Strategie für das Speichern, Schützen und Sichern ihrer Daten. Diese sollte die folgenden sieben Schritte umfassen.

1. Standardisieren: Für eine holistische Backup-Strategie braucht es Überblick. Unternehmen sollten daher zunächst herausfinden, wo geschäftskritische Daten liegen und welche Folgen deren Verlust für sie im schlimmsten Falle haben würde. Beliebte Orte, die gern übersehen werden, sind Datenbanken, virtuelle Maschinen, Edge- und Multi-Cloud-Umgebungen sowie Daten aus persistenten Kubernetes- und „As-a-Service"-Anwendungen.

2. Data Protection modernisieren: Es gibt viele Möglichkeiten, Backups durchzuführen. Der richtigere Begriff wäre hier Data Protection. Moderne Data-Protection-Szenarien verbinden mehrere Elemente miteinander, darunter verschiedene Arten der Datenreplikation, die Sicherstellung der Unveränderlichkeit der Daten und Methoden zur Steigerung der Wirtschaftlichkeit und Effizienz wie die Deduplizierung. Sie alle helfen dabei, Backups schneller zu erstellen und die Wiederaufnahme des Geschäftsbetriebs nach einer Cyberattacke zu beschleunigen. Zudem sollten Unternehmen sicherstellen, daß sie die Daten auf dem Backup-Storage jederzeit zur nahtlosen Wiederherstellung verwenden können. Durch diese Vorgehensweise liegt somit automatisch ein Fokus auf der Datenintegrität.

„Cyberattacken und Angriffe mit Ransomware werden früher oder später jeden treffen und Erfolg haben, da braucht sich niemand etwas vorzumachen …"

Christian Winterfeldt, Senior Director, Data Center Sales bei Dell Technologies (Bild: Dell Technologies)

3. Backup-Umgebungen abhärten: Nicht nur die Live-Systeme, auch die Backup-Umgebungen haben Betriebssysteme. Darum gilt es für Unternehmen darauf zu achten, diese auf dem aktuellsten Stand zu halten und Patches möglichst umgehend aufzuspielen. Für zusätzliche Sicherheit sorgt die Verschlüsselung der Backup-Daten während ihrer Übertragung. Angesichts zunehmender Angriffe auf die Backup-Umgebungen selbst sollten Unternehmen gesicherte Daten zudem unveränderlich machen. Dafür müssen sie ihre Backup-Systeme so einstellen, daß nachträgliche Änderungen an den auf ihnen gesicherten Daten nicht möglich sind.

4. Zugänge sichern: Den Zugang auf die Backup-Umgebung sollten Unternehmen so restriktiv wie möglich gestalten. Dafür stehen verschiedene Methoden zur Auswahl. Multi-Faktor-Authentifizierung (MFA) und API-Zugangsdaten dienen dazu, den Zugang nur berechtigten Personen zu gewähren. Die rollenbasierte Zugriffskontrolle (RBAC) sorgt dafür, daß Personen nur auf die Bereiche Zugriff erhalten, die sie auch wirklich für ihre Arbeit benötigen – so kann ein gehackter Account nicht das gesamte System infiltrieren. Transport Layer Security (TLS)-Zertifikate verschlüsseln zudem die Verbindung zwischen Client und Backup-Umgebung.

5. Anomalien aufspüren: Backup-Daten sind nicht nur als Sicherungskopie geeignet. Unternehmen können sie auch verwenden, um Anomalien und Datenbeschädigungen (auch Datenkorruption) zu erkennen, indem sie sie mit den Dateien auf den Live-Systemen abgleichen. Dadurch ist es ihnen möglich, frühzeitig Cyberattacken aufzudecken und geeignete Gegenmaßnahmen einzuleiten. Überdies stellen sie durch das Aufspüren von Anomalien sicher, daß sie nur unbeschädigte und sichere Daten nach einem Hackerangriff wiederherstellen.

6. Automatisierung nutzen: Viele Backup-Plattformen bieten umfangreiche Möglichkeiten, die Datensicherung zu automatisieren. Der größte Vorteil dieser Mechanismen ist ihre Zuverlässigkeit: Einen Datenverlust können Unternehmen so nahezu ausschließen. Zudem reduzieren diese Automatisierungskapazitäten den Workload der IT-Abteilung, die sich stattdessen strategischeren Aufgaben widmen kann.

7. Daten isolieren: In Sachen Data Protection ist auch die Nutzung eines Datentresors mit Operational Air Gap eine sinnvolle Maßnahme. Er vereint viele Punkte dieser Liste nativ: So erstellt der sogenannte Cyber Vault automatisch unveränderliche Sicherungskopien geschäftskritischer Daten. Für Hacker ist der Speicher durch seine Isolation vom Betriebsnetzwerk praktisch unsichtbar. Um die Datenintegrität sicherzustellen, enthalten solche Lösungen außerdem in der Regel passende Analysewerkzeuge. Und schließlich läuft der Datentransfer unidirektional über Datendioden, was den Datenabfluß verhindert. <<

Noch Fragen?
https://www.delltechnologies.com/de-de/blog