Schutz vor Ransomware und Insider-Bedrohungen durch Datenisolierung

Wichtige Vorteile

- Stärkung der Datensicherheitsstrategie
- Sicherung der Daten vor Cyber- und internen Bedrohungen
- Einhaltung der SLAs und Reduzierung der Unternehmensrisiken
- Verringerung der Ausfallzeit durch sofortige Wiederherstellung im großen Maßstab

Laut einer aktuellen Studie von Cybersecurity Ventures werden Unternehmen bis 2031 alle zwei Sekunden von einem Ransomware-Angriff betroffen sein, der Kosten in Höhe von über 265 Milliarden US-Dollar verursacht. Gleichzeitig werden 34 % aller Firmen weltweit mit einem Insider-Angriff zu tun haben – eine Zunahme um 47 % in den vergangenen zwei Jahren, so Tech Jury. Aufgrund der zunehmenden Häufigkeit und Schwere von Cyberangriffen und Insider-Bedrohungen versuchen Unternehmen, stärkeren Schutz für ihre IT-Systeme und Daten aufzubauen. Viele folgen der Richtlinie des NIST Cybersecurity Framework, um eine mehrschichtige Abwehrstrategie umzusetzen.

Unternehmen, die in das Next-Gen Data Management von Cohesity investieren, haben einen Vorsprung. Cohesity wurde speziell mit Defense-in-Depth-Funktionen entwickelt, einem mehrschichtigen Sicherheitskonzept. Dazu zählen:

- **Unveränderliche Snapshots** – Eine goldene Kopie der Sicherungsdaten, die niemals offengelegt oder extern gemountet wird
- **DataLock** – Eine zeitlich festgelegte WORM-Sperre des Backup-Snapshots, der nicht geändert werden kann
- **Verschlüsselung** – Daten werden im Ruhezustand und während der Übertragung verschlüsselt
- **Rollenbasierte Zugriffskontrolle (RBAC)** – Granularer Verwaltungs- und Benutzerzugriff kann nach den Grundsätzen der geringsten Berechtigung und nach dem Need-to-Know-Prinzip implementiert werden
- **Keine Hintertür** – Unterstützung der Kontoaktivierung nur durch autorisierte Kundenbenutzer(innen)
- **Sicherer SSH-Zugriff** – Ein sicherer Zugangsweg über ein ungesichertes Netzwerk
- **Datenisolierung** – Isolierung von Daten, um sie vor Cyber- und internen Bedrohungen zu schützen

Die Datenisolierung ist kein Ersatz für bestehende Sicherungs- und Wiederherstellungslösungen oder Disaster-Recovery-Lösungen (DR), sondern vielmehr eine Möglichkeit, eine zusätzliche Schutzschicht zu schaffen. Ihr Zweck ist die Stärkung der Gesamtstrategie für die Datensicherheit.

Moderne Datenisolierung mit Cohesity

Gemäß der NIST-Definition erfordert das Air Gapping, dass Unternehmen mindestens eine Kopie ihrer Daten physisch und elektronisch isoliert aufbewahren, um zusätzliche Sicherheit zu gewährleisten. Dieser Ansatz ist zwar sehr sicher, unterstützt aber nicht die RTO- und RPO-Ziele moderner Unternehmen. Infolgedessen hat sich die Datenisolierung als Alternative herauskristallisiert, um die modernen RTO- und RPO-Anforderungen besser zu erfüllen; die Sicherungsdaten werden in der Cloud oder an einem anderen Ort mit einer temporären und hochsicheren Verbindung gespeichert. Dadurch wird eine manipulationssichere Umgebung geschaffen, die vor Ransomware und Insider-Bedrohungen schützt und die SLAs des Unternehmens unterstützt.

Mit Cohesity gefährden Unternehmen nie ihre SLAs oder ihre Risikotoleranz und haben ein Maximum an Optionen und Flexibilität bei der Isolierung und dem Schutz ihrer Daten vor unerwünschten Akteuren. Cohesity unterstützt eine flexible Bereitstellung mit Isolierung:

- **Cohesity FortKnox** – Eine SaaS-Lösung zur Datenisolierung und -wiederherstellung, die die Cyber-Resilienz mit einer unveränderlichen Kopie der Daten in einem von Cohesity gemanagten Cloud-Tresor mittels Virtual Air Gap verbessert. Die Lösung bietet Ransomware-Erkennung, Quorom und Zero-Trust-Merkmale für den Schutz Ihrer Daten. In Verbindung mit physischer Trennung, Netzwerk- und Managementisolierung bietet FortKnox den ultimativen Schutz und die Benutzerfreundlichkeit, die bei der Abwehr von Ransomware und anderen Cybersecurity-Bedrohungen erforderlich sind.
- **Cohesity Remote-Cluster** – Kunden können von einem unveränderlichen Cohesity-Cluster in einen anderen Remote-Cluster replizieren, der entweder vor Ort oder als virtueller Cluster in einer Public Cloud läuft. Im Vergleich zum herkömmlichen Datenisolierungsansatz, der den Versand von Bändern an einen anderen Standort erfordert, senkt diese Datenisolierungsmethode die RTOs und RPOs, da die Daten auf dem Remote-Cluster sofort zur Verfügung stehen.
- **NAS-Ziel** – Cohesity archiviert Daten in einem externen NAS-Speicherplatz, der WORM zum Isolieren von Daten mit geringeren RTOs und RPOs unterstützt.
- **Cloud** – Um die Vorteile der Skalierbarkeit und Elastizität der öffentlichen Cloud zu nutzen, haben Unternehmen die Cloud als eine der modernen Möglichkeiten zur Datenisolierung genutzt. Cohesity unterstützt die Archivierung in der Cloud oder in jedem S3-kompatiblen Speicher, der Object Lock und Object Versioning unterstützt, um Datenisolierung, niedrigere RTOs und RPOs sowie niedrigere TCOs zu erreichen.
- **Tape (Air Gap)** – Cohesity ermöglicht die Archivierung von Daten von einem Backup auf Band, so dass die IT-Abteilung die Bänder an einen externen Speicherort senden kann und der Zugang nur durch physischen Eingriff möglich ist.

Optimale Risiko-SLA-Prämien mit Isolierung in einem Cluster von Cohesity

Die Kunden von Cohesity erhalten nicht nur Datenresilienz, sondern werden überdies in die Lage versetzt, anspruchsvolle Unternehmens-SLAs einzuhalten und gleichzeitig ihre Risiken durch Replizieren ihrer Backup-Daten in einen externen Cluster von Cohesity zu verringern. In Übereinstimmung mit dem Defense-in-Depth-Modell des NIST Cybersecurity Frameworks ermöglicht Cohesity die Replikation von Daten auf einen anderen unveränderlichen Cluster von Cohesity an einem isolierten Standort, der einen modernen Datentresor bietet, sich in einem isolierten Netzwerk befindet und WORM unterstützt.

Abbildung 1 zeigt die Flexibilität bei der Bereitstellung von FortKnox mit der Möglichkeit, Daten bei der Notfallwiederherstellung an mehreren Zielen wiederherzustellen. Lediglich die Unternehmensadministratoren öffnen und schließen die erforderlichen Ports – und zwar nur während der Datenübertragung, damit die Daten sicher sind.

Durch die Replikation auf einen isolierten Cluster von Cohesity modernisieren Unternehmen nicht nur ihre Rechenzentren. Sie erreichen auch eine stärkere Cyberabwehr, schnellere Recovery – mit sofortiger Wiederherstellung bei Skalierung – sowie kürzere RTOs und RPOs bei gleichzeitiger Reduzierung der Anforderungen an die Netzwerkbandbreite. Schützen Sie Ihr Unternehmen vor den zunehmenden Ransomware- und Insider-Bedrohungen, indem Sie Ihre IT-Systeme mit dem Air-Gap-Schutz von Cohesity verstärken.

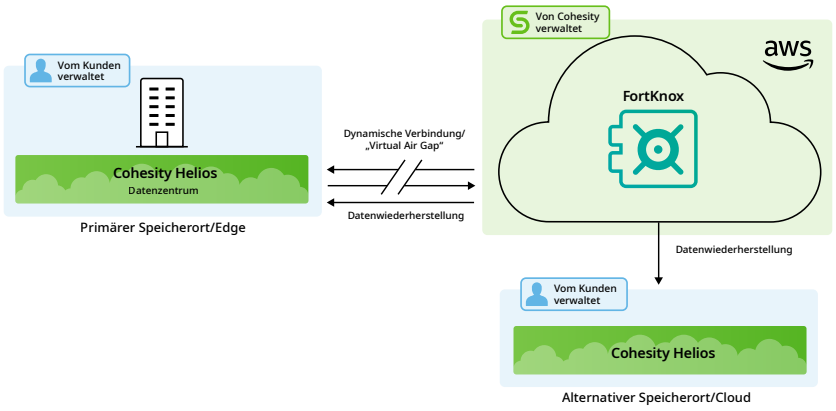

Abbildung 1: Flexibilität bei der Wiederherstellung mit FortKnox

Erfahren Sie mehr auf www.cohesity.com/de

COHESITY