OBJECT FIRST

Checklist

Checkliste für den Ransomware-Schutz

Überprüfen Sie, ob Ihr Backup-Storage absolute Immutability gewährleistet

Ransomware-Angriffe werden immer ausgefeilter. 66% der Unternehmen wurden in den vergangenen zwei Jahren mindestens einmal Opfer eines Angriffs und in 96% der Fälle waren Backup-Daten das Ziel.*

Bei einem Angriff – und ein solcher wird über kurz oder lang unvermeidbar sein – stehen Ihr Unternehmen, Ihr Ruf und Ihre Karriere auf dem Spiel. Deshalb ist Immutable Backup-Storage Ihr Rettungsanker und bester Schutz vor Ransomware.

Wenn eine Storage-Lösung allerdings Immutability verspricht, Daten aber von Backup- oder Storage-Administratoren, Anbietern oder Angreifern überschrieben werden können, handelt es sich nicht um eine Lösung mit absoluter Immutability.

Überprüfen Sie anhand dieser Checkliste mit drei Schritten, ob Ihre derzeitige (oder geplante) Backup-Lösung ausreichenden Schutz vor Ransomware bietet.

* ESG Research 2025

Machen Sie sich bereit

Schritt 1. Nutzung von S3-Objektspeicher

- ☐ Nutzt Ihre Storage-Lösung S3 Object Lock und Versionsverwaltung, um Immutability durchzusetzen und auch die Backup-Historie zu speichern?
- ☐ Wendet sie den Compliance-Modus (anstelle des Governance-Modus) an und unterstützt sie die End-to-End-Verschlüsselung bereits bei der Erstellung der Daten?
- ☐ Lässt sich die Immutability mithilfe von offenen Standards und Penetrationstests durch unabhängige Dritte überprüfen?

Nur S3-Objektspeicher bietet integrierte Sicherheit mit nativer Immutability, die direkt in das Protokoll und die APIs eingebettet ist. Mit diesem Design wird sichergestellt, dass Daten nach dem Speichern nicht mehr geändert oder gelöscht werden können. S3-Objektspeicher basiert auf einer offenen Architektur nach Branchenstandard, die sich an Best Practices für die ITSicherheit orientiert und Tests durch unabhängige Dritte ermöglicht.

Schritt 2. Gewährleistung von sofortiger Immutability

- ☐ Gewährleistet Ihre Lösung die Immutability von Backup-Daten bereits bei der Erstellung, und zwar ohne Verzögerungen oder Landing Zones?
- ☐ Lässt sich damit Immutability auf Snapshot- Basis oder auf Deduplizierungsebene vermeiden, bei der Schutzmaßnahmen erst nach
- ☐ Abschluss des Jobs angewendet werden?
  Werden die Backup-Daten mit aktiviertem S3 Object Lock direkt im Objektspeicher abgelegt?

Die Gewährleistung der Immutability von Backup-Daten bereits bei der Erstellung ist entscheidend, um unbefugte Änderungen zu verhindern, die Datenintegrität aufrechtzuerhalten und Daten vor Ransomware zu schützen. Die bewährte und sicherste Methode dafür ist die S3- Versionsverwaltung in Kombination mit Object Lock. Sie gewährleistet Immutability bereits bei der Erstellung eines Objekts im Speichersystem.

Schritt 3: Einsatz einer speziellen Zielspeicher-Appliance

- ☐ Ermöglicht Ihr System eine strikte Trennung zwischen Backup-Software und Backup-Storage, sodass der Radius von Angriffen verringert werden kann?
- ☐ Nutzen Sie eine dedizierte, vom Anbieter verwaltete Zielspeicher-Appliance anstelle einer selbst entworfenen Storage-Lösung, für die manuelle Updates, Patches und Überwachung erforderlich sind?
- ☐ Ist Ihre Lösung nachweislich sicher oder nutzt sie ein herstellereigenes Dateisystem, das Tests durch unabhängige Dritte verhindert und keinen Einblick in die Maßnahmen zur Durchsetzung der Immutability gewährt?

Speziell entwickelte Backup-Storage-Lösungen bestehen aus eigenständigen Storage-Geräten, die für die Speicherung von Backup-Daten konfiguriert und optimiert sind. Es gibt zwei Arten dieser Appliances: integrierte Appliances, die Backup-Software und Storage in einem System vereinen, und Zielspeicher-Appliances, mit denen ein schlüsselfertiges Storage-Gerät für externe Backup-Software wie Veeam zur Verfügung steht. Nur spezielle, schlüsselfertige S3-Zielspeicher-Appliances können Zero-Trust-Datenresilienz gewährleisten, indem sie Software und Storage ordnungsgemäß voneinander trennen und Sicherheitstests durch unabhängige Dritte ermöglichen.

Absolute Immutability: der ultimative Ransomware-Schutz

Wenn Sie nicht bei jeder Frage dieser Checkliste ein Häkchen setzen können, sind Ihre Backups möglicherweise dem Risiko eines Ransomware-Angriffs ausgesetzt. **Absolute Immutability** bedeutet keinerlei Zugriff auf schädliche Aktionen (Zero Access).

Dadurch kann niemand – auch kein Administrator mit weit gefassten Rechten oder ein Angreifer mit Zugriff auf den Backup-Storage – Ihre Daten ändern oder löschen.

Um durch Zero Access absolute Immutability zu gewährleisten, müssen **drei Grundprinzipien befolgt werden:**

1. **S3-Objektspeicher:** Ein umfassend dokumentierter, offener Standard mit nativer integrierter Immutability, der Penetrationstests und die Überprüfung durch unabhängige Dritte ermöglicht
2. **Sofortige Immutability:** Die Immutability von Backup-Daten muss ab dem Zeitpunkt ihrer Erstellung gewährleistet sein.
3. **Zielspeicher-Appliance:** Bei einer dedizierten Zielspeicher-Appliance sind Storage und Backup-Software voneinander getrennt. Dadurch entfallen die Risiken, die beim Betrieb von selbst entworfenem und verwaltetem Backup-Storage entstehen.

Laden Sie unser Whitepaper herunter und erfahren Sie, warum **Absolute Unveränderlichkeit** der ultimative Schutz vor Ransomware ist.

Lesen Sie das Whitepaper ↗

Über Object First

Object First stellt sicheren, unkomplizierten und leistungsfähigen Backup-Storage speziell für Veeam bereit, der absolute Immutability gewährleistet. Durch diesen ultimativen Ransomware-Schutz profitieren Sie und Ihr Unternehmen von einfacher Resilienz.

Demotermin vereinbaren ↗