COHESITY

EIN LEITFADEN FÜR FÜHRUNGSKRÄFTE ZUR BEWERTUNG VON DATENTRESOREN

Zusammenfassung: Warum Cyber-Vaulting für die Cyber-Resilienz unerlässlich ist

Kein Unternehmen ist vor Cyberangriffen gefeit, daher sind wirksame Reaktions- und Wiederherstellungsmaßnahmen für jede Organisation unerlässlich. Angreifer scheuen keine Mühen, um Sie zur Zahlung eines Lösegeldes zu zwingen, und nehmen dabei sogar jene Systeme ins Visier, die eigentlich zum Schutz Ihrer Daten gedacht sind. Herkömmliche Backup-Strategien, die zum Schutz vor Hardwareausfällen und Naturkatastrophen konzipiert sind, bieten Ihrem Unternehmen kaum Schutz vor gezielten, mehrstufigen Cyberangriffen. Wenn Ransomware zuschlägt, können Sicherungskopien von Daten, die mit Produktionsnetzwerken verbunden sind, verschlüsselt oder gelöscht werden, was eine saubere und schnelle Wiederherstellung nahezu unmöglich macht. Für IT-Führungskräfte stellt sich nicht die Frage, ob es zu einem Angriff kommen wird, sondern wann. Ist Ihr Unternehmen bereit, sich im Falle eines Angriffs sicher wieder zu erholen?

In einer Zeit, in der Unternehmen wie das Ihre ihre Strategien zum Schutz und zur Wiederherstellung von Daten überdenken, ist Cyber-Vaulting zu einem grundlegenden Bestandteil einer modernen Strategie zur Cyber-Resilienz geworden. Ein Datentresor stellt sicher, dass Sie über eine unberührte Kopie Ihrer Daten verfügen, auf die Sie zurückgreifen können, wenn alle anderen Möglichkeiten versagen. Vaulting bietet die erforderliche Trennung, Überprüfung und Kontrolle, um saubere, wiederherstellbare Daten zu gewährleisten – selbst im Falle zerstörerischer Cyberangriffe. Aus diesem Grund setzen Ihre Mitbewerber auf Cyber-Vaulting als unverzichtbare Maßnahme zur Gewährleistung der Ausfallsicherheit.

Die Herausforderung: Die Wiederherstellung nach Cyberangriffen ist weitaus komplexer als die Notfallwiederherstellung

Jahrelang entwickelten Unternehmen Backup-Systeme, um Hardwareausfälle, versehentliche Löschungen und Naturkatastrophen zu bewältigen. Diese Systeme erfüllten oft ihren Zweck. Doch sie reichen nicht aus, um Daten vor den zerstörerischen Cyberangriffen zu sichern und zu schützen, die heutzutage vorherrschen.

Infolgedessen hat sich ein kritischer Risikofaktor herauskristallisiert: Backup-Daten können genauso anfällig sein wie Produktionsdaten. Angreifer konzentrieren sich nicht mehr ausschließlich auf die Verschlüsselung von Produktionsdaten. Sie dringen in Backup-Repositorys ein, deaktivieren Snapshot-Zeitpläne, schleusen Malware ein und verfälschen Metadaten, um Wiederherstellungsmöglichkeiten auszuschalten.

Diese Risiken bestehen auch dann, wenn Sie über eine moderne Datenschutzplattform verfügen.

Warum Ihre Datenlandschaft gefährdet ist

Vielleicht denken Sie: „Ich habe eine sichere Datenplattform für alle meine Backups, auf der alle Sicherheitsfunktionen aktiviert sind. Ist das nicht genug?“ Die Antwort lautet: Nein.

Eine solche Plattform verringert Ihr Risiko und Ihre Angriffsfläche erheblich. Aber für sich genommen beseitigt sie die Exponiertheit nicht.

Hier ist der Grund dafür:

- **Gemeinsame Konnektivität**: Die meisten Backup-Systeme bleiben mit dem Produktionsnetzwerk verbunden. Sollte diese Produktionsumgebung kompromittiert werden, haben Angreifer bereits einen Zugang zu den Sicherungsdaten.
- **Überschneidung von Anmeldedaten**: Administratoranmeldedaten werden häufig in verschiedenen Umgebungen gemeinsam genutzt. Sobald sich ein Angreifer privilegierten Zugriff verschafft hat, kann er Backups ebenso leicht löschen oder verschlüsseln wie Produktionsdaten.
- **Trügerische Unveränderlichkeit**: Manche „unveränderliche“ Backups sind lediglich softwaremäßig gesperrt. Sollte die Speicher-Steuerungsebene oder die API kompromittiert werden, kann das Unveränderlichkeits-Flag aufgehoben werden.
- **Latente Bedrohungen können bestehen bleiben**: Viele Unternehmen führen Wiederherstellungen aus Backups durch, ohne die Datenintegrität zu überprüfen oder nach versteckter Malware zu suchen, wodurch sich das Risiko einer erneuten Infektion während der Wiederherstellung erhöht.

Die Auswirkungen auf das Geschäft

Das Ergebnis ist eine Vertrauenslücke: Die wahrgenommene Integrität der Sicherungsdaten ist weitaus höher als die tatsächliche. Die negativen Folgen kaskadieren:

- **Längere Ausfallzeit**: Nicht überprüfte oder kompromittierte Backups verlängern die Wiederherstellung von Stunden auf Tage oder Wochen.
- **Operative Belastung**: Teams verbringen Zeit damit, Systeme oder Datensätze neu zu erstellen, anstatt Wiederherstellungspläne umzusetzen.
- **Steigende Kosten**: Jede Stunde Ausfallzeit führt zu höheren Umsatzverlusten, erhöhten aufsichtsrechtlichen Risiken und stärkerem Imageverlust.
- **Schwindendes Vertrauen**: Wenn die IT keine schnelle und reibungslose Wiederherstellung gewährleisten kann, schwindet das Vertrauen der Führungskräfte und des Vorstands in die Widerstandsfähigkeit des Unternehmens.

Cyber-Vaulting: Ihre letzte Verteidigungslinie, wenn alles andere versagt

Ein Datentresor schließt diese Vertrauenslücke. Ein Datentresor ist ein sicheres, isoliertes und unveränderliches Repository, in dem saubere Kopien kritischer Daten aufbewahrt werden. Der Tresor ist bewusst von den Produktionsnetzwerken und den primären Backup-Systemen getrennt.

Die Einführung eines Datentresors aktualisiert die 3-2-1-Sicherungsregel: Bewahren Sie drei Kopien Ihrer Daten auf zwei verschiedenen Medientypen auf, wobei eine Kopie an einem externen Standort gespeichert sein sollte, der isoliert und unveränderlich ist.

In der Praxis setzen Unternehmen diese moderne Backup-Regel wie folgt um:

- **Es müssen drei (3) Kopien von Daten unveränderlich sein:** Kopien sollten durch „Write-Once, Read-Many“ (WORM) oder eine Sperrung auf Objektebene geschützt und kontinuierlich mithilfe von KI-gestützter Anomalieerkennung und regelmäßigen Bedrohungsscans überprüft werden, um sicherzustellen, dass die Daten fehlerfrei sind.
- **„Zwei (2) verschiedene Medien“ bedeutet, dass Daten auf zwei verschiedenen Plattformen oder Vertrauensgrenzen gespeichert werden:** Die Kopien sollten sich auf unterschiedlichen Systemen befinden, die nicht dieselbe Steuerungsebene oder Angriffsfläche nutzen. Dies kann Kombinationen aus Festplatten-, Band- oder Cloudspeicher umfassen, die für die Datenisolierung ausgelegt sind.
- **Eine (1) externe Kopie muss isoliert sein:** Die endgültige Kopie sollte durch ein logisches oder physisches Air Gapping getrennt und durch ein isoliertes Sicherheitsmodell sowie durch die Verwahrung durch einen unabhängigen Dritten geschützt sein. Diese Kopie sollte zudem durch Multi-Faktor-Authentifizierung (MFA), Quorum und Datenintegritätsprüfungen geschützt werden.

Zusammen machen diese Fortschritte die 3-2-1-Regel zu einer tragenden Säule der Cyber-Resilienz. Der Datentresor dient als letzter, einwandfreier Wiederherstellungspunkt für kritische Daten. Durch die Kombination von Unveränderlichkeit, Isolation, verschiedenen Speicherbereichen und strenger Integritätsprüfung ermöglicht der Datentresor Unternehmen eine sichere Wiederherstellung nach zerstörerischen Cyberangriffen – selbst im schlimmsten Fall, in dem Ihre Backup-Infrastruktur kompromittiert wurde.

Bewertung von Datentresor-Lösungen

Bei der Auswahl einer Datentresor-Lösung sollten IT-Führungskräfte sowohl die Sicherheitsarchitektur als auch die betriebliche Bereitschaft bewerten. Aufgrund der Rückmeldungen von Hunderten von IT-Führungskräften stellen die folgenden fünf Säulen entscheidende Fähigkeiten dar:

1. **Isolierung und Zugriffskontrolle:** Tresordaten sollten von Produktionsnetzwerken unerreichbar sein. Achten Sie auf zwingend vorgeschriebenes Air Gapping, unabhängige Identitätsdomänen, MFA und auf Quorum basierende administrative Genehmigungen.
2. **Unveränderlichkeit und Integrität:** Die Daten müssen manipulationssicher sein und über WORM-Speicher sowie Aufbewahrungsrichtlinien verfügen, die eine Änderung oder Löschung verhindern – selbst durch Administratoren.
3. **Automatisierung und Orchestrierung:** Die Replikation, Validierung und Wiederherstellung des Tresors sollte automatisiert werden. Eine richtlinienbasierte Orchestrierung verringert das Risiko menschlicher Fehler und beschleunigt die Wiederherstellung.
4. **Bedrohungsschutz:** Die KI-gestützte Anomalieerkennung und das Scannen auf Malware weisen auf potenzielle Bedrohungen in Snapshots hin, um sicherzustellen, dass ausschließlich saubere, nicht kompromittierte Daten gespeichert und wiederhergestellt werden.
5. **Compliance und Berichterstattung:** Unveränderliche Auditprotokolle, Verschlüsselung und Aufbewahrungsmanagement sollten mit Rahmenwerken wie NIST SP 800-209, ISO 27040 und DORA im Einklang stehen, um die Wiederherstellbarkeit und die Ausfallsicherheit nachzuweisen.

Bewertungsbogen: Verwenden Sie diesen Bewertungsbogen bei Ihren Gesprächen mit Herstellern.

Anleitung:

1. Weisen Sie jedem Hersteller in jeder Kategorie eine Note von 1 bis 5 zu, wobei 1 bedeutet, dass die Anforderung nicht erfüllt ist, und 5, dass die Anforderung vollständig erfüllt ist.
2. Multiplizieren Sie die Punktzahl des jeweiligen Herstellers mit der **Gewichtung** für diese Kategorie und tragen Sie das Ergebnis in die entsprechende Zelle „Gewichtete Punktzahl“ ein.
3. Addieren Sie für jeden Hersteller alle **Gewichteten Punktzahlen** in der Spalte und tragen Sie die Summe in der Zeile **Gewichtetes Gesamtergebnis** am Ende der Tabelle ein.
4. Verwenden Sie das **Gewichtete Gesamtergebnis**, um Hersteller insgesamt zu vergleichen, und erfassen Sie qualitative Beobachtungen oder Risiken separat.

		Hersteller 1		Hersteller 2		Hersteller 3		Hersteller 4	
Kategorie	**Gewichtung**	**Bewertung**	**Gewichtete Bewertung**	**Bewertung**	**Gewichtete Bewertung**	**Bewertung**	**Gewichtete Bewertung**	**Bewertung**	**Gewichtete Bewertung**
Isolation / Air Gap	10								
Unveränderlichkeit / WORM	10								
Trennung von Zugriffskontrollen	10								
Starke Authentifizierung (MFA / Quorum)	8								
Bedrohungserkennung / Anomalie	8								
Blockieren der Wiederherstellung infizierter Snapshots	8								
Wiederherstellungsorchestrierung	8								
Reinraum / Validierung	8								
Compliance / Auditierbarkeit	8								
SaaS-Einfachheit / TTV	7								
Hybrid / Multicloud-Flexibilität	8								
TCO / Betriebsaufwand	7								
Gewichtete Gesamtsumme									

Moderne Cyber-Vaulting-Lösungen liefern messbare Geschäftsergebnisse:

- **Ausfallsicherheit**: Eine physisch oder logisch isolierte Wiederherstellungskopie, die auch dann intakt bleibt, wenn die Backup-Plattformen kompromittiert werden.
- **Kontinuität**: Die Speicherung von Backups in einem Tresor stellt sicher, dass Unternehmen unabhängig vom Ausmaß des Angriffs über eine Kopie ihrer Daten zur Wiederherstellung verfügen.
- **Compliance**: Unveränderlicher Speicher und die Durchsetzung von Aufbewahrungsfristen liefern nachprüfbare Nachweise für den Datenschutz und die Wiederherstellungsbereitschaft.
- **Vertrauen**: Wiederherstellungspunkte werden außerhalb des operativen Einflussbereichs gesichert und können vor der Verwendung überprüft werden, wodurch sichergestellt wird, dass die wiederhergestellten Daten fehlerfrei und unbeeinträchtigt sind.

Cyber-Vaulting verbindet IT-Betrieb, Sicherheit und Compliance miteinander, sodass im Krisenfall eine saubere Wiederherstellung gewährleistet ist und nicht dem Zufall überlassen bleibt.

Von der Abhängigkeit von Backups hin zu einer widerstandsfähigen Wiederherstellung: Bethany Children's Health Center

Viele Organisationen integrieren Cyber-Vaulting als festen Bestandteil ihrer Datensicherungsstrategie. Ein Beispiel hierfür ist das Bethany Children's Health Center in Oklahoma, das Kinder mit komplexen medizinischen Bedürfnissen betreut. Um eine lückenlose Versorgung zu gewährleisten, muss das Zentrum sensible Gesundheitsdaten schützen und diese im Falle eines Cyberangriffs oder einer Katastrophe schnell wiederherstellen. Bethany erfüllt diese Anforderungen, indem es unveränderliche Backups sowohl On-Premise als auch in Cohesity FortKnox, einem isolierten Cloudspeicher, speichert.

Um die Ausfallsicherheit zu erhöhen, hält sich Bethany an das 3-2-1-Prinzip, wonach drei Kopien der Daten auf zwei verschiedenen Datenträgern aufbewahrt werden, von denen eine Kopie an einem externen Standort gelagert wird. Zwei unveränderliche Sicherungskopien werden vor Ort aufbewahrt, während die dritte in Cohesity FortKnox gespeichert wird.

Cohesity FortKnox bietet einen verwalteten Cyber-Vaulting-Dienst für DataProtect- und NetBackup-Umgebungen, der über AWS, Azure und GCP bereitgestellt wird sowie als On-Premise-Lösung für Umgebungen mit höchsten Sicherheitsanforderungen. FortKnox vereint Isolation, Unveränderlichkeit und Automatisierung, um eine schnelle, saubere und verifizierte Wiederherstellung im Unternehmensmaßstab zu gewährleisten.

FortKnox bietet eine zusätzliche Sicherheitsebene: einen sicheren, luftisolierten Tresor, der gewährleistet, dass kritische Daten sicher, konform und wiederherstellbar bleiben.

Nächste Schritte zur Bewertung Ihrer Cyber-Resilienz

Ihr Resilienzplan darf sich nicht auf Annahmen stützen, die nicht mehr zutreffen. Da Cyberangriffe immer aggressiver werden, hängt die Geschäftskontinuität zunehmend von der Zuverlässigkeit Ihrer letzten und sichersten Datenkopie ab. Cyber-Vaulting stellt einen proaktiven Ansatz dar, der die Wiederherstellung nach Cyberangriffen verbessert und Ausfallzeiten verringert.

Beginnen Sie mit einer Bewertung:

- **Sichern Sie die SaaS-, On-Premise- und Cloud-Daten aus all Ihren Datenquellen auf einer zentralen, modernen Plattform?**
- **Haben Sie Ihre Plattform durch MFA, Unveränderlichkeit und rollenbasierte Zugriffskontrolle (RBAC) gesichert?**
- **Halten Sie die 3-2-1-Backup-Regel ein?**
- **Welche Isolationsmaßnahmen trennen Ihre Backup-Daten von den Produktionsnetzwerken?**
- **Wie oft scannen Sie Ihre Backups auf Bedrohungen?**
- **Wie oft testen Sie Ihren Cyber-Notfallplan?**
- **Wie schnell konnten Sie bei Ihrem letzten Cyber-Notfalltest den Betrieb wiederherstellen?**

Jetzt ist es an der Zeit, die Cyber-Resilienz von einem technischen Ziel zu einer strategischen Notwendigkeit zu erheben. Vorbereitung – statt Vermutungen – ist der entscheidende Wettbewerbsvorteil.

Erfahren Sie, wie moderne Cyber-Vaulting-Lösungen Ihre Daten schützen, Ihre Wiederherstellungsfähigkeit stärken und Ihnen die Gewissheit geben, unabhängig von der jeweiligen Bedrohung sicher zu arbeiten. Erfahren Sie mehr auf https://www.cohesity.com/de-de/platform/fortknox/

COHESITY

cohesity.com/de-de
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

4500065-001-DE 2-2026