Die vier wichtigsten Sicherheitsmaßnahmen für eine saubere und zuverlässige Recovery

Daten sind anfällig für unzählige Bedrohungen – von Cyberangriffen und Hardwareausfällen bis hin zu Naturkatastrophen. Eine robuste, mehrschichtige Backup-Strategie schützt Ihre Daten, gewährleistet die Geschäftskontinuität, reduziert das Risiko von Datenverlust und stärkt Ihre allgemeine Sicherheitslage.

Hier sind vier Maßnahmen zur Verbesserung Ihrer Sicherheitslage, damit Ihre Daten immer sauber und wiederherstellbar sind.

1. Implementierung von Zugriffskontrollen und Authentifizierungen

- Stellen Sie sicher, **dass nur autorisierte Benutzer auf Ihre Daten zugreifen können.** Eine zusätzliche Sicherheitsebene ist für den Schutz vor internen und externen Bedrohungen unerlässlich. Die allgemeine Aktivierung der Multifaktor-Authentifizierung (MFA) ist ein effektives Mittel zum Schutz vor diesen Bedrohungen und zur Pflege Ihrer bestehenden Identitäts- und Zugriffsverwaltungsrichtlinien.
- **Beschränken Sie Zugriffe und Berechtigungen basierend auf Benutzerrollen.** Wenden Sie eine rollenbasierte Zugriffskontrolle (RBAC) an, um den Benutzern in Ihrer Backup-Umgebung begrenzten, granularen Zugriff und Berechtigungen basierend auf ihren spezifischen Rollen zu gewähren. Dadurch wird sichergestellt, dass jede Person nur über die Mindestzugriffsberechtigungen verfügt, die zur Erfüllung ihrer Verantwortlichkeiten erforderlich sind.

2. Priorisierung von Datenschutz und -integrität

- **Implementieren Sie einen unveränderlichen Datentresor.** Um Ihre Daten vor Manipulationen zu schützen, sollten Sie Cohesity NetBackup Flex Appliance oder Cohesity FortKnox für einen sicheren und manipulationssicheren, unveränderlichen Speicher On-Premises oder in der Cloud in Betracht ziehen.
- Implementieren Sie eine 3-2-1-Backup-Strategie für kritische Workloads. Bewahren Sie drei Kopien von Daten auf zwei verschiedenen Medien mit mindestens einer Kopie außerhalb des Standorts in einem unveränderlichen und unlöschbaren Speicher auf. Dies sorgt für Datenredundanz und trägt dazu bei, dass Ihre Daten immer wiederhergestellt werden können.
- Verhindern Sie die Exfiltration von Daten mittels starker Verschlüsselung. Schützen Sie Ihre Daten vor unbefugtem Zugriff während der Übertragung und Speicherung. Um unbefugten Zugriff und Datendiebstahl zu verhindern, verwenden Sie eine starke Verschlüsselung für alle Ihre Daten, unabhängig davon, ob sie On-Premises oder in der Cloud gespeichert werden.

3-2-1-Backup-Strategie

3. Nutzung der Vorteile von Sicherheitsüberwachung und Erkennung

- Verwenden Sie Automatisierungen zur intelligenten Erkennung von Benutzerbedrohungen. Unsere adaptive Risiko-Engine überwacht das Benutzerverhalten kontinuierlich auf verdächtige Aktivitäten. Nach dem Erkennen von Anomalien oder anderen verdächtigen Benutzeraktionen initiiert die Plattform eigenständig Sicherheitsmaßnahmen, wie z. B. Multifaktor-Authentifizierung, um den Zugriff auf Backup-Daten zu sperren.
- Beschleunigen Sie die Erkennung von Bedrohungen und die Reaktion darauf. Cohesity bietet schnelle Funktionen zur Bedrohungssuche, die proaktiv nach Indikatoren für eine Gefährdung suchen und auf Bedrohungen reagieren. Wir bieten auch eine vollständige Analyse der Angriffsbereiche in der gesamten Umgebung – und zwar bis zu 93 % schneller als herkömmliches Malware-Scanning.

4. Härtung Ihrer Systemkonfiguration

- **Erstellen Sie eine Digital Jump Bag**™. Hierbei handelt es sich um ein geschütztes und vertrauenswürdiges Repository, das schnellen Zugriff auf die Tools bietet, die für die Fernerfassung und -analyse benötigt werden. Sie enthält die für die Reaktion auf einen Vorfall erforderlichen Tools, Software, Konfigurationsdateien und Dokumentationen in einem verschlüsselten, unveränderlichen Speicher – außerhalb der Reichweite von Angreifern.
- **Verringern Sie die Netzwerkexposition**. Implementieren Sie Netzwerkzugriffskontrollen, um den Netzwerkzugriff auf Backup-Systeme und -Daten zu beschränken und unbefugten Zugriff zu verhindern. Segmentieren Sie ganz einfach Ihr Netzwerk und erstellen Sie eine Clean-Room-Umgebung, um die Sicherheit zu erhöhen und die Auswirkungen potenzieller Sicherheitsverletzungen zu minimieren.
- **Implementieren Sie die Wiederherstellung von Clean-Room-Daten.** Schaffen Sie eine separate, sichere Umgebung für Forensik- und Wiederherstellungsvorgänge, um das Kontaminationsrisiko zu verringern.
- **Halten Sie Systeme und Software auf dem neuesten Stand**. Aktualisieren Sie regelmäßig Ihre Software und installieren Sie Sicherheitspatches, um neue Funktionen und verbesserte Sicherheitsmaßnahmen zu nutzen.

Teilen Sie diese Richtlinien Ihrem Team mit und ermutigen Sie es, diese wichtigen Schritte umzusetzen, um die Daten Ihres Unternehmens zu schützen und Ihre Sicherheitslage zu stärken.

Blueprints und Best Practices für die Erstellung einer Backup-Umgebung für Ihr Unternehmen finden Sie hier: *Moderne Topologien für Datensicherheit und -management: Ein Leitfaden für IT-Führungskräfte*.

COHESITY

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

9100085-001-DE 6-2025