Cove Data Protection™ from N-ABLE

Datenresilienz für Cyberversicherungen

Erfahren Sie, wie Cove Data Protection Ihnen dabei hilft, Risiken zu reduzieren, Compliance zu gewährleisten und Ihre Position in Sachen Cyberversicherung zu stärken

Für Cyberversicherer reicht ein Mindestmaß an Cybersicherheit längst nicht mehr aus. Mittlerweile verlangen sie greifbare und überprüfbare Datensicherheitspraktiken als Voraussetzung für Versicherungsschutz. Deshalb müssen IT-Verantwortliche proaktive Maßnahmen ergreifen, um robuste Backup-Strategien zu implementieren, die mehr leisten als nur die Speicherung von Daten. Sie müssen nachweisen, dass die Organisation sicher, schnell und zuverlässig wiederhergestellt werden kann. Hier sehen Sie fünf Möglichkeiten, dies zu erreichen – und erfahren, wie Cove Data Protection Sie dabei unterstützen kann.

Fünf Anforderungen an Backups für die Compliance mit Cyberversicherungen

1 Regelmäßige, verschlüsselte Datensicherungen

Das bedeutet: Regelmäßige Datensicherung und Verschlüsselung während der Übertragung und im Speicher.

Warum das wichtig ist: Gewährleistet, dass Daten sicher und wiederherstellbar sind, selbst wenn sie abgefangen oder gestohlen werden.

Wie Cove überzeugt: Mit der TrueDelta-Technologie werden bis zu 60-mal weniger Daten übertragen, und das alle 15 Minuten, wobei alle Backups während der Übertragung und im Speicher mit einer 256-Bit-Verschlüsselung geschützt werden.

2 Trennung von Backup- und Produktionsumgebungen

Das bedeutet: Entwicklung von Backup-Systemen, die physisch und/oder logisch von Produktionsumgebungen getrennt sind.

Warum das wichtig ist: Verhindert, dass Ransomware oder Insider-Bedrohungen gleichzeitig Produktions- und Backup-Daten kompromittieren.

Wie Cove überzeugt: Cove reduziert die Angriffsfläche durch ein cloud-natives Design, bei dem jedes Backup direkt an einen externen Standort gesendet wird. Wir verfügen über Rechenzentren, die den Anforderungen von NIST800-53, SOC 1 Typ II, SOC 2 Typ II, ISO27001, PCI DSS und HIPAA entsprechen, mit insgesamt 30 Standorten in 17 Ländern für eine sichere, geografisch eingeschränkte Datenspeicherung.

3 Unveränderliche Backups

Das bedeutet: Datenbackups, die während eines festgelegten Zeitraums von keinem Benutzer oder Prozess, einschließlich Administratoren, geändert, gelöscht oder manipuliert werden können.

Warum das wichtig ist: Gewährleistet den Zugriff auf unverfälschte Wiederherstellungsdaten, selbst bei komplexen Angriffen.

Wie Cove überzeugt: Cove Fortified Copies sind sekundäre, unveränderliche Backups, die in einer isolierten Umgebung ohne Verbindung zur Backup-Umgebung gespeichert werden. Immer aktiv, stündlich erstellt und 30 Tage lang ohne manuelles Eingreifen aufbewahrt.

4 Wiederherstellungstests

Das bedeutet: Regelmäßige Überprüfungen, ob Backups erfolgreich wiederhergestellt werden können.

Warum das wichtig ist: Bietet die Gewissheit, dass Backups bei Bedarf sicher wiederhergestellt werden können.

Wie Cove überzeugt: Die gehosteten und automatischen Wiederherstellungstests starten eine Wiederherstellungsmaschine in der sicheren N-able-Cloud und machen einen Screenshot des Startbildschirms als Nachweis für die Wiederherstellbarkeit an die Konsole. Darüber hinaus bietet unsere KI/ML-gestützte Boot-Verifizierung mit einer Erfolgsquote von über 99 % Gewissheit.

5 Mehrfaktor-Authentifizierung (MFA) für den Zugriff auf Backups

Das bedeutet: Für den Zugriff auf Backup-Systeme oder die Einleitung einer Wiederherstellung ist eine MFA erforderlich.

Warum das wichtig ist: Fügt eine wichtige Ebene der Zugangskontrolle hinzu und verhindert so unbefugte Manipulationen an Backups.

Wie Cove überzeugt: Obligatorische MFA automatisch für alle Benutzer aktiviert (Google Authenticator, Microsoft Authenticator, Duo Mobile, Authy). Zusätzlich legen rollenbasierte Zugriffskontrollen fest, welche Aktionen Benutzer ausführen dürfen.

Warum diese Anforderungen wichtig sind

- **Risikominderung**
  Jede Maßnahme – Kontrolle, Verschlüsselung, MFA, Unveränderlichkeit und Air Gap – fügt eine weitere Verteidigungsschicht hinzu. Gemeinsam reduzieren sie die Wahrscheinlichkeit und die Auswirkungen eines erfolgreichen Cyberangriffs erheblich.
- **Geringere Versicherungskosten**
  Versicherungsgesellschaften knüpfen Prämien und Selbstbehalte zunehmend an die Cybersicherheit eines Unternehmens. Proaktive Backup-Richtlinien können zu Kosteneinsparungen oder einem umfassenderen Versicherungsschutz führen.
- **Einhaltung von Richtlinien**
  Von der DSGVO über HIPAA bis hin zu Datenschutzgesetzen auf Landesebene sind sichere und wiederherstellbare Backups häufig vorgeschrieben. Diese Maßnahmen tragen dazu bei, gesetzliche Verpflichtungen zu erfüllen und Sanktionen zu vermeiden.
- **Reduzierte Ausfallzeiten**
  Dank zuverlässiger Backups, die an sicheren, externen Standorten gespeichert werden, erfolgt die Wiederherstellung schnell und effizient, wodurch Umsatzverluste und Betriebsunterbrechungen während eines Cyberangriffs auf einen Minimum beschränkt werden.

Fazit: Cyberresilienz beginnt mit intelligenteren Backups

Durch die Umsetzung dieser fünf elementaren Maßnahmen mit Cove können IT-Verantwortliche Versicherungsanforderungen erfüllen, die betriebliche Ausfallsicherheit verbessern und sicherstellen, dass sie im Falle eines Cybervorfalls ohne Kompromisse schnell wieder betriebsbereit sind.

So können Sie aktiv werden

Analysieren Sie Ihre aktuelle Backup-Umgebung anhand dieser fünf Vorgehensweisen.

Sprechen Sie mit Ihrem Cyberversicherer, um die spezifischen Versicherungsbedingungen zu klären.

Rüsten Sie auf eine moderne Backup-Lösung auf, mit der diese Best Practices mühelos umgesetzt und durchgesetzt werden können.

Sichere Backups sind kein Luxus mehr, sondern eine Voraussetzung für die Versicherbarkeit. Cove unterstützt Sie dabei, Ihre Compliance-Anforderungen problemlos zu erfüllen.

Cove Data Protection™ from N-ABLE

Cloud-native Datensicherheit-as-a-service

Cove Data Protection™ ist Ihr sicherer Ausweg aus komplexen Backups, Personalmangel und Angst vor unvollständiger Wiederherstellung. Was andere Lösungen nicht können, ist für Cove ein Klacks.

n-able.com/de/products/cove-data-protect