eBOOK

Cyber Recovery 101

Ihr Leitfaden zum Aufbau eines widerstandsfähigen, Cloud-first Unternehmens

Commvault®

KONTENT

Überblick

Es vergeht kaum eine Woche, in der nicht Schlagzeilen über einen weiteren Cybervorfall eines Unternehmen berichten.

Selten vergeht eine Woche, ohne dass die Schlagzeilen von einem weiteren Datenleck berichten, das Kunden eines weiteren Unternehmens betrifft.

Während Verbraucher ihre Konten im Auge behalten, um den persönlichen Schaden zu ermitteln, bemüht sich das Unternehmen, die Auswirkungen auf den Geschäftsbetrieb, die Daten von Kunden, Mitarbeitern und dem Unternehmen, den Ruf der Marke und die finanzielle Bilanz zu minimieren. Jeder Aspekt eines Unternehmens ist bei einem Cyberangriff gefährdet, wodurch Cyber-Resilienz nicht nur ein Luxus, sondern eine Notwendigkeit wird. Unternehmen müssen darauf vorbereitet sein, Cyberbedrohungen standzuhalten und sich davon zu erholen, um den kontinuierlichen Geschäftsbetrieb zu ermöglichen. Dieser Leitfaden beschreibt effektive Strategien, um diese Cyber-Resilienz zu erreichen, von der Definition der Cyber-Recovery bis hin zur Unterstützung beim Aufbau eines effektiven Recovery-Plans.

Cyber Recovery

vs.

Cyber Recovery konzentriert sich auf spezifische Maßnahmen und Strategien, die erforderlich sind, um sich von cyberbezogenen Vorfällen wie Datenverletzungen, Malware-Angriffen und Ransomware zu erholen. Dabei geht es darum, Daten, Systeme und Betriebsabläufe wiederherzustellen, die von Cyberbedrohungen betroffen sind.

Disaster Recovery

Disaster Recovery hingegen ist ein breiteres Konzept, das alle Arten von Katastrophen umfasst, einschließlich Naturkatastrophen, Hardwareausfällen und menschlichen Fehlern. Es zielt darauf ab, den normalen Betrieb nach jeder Art von störendem Ereignis wiederherzustellen. Ihr Unternehmen muss darauf vorbereitet sein, auf alle Bedrohungen zu reagieren und zu antworten, die ihm begegnen. Und obwohl sie häufig zusammen diskutiert werden, sind Cyber Recovery und Disaster Recovery nicht dasselbe.

Das Verständnis der Unterschiede ist entscheidend für den Aufbau einer effektiven Wiederherstellungsstrategie. Während beide entscheidend sind, ist Cyber Recovery eine spezialisierte Teilmenge von Disaster Recovery, die darauf abzielt, die einzigartigen Herausforderungen zu bewältigen, die durch Cyberbedrohungen entstehen. Weitere Informationen finden Sie in unserem eBook “Beyond Disaster Recovery: Why You Need a Different Strategy When Cyber Attacks Strike” und unserer Infografik “Disaster Recovery ≠ Cyber Recovery”.

Aufbau eines effektiven Cyber Recovery Plans

Ein umfassender Cyber Recovery Plan ist für jede Organisation, die Cyber-Resilienz anstrebt, unerlässlich. Hier erfahren Sie, was ein solcher Plan beinhaltet und was nicht, zusammen mit einer detaillierten Beispielvorlage. Beim Aufbau Ihres Cyber Recovery Plans ist es wichtig, die Bedürfnisse in Ihrer gesamten Organisation zu bewerten. Das bedeutet, Sie müssen:

Kritische Vermögenswerte identifizieren:

Systeme, Daten und Anwendungen sowie Teammitglieder auf, die Schutz benötigen.

Risikobewertung durchführen:

und Schwachstellen identifizieren, die mit diesen Vermögenswerten verbunden sind. Stellen Sie sicher, dass Ihr Plan Wege zur Behebung von Schwachstellen und zur Risikominderung enthält.

Schlüssel-Teams und Teammitglieder identifizieren:

Definieren Sie Rollen und Verantwortlichkeiten für alle Teams, die für die Reaktion und Wiederherstellung in Ihrer gesamten Organisation zuständig sind.

Wiederherstellungsverfahren festlegen:

Erstellen Sie detaillierte Schritte zur Wiederherstellung von Daten, Systemen und Betriebsabläufen.

Kommunikationsplan erstellen:

Skizzieren Sie, wie Sie während und nach einem Vorfall mit Stakeholdern, Mitarbeitern, Kunden, Lieferanten und den Medien kommunizieren.

Tests und Schulungen durchführen:

Testen Sie Ihren Plan regelmäßig und schulen Sie das Personal in Bezug auf ihre Rollen. Bieten Sie regelmäßige Cyber-Sicherheitsschulungen für Mitarbeiter zu Themen wie Phishing an und ermutigen Sie sie, verdächtige Vorfälle sofort zu melden.

× WAS EIN CYBER RECOVERY PLAN NICHT ENTHÄLT

So umfassend Ihr Cyber Recovery Plan auch sein sollte, es ist wichtig zu beachten, dass es Bereiche gibt, die nicht Teil davon sein sollten. Dazu gehören die routinemäßigen Aufgaben und allgemeine Wartung Ihrer IT-Abteilung, Prozesse im Zusammenhang mit dem täglichen Betrieb Ihres Unternehmens und Disaster Recovery-Verfahren für Naturkatastrophen und Hardwareausfälle.

Cyber Recovery Plan Vorlage

Verwenden Sie diese Vorlage, um Ihren eigenen Cyber Recovery Plan zu erstellen – oder um sicherzustellen, dass Ihr Plan alle notwendigen Schritte zur Minderung der Auswirkungen eines Cyberangriffs enthält.

Kritische Vermögenswerte identifizieren:

- **Systeme:** CRM, ERP, E-Mail-Server
- **Daten:** Kundeninformationen, Mitarbeiterdaten, Finanzunterlagen, geistiges Eigentum
- **Anwendungen:** Vertriebssoftware, Buchhaltungssoftware, HR-Management-System, kundenorientierte Anwendungen

Risikobewertung durchführen

- **Risiken:** Datenverletzungen, Ransomware-Angriffe, DDoS-Angriffe
- **Schwachstellen:** Veraltete Software, schwache Passwörter, mangelnde Mitarbeiterschulungen
- **Maßnahmen:** Software aktualisieren, stärkere Passwörter durchsetzen, regelmäßige Schulungen einführen

Schlüssel-Teams identifizieren

- **Teams:** Breach Response und Recovery Team, Regulatory und Legal Team, Business Readiness Team
- **Rollen:** Incident Commander, Technical Lead, Communications Lead, Legal Adviser
- **Verantwortlichkeiten:** Reaktion koordinieren, Systeme wiederherstellen, mit Stakeholdern kommunizieren, Compliance sicherstellen

Wiederherstellungsverfahren festlegen

- **Schritt 1:** Betroffene Systeme isolieren, um eine weitere Ausbreitung zu verhindern.
- **Schritt 2:** Quelle und Art des Angriffs identifizieren.
- **Schritt 3:** Daten aus Backups wiederherstellen.
- **Schritt 4:** Software neu installieren und aktualisieren.
- **Schritt 5:** Wiederhergestellte Systeme auf Funktionalität testen

Kommunikationsplan erstellen

- **Interne Kommunikation:** Mitarbeiter über den Vorfall und den Fortschritt der Wiederherstellung informieren.
- **Externe Kommunikation:** Kunden, Partner und Aufsichtsbehörden nach Bedarf informieren.

Tests und Schulungen durchführen

- **Tests:** Regelmäßige Übungen und Simulationen durchführen, um den Wiederherstellungsplan zu testen. Vollständige Datenwiederherstellungen in temporären Umgebungen durchführen, um den Prozess und die Datenintegrität zu validieren.
- **Schulungen:** Fortlaufende Schulungen für die Incident Response Teams und alle Mitarbeiter anbieten.

Durch die Befolgung dieser Anleitung kann Ihre Organisation einen soliden Cyber Recovery Plan erstellen, der Ihre Cyber-Resilienz erheblich verbessert und Sie besser auf jeden Cyber-Vorfall vorbereitet. Erfahren Sie mehr darüber, wie Commvault Ihnen helfen kann, indem Sie hier klicken.

commvault.com | 888.746.3849 | get-info@commvault.com

Commvault®