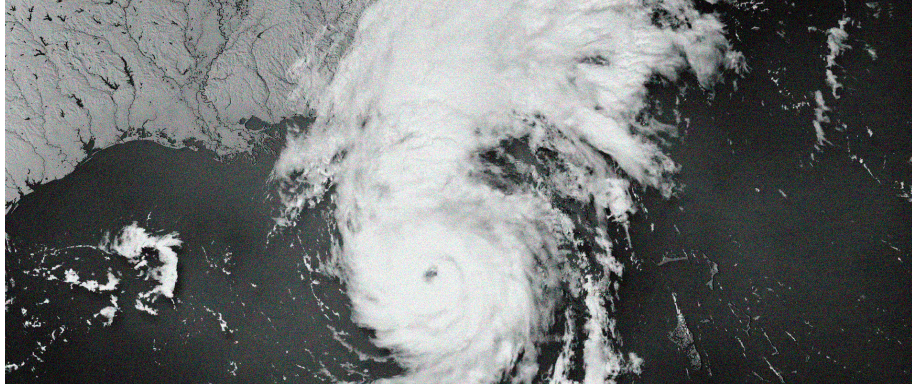
eBOOK

MEHR ALS
NUR

DISASTER RECOVERY

Warum Sie bei Cyberangriffen eine andere Strategie benötigen

Commvault®



Ihr Ansatz zur Wiederherstellung beginnt hier

Von Wetterereignissen bis hin zu böswilligen Cyberangriffen gibt es heutzutage keinen Mangel an zerstörerischen Ereignissen, die Ihre Geschäftsabläufe bedrohen. Unsere Nachrichtenfeeds sind gefüllt mit Geschichten über Schäden von Hurrikanen bis hin zu Ransomware.

Als Teil einer jeden guten Geschäftskontinuität müssen Sie einen Plan haben, wie Ihre Organisation nach einem Vorfall schnell wieder auf die Beine kommt. Sie sollten sich darauf konzentrieren, Ihre Mitarbeiter, Ihre Kunden und all Ihre Daten zu schützen, während Sie den Schaden an Ihren Vermögenswerten, Finanzen und sowie Ihrer Reputation minimieren.

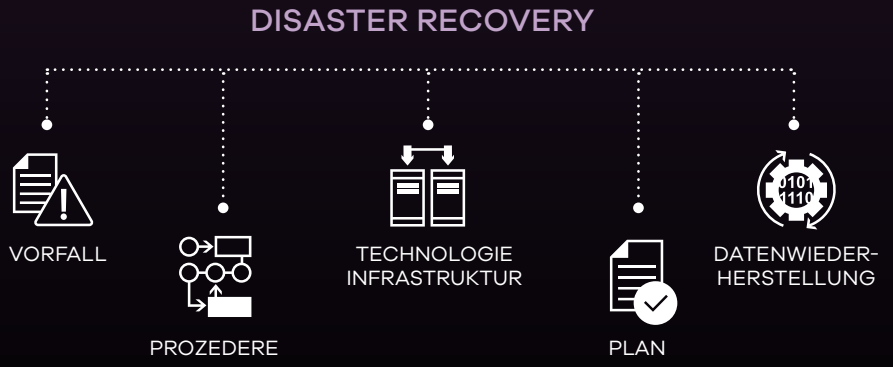
Aber die Widerstandsfähigkeit gegenüber diesen Bedrohungen erfordert Wachsamkeit. Disaster Recovery und Cyber Recovery sind nicht dasselbe, daher ist es entscheidend, die Unterschiede zu verstehen. Lesen Sie weiter, um zu erfahren, warum Sie beide Arten von Wiederherstellungsplänen in Ihrem Arsenal haben sollten – und warum die Definition der Mindestfunktionalität in Ihrer Organisation ein wichtiger Bestandteil der Cyber Recovery ist.

Mit gründlicher Vorbereitung, einer umfassenden Teststrategie, die regelmäßig durchgeführt wird, und Lösungen für eine schnelle Wiederherstellung und Neuaufbau aller Ihrer Anwendungen und Daten – werden Sie in der Lage sein, die Herausforderungen der Wiederherstellung zu meistern.

Warum Sie eine Disaster Recovery benötigen

Sie benötigen einen Disaster Recovery-Plan, um vorhersehbare Ereignisse wie Hardware-Ausfälle oder Naturkatastrophen wie Brände und Überschwemmungen zu bewältigen. Im Allgemeinen sind diese Vorfälle nicht beabsichtigt und zielen nicht aktiv auf Ihre Daten ab.

Die Disaster Recovery folgt in der Regel einem vorab erstellten Plan mit festgelegten Schritten zur schnellen Wiederherstellung von Systemen. Durch die Wiederherstellung von Backups können Sie auch dann wieder online gehen, wenn einige Daten verloren gehen. Dieser Prozess zielt darauf ab, die kontinuierliche Geschäftstätigkeit aufrechtzuerhalten, den langfristigen Einfluss zu minimieren und kritische Daten zu schützen.



Warum Sie eine Cyber-Wiederherstellung benötigen

Im Gegensatz dazu bekämpft die Cyber Recovery bösartige Angriffe wie Ransomware oder Datenschutzverletzungen, bei denen Angreifer aktiv versuchen, Ihre Systeme zu schädigen und Ihre Daten zu zerstören. Dabei kann es sich um einen Teil der Daten oder die gesamte Infrastruktur handeln, einschließlich eines Disaster Recovery Failover-Standorts.

Cyberangriffe umfassen häufig Untersuchungen und Maßnahmen zur Problembehebung, bevor eine Wiederherstellung erfolgt, was einen längeren Zeitraum in Anspruch nehmen kann. Sie müssen den Angriff eindämmen und sicherstellen, dass keine Exploit-Spuren übrigbleiben. Jedes Element Ihrer Umgebung, von der Hardware bis hin zu Daten und Sicherungen, muss vor der Wiederherstellung auf Infektionen untersucht werden, da Angreifer möglicherweise Malware versteckt oder Sicherungsdateien geändert haben. Sie müssen den Schaden minimieren, Datenverlust verhindern und den Sicherheitsstatus aufrechterhalten.

Keine Geschäftstätigkeit ohne Mindestfunktionalität

Wenn ein Cyberangriff Ihre Organisation offline stellt, ist der Druck hoch, die Betriebsabläufe so schnell wie möglich wiederherzustellen, um finanzielle und reputative Schäden zu minimieren. Ein wichtiger Aspekt der Cyber Recovery ist daher die Definition der Mindestfunktionalität Ihrer Firma – das heißt, der minimale Satz an Systemen, Daten und Prozessen, die Sie wiederherstellen müssen, um nach einer Unterbrechung weiter operativ zu bleiben.

01 Kritische Vermögenswerte

Beginnen Sie damit, Ihre kritischsten Vermögenswerte zu identifizieren – Systeme (Infrastruktur, mission-kritische Anwendungen, Kommunikationswerkzeuge); Daten (Betriebsdaten, Compliance-Daten, Backups); und Prozesse (Geschäftsabläufe, IT und Sicherheit, Kundenbindung).

02 Bewerten Sie die Auswirkungen eines Ausfalls

Sobald Sie diese Vermögenswerte identifiziert haben, müssen Sie den Ausfalleinfluss bewerten. Wie viel kostet es IhreOrganisation, wenn Sie nicht operativ sind? Das Verständnis der Auswirkungen von Downtime auf Ihre kritischen Vermögenswerte ist entscheidend für die Entscheidungsfindung und hilft dabei, deren Wiederherstellung zu priorisieren.

03 Einen Plan erstellen

Als Nächstes müssen Sie einen Plan erstellen, um Ihre kritischsten Vermögenswerte im Falle eines Ausfalls wiederherzustellen – und diesen Plan gründlich testen. Stellen Sie sicher, dass Ihre Mitarbeiter in ihren Aufgaben bei der Wiederherstellung ausgebildet sind.

04 Konzentrieren Sie sich auf eine saubere, validierte Wiederherstellung

Schließlich ist es wichtig zu betonen, dass Sie eine saubere Kopie Ihrer Daten wiederherstellen sollten; air-gapped Kopien können die schnelle Wiederherstellung dieser Daten erleichtern. Außerdem sollten Sie Forensik in einem isolierten Wiederherstellungsraum durchführen, um die Ursache zu finden und zukünftige Angriffe zu verhindern.

Die Auswirkungen eines Ausfalls kennen:

$4.88M

Die durchschnittlichen Kosten eines Datenbruchs

$14,056

Die durchschnittlichen Kosten pro Minute Downtime[2]

24 TAGE

Die durchschnittliche Downtime nach einem Ransomware-Angriff[3]

1 Cost of a Data Breach Report 2024, IBM
2 IT outages: 2024 costs and containment, Enterprise Management Associates
3 Statista

Cyber-Wiederherstellung Entwurfsumfang

SZENARIEN

Die Cyber Recovery erfordert im Allgemeinen andere Bedürfnisse im Vergleich zu Katastrophenwiederherstellungs- und Business-Continuity-Plänen.

Diese Strategien können kombiniert werden, um Ressourcen und Prozesse zu bündeln.

ELEMENTE	DISASTER RECOVERY/ BUSINESS CONTINUITY	CYBER RECOVERY
KOMPROMIT-TIERUNG	Vollständiger Verlust der Betriebsabläufe	Daten, Netzwerke, Sicherheit
WIEDERHER-STELLUNG	Failover/RückfallRTO, Wiederherstellung	Auswahlweise wiederherstellen, um zu reparieren.
RESSOURCEN	Vollständiger Verfügbarkeitsstapel	Validierung, Wiederherstellung, Wiederaufbau
PLANUNG	Anhaltend	Elastisch

ORGANISATION

Die Cyber Recovery umfasst Ergebnisse der gemeinsam getragenen Verantwortung im gesamten Unternehmen (Menschen, Prozesse).

Die Integration und Automatisierung von Benachrichtigungen, Maßnahmen und nahtlosen Workflows über die Teams hinweg kann die Ergebnisse beschleunigen.

FÄHIGKEITEN

Die Anforderungen an die Cyber Recovery hängen von den Zielen der Organisation ab.

- Sichere, isolierte und unveränderliche Vault-Backups
- Frühe Erkennung von verdächtigen Mustern
- Cyberanalyse und Datensanitierung
- Automatisierte Wiederherstellungsvalidierung
- Geplante, schnelle Wiederherstellung

Disaster Recovery-Tests reichen hier nicht aus

Disaster Recovery-Tests sind wichtig, aber Cyber Recovery geht weit darüber hinaus. Beide zielen zwar darauf ab, nach Unterbrechungen die Betriebsfähigkeit wiederherzustellen, die grundlegenden Unterschiede erfordern aber unterschiedliche Reaktionen. Herkömmliche Disaster Recovery-Pläne sind nicht in der Lage, die nuancierten Bedrohungen und Komplexitäten von Cyberangriffen effektiv zu bekämpfen.

Und zwar aus folgenden Gründen:

Daher bieten Disaster Recovery-Pläne zwar eine wertvolle Grundlage für Incident-Response-Maßnahmen, es kann jedoch gefährlich sein, sich bei einem Cyberangriff darauf zu verlassen. Ein spezieller Cyber-Recovery-Plan, der durch spezielle Tools, geschultes Personal und häufige Tests unterstützt wird, ist für die Minderung der spezifischen Risiken und Komplexitäten dieser böswilligen Angriffe unerlässlich.

Cyber Recovery-Tests sind von entscheidender Bedeutung

Cyber Recovery-Tests sind sozusagen ein Probelauf (oder Funktionstest) zur Wiederherstellung einer Anwendung und ihrer Daten aus einem Backup. Dies ist die Art von Wiederherstellungsprozess, der bei einem Cybervorfall durchgeführt wird, und es ist der Prozess, den das NIST empfiehlt. Disaster Recovery-Tests und Cyber Recovery-Tests haben jeweils ihren Nutzen in den zutreffenden Szenarien, aber Cyber Recovery ist viel umfassender.

Cyber Recovery Tests ermöglichen Ausfallsicherheit für Ihre Systeme und Daten sowie Geschäftskontinuität. Die Wiederherstellung kritischer Anwendungen und Daten ist komplex und mit Problemen verbunden. Cyber-Recovery-Tests helfen dabei, Fehler aufzudecken und zu beheben, wenn nichts auf dem Spiel steht.

Tests geben Ihren Teams die Praxis und das Vertrauen, wichtige Anwendungen und Daten bei einem Cyber-Vorfall wiederherstellen zu können.

Das NIST empfiehlt sogar „Datensicherungen durchzuführen, zu schützen, zu pflegen und zu testen", da „es besser ist, ein unerwartetes Problem während eines Tests zu erkennen als während eines tatsächlichen Cyber-Vorfalls". Aber in Wirklichkeit führen nur sehr wenige Unternehmen umfassende, häufige und erfolgreiche Tests durch.

IN ZAHLEN

194 TAGE
Durchschnittliche Zeit eines Angreifers in einem Unternehmen[1]

Angreifer beginnen sich innerhalb von

48 MINUTEN
nach einem Angriff lateral zu bewegen[2]

82% DER UNTERNEHMEN
die Lösegeld zahlen, erhalten nicht alle ihre Daten zurück[3]

1 https://www.ibm.com/reports/data-breach
2 https://go.crowdstrike.com/2025-global-threat-report.html
3 https://www.hiscoxgroup.com/news/blog/hiscox-cyber-readiness-report-2024

Wie Commvault Ihnen Hilft

KRITISCHE DATEN SICHER SPEICHERN:

Kritische Daten sicher speichern: Air-gapped Kopien schützen Ihre Daten vor unbefugtem Zugriff.

Häufig testen: Stellen Sie sicher, dass Ihr Wiederherstellungsplan funktioniert und Ihre Mitarbeiter wissen, was sie zu tun haben.

Saubere Kopien Ihrer Daten wiederherstellen: Überprüfen Sie, dass Sie eine unverseuchte Kopie Ihrer Daten wiederherstellen.

Forensik in einer isolierten Umgebung durchführen: Ein sicherer, isolierter Wiederherstellungsraum ermöglicht die Analyse von Angriffen und die Verhinderung zukünftiger Vorfälle.

LÖSUNGEN VON COMMVAULT:

Commvault® Cloud for AD: Enterprise Edition

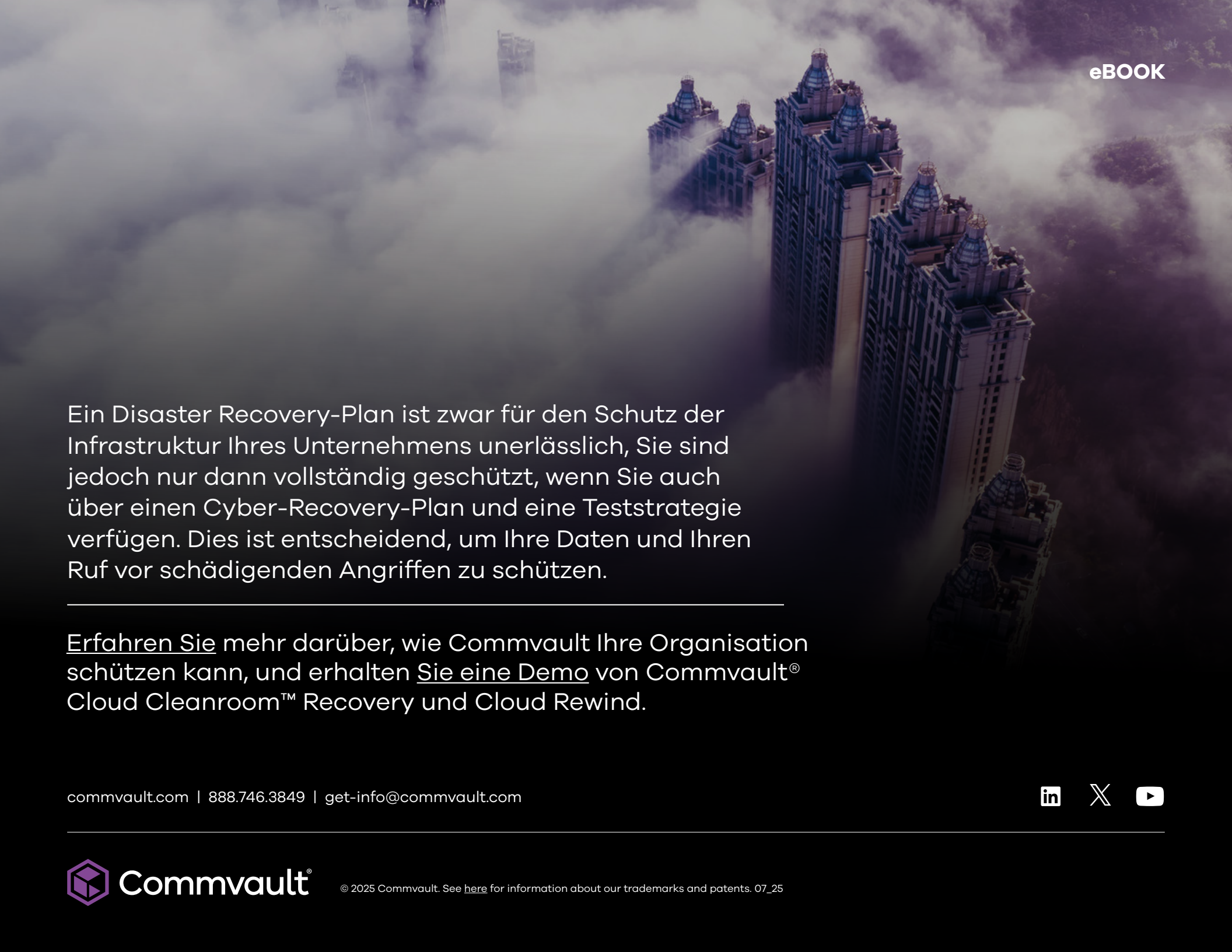
Identitäts- und Zugriffsmanagement sind entscheidend für die Wiederherstellung Ihrer Betriebsabläufe nach einem Angriff. Commvault Cloud for Active Directory Enterprise Edition ermöglicht es Ihnen, AD-Daten bei Verfälschungen, versehentlichen Löschungen und Ransomware-Angriffen zu schützen und die Wiederherstellung zu beschleunigen, indem es automatisierte Wiederherstellungen auf Forstebene ermöglicht.

Commvault® Cloud Cleanroom™ Recovery

Bietet eine sichere, isolierte Wiederherstellungsgebung nach Bedarf. Diese Lösung ist mehr als nur ein sicherer Raum. Sie ermöglicht es Organisationen, die Effektivität ihrer Cyber Recoverypläne zu testen, saubere und schnelle Wiederherstellungen Ihrer Anwendungen und Daten durchzuführen und sichere forensische Analysen durchzuführen. Mit luftgekoppeltem, unveränderlichem Speicher, eingebauter Automatisierung und künstlich-intelligenzgestützter Skalierung der Wiederherstellung hilft Cleanroom Recovery Ihnen, kontinuierliche Geschäftsbetriebe aufrechtzuerhalten, selbst bei komplexen Cyberdrohungen.

Commvault® Cloud Rewind™

Geht über traditionelle Backup- und Disaster Recovery hinaus. Sie können kontinuierlich entdecken, schützen, wiederherstellen und neu aufbauen, um Cyber-Resilienz zu schaffen und kontinuierliche Geschäftsbetriebe aufrechtzuerhalten. Mit einer patentierten Dual-Vault-Cloud-Zeitmaschine können Sie zu einem bestimmten Zeitpunkt zurückkehren und dynamische und verteilte Cloud-Anwendungen schnell von Ausfällen und Ransomware-Angriffen wiederherstellen. Mit dieser Lösung können Sie Ihre Daten, Anwendungen und Konfigurationen schnell wiederherstellen.



eBOOK

Ein Disaster Recovery-Plan ist zwar für den Schutz der Infrastruktur Ihres Unternehmens unerlässlich, Sie sind jedoch nur dann vollständig geschützt, wenn Sie auch über einen Cyber-Recovery-Plan und eine Teststrategie verfügen. Dies ist entscheidend, um Ihre Daten und Ihren Ruf vor schädigenden Angriffen zu schützen.

Erfahren Sie mehr darüber, wie Commvault Ihre Organisation schützen kann, und erhalten Sie eine Demo von Commvault® Cloud Cleanroom™ Recovery und Cloud Rewind.

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

Commvault®