

eBOOK

Mehr als nur Disaster Recovery

WARUM SIE BEI CYBERANGRIFFEN
EINE ANDERE STRATEGIE BENÖTIGEN



CONTENTS

04 Disaster
Recovery

05 Cyber
Recovery

06 Cyber Recovery-Ready
Design Scope

07 Disaster Recovery-Tests
reichen hier nicht aus

08 Cyber Recovery-Tests sind von
entscheidender Bedeutung

10 So Hilft Commvault Cloud

Sie haben Rauchmelder im ganzen Haus installiert, Ihre Kinder darin geschult, welche Rufnummer im Notfall zu wählen ist und wissen, wie Sie Ihre Privathaftpflichtversicherung kontaktieren können. Sie sind auf einen Brandfall gut vorbereitet.

Aber Sie würden nicht dieselben Maßnahmen ergreifen, um sich vor Identitätsdiebstahl zu schützen, oder? Stattdessen sind Sie vorsichtig bei der Weitergabe Ihrer Daten, haben die Telefonnummer Ihrer Bank immer griffbereit und achten auf Ihren Kontostand. Es handelt sich um ein anderes Problem, das einen anderen Ansatz erfordert.

Dasselbe gilt auch für das Rechenzentrum. Disaster Recovery und Cyber Recovery sind nicht das Gleiche. Es ist wichtig, die Unterschiede zu verstehen und eine umfassende Teststrategie zu entwickeln, damit Ihr Unternehmen auf Probleme vorbereitet ist.

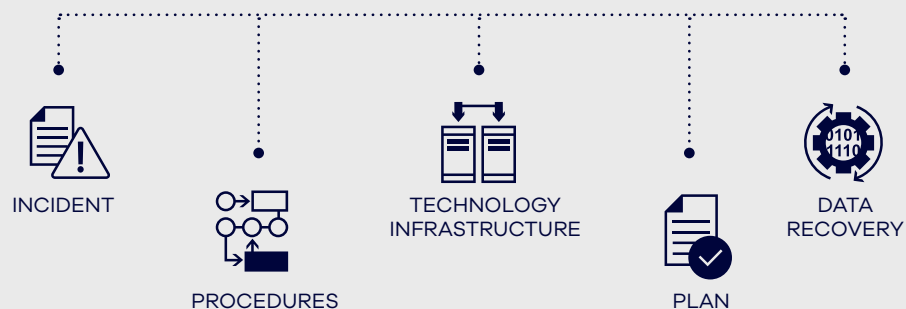


DISASTER RECOVERY

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 Geschäftskontinuität sicherzustellen, langfristige Auswirkungen zu minimieren und kritische Daten zu schützen.

DISASTER RECOVERY PROCESS



CYBER RECOVERY

Im Gegensatz dazu bekämpft die Cyber Recovery bössartige 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 Problembekämpfung, 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.



CYBER RECOVERY-READY DESIGN SCOPE

SCENARIOS

Cyber recovery generally drives a different set of needs vs. disaster recovery/business continuity plans

ELEMENTS	DISASTER RECOVERY/ BUSINESS CONTINUITY	CYBER RECOVERY
COMPROMISE	Full-site loss of operations	Data, networks, security
RECOVERY	Failover/back RTO, rebuild	Selective restore to repair
RESOURCES	Full availability stack	Validation, restore, rebuild
PLANNING	Persistent	Elastic

These strategies can be blended to converge resources and processes.

ORGANIZATION






Cyber recovery involves collaborative shared responsibility outcomes across the organization (people, process)



Integrating and automating notifications, informed actions, and seamless workflows across the teams can accelerate the outcomes.

CAPABILITIES

Cyber recovery requirements depend on the goals of the organization

-  Secure, isolated, and immutable vault backups
-  Early detection of suspicious patterns
-  Cyber analysis and data sanitization
-  Automated recovery validation
-  Planned, rapid recovery

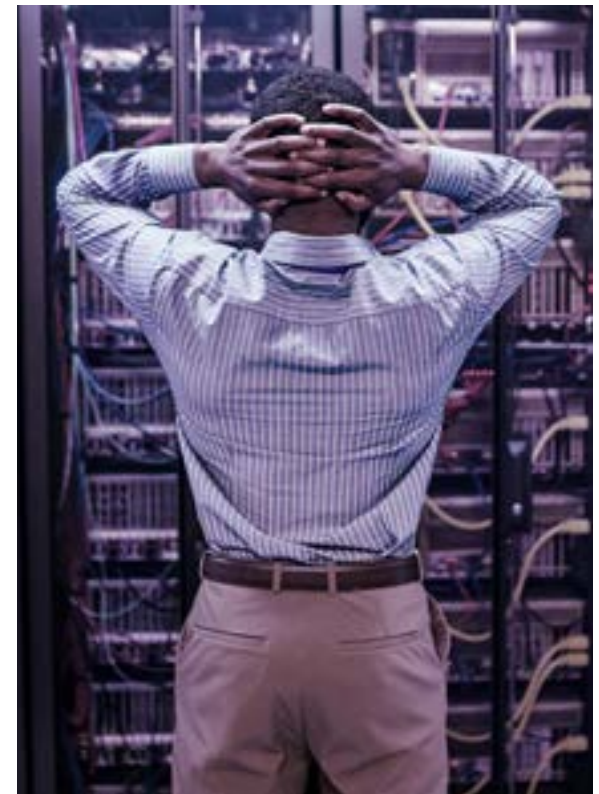
DISASTER RECOVERY-TESTS REICHEN HIER NICHT AUS

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:

- Art der Bedrohung
- Umfang und Fokus
- Methoden und Werkzeuge
- Datenintegrität und -schwachstellen

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“¹. Aber in Wirklichkeit führen nur sehr wenige Unternehmen umfassende, häufige und erfolgreiche Tests durch.

204 TAGE

Durchschnittliche Zeit
eines Angreifers in
einem Unternehmen²

92%

der Unternehmen,
die Lösegeld zahlen,
erhalten nicht alle
ihre Daten zurück⁴

Angreifer beginnen sich innerhalb von

84 MINUTEN

nach einem Angriff lateral zu bewegen³

² <https://www.ibm.com/reports/data-breach>

³ <https://www.crowdstrike.com/resources/reports/threat-hunting-report/>

⁴ <https://www.sophos.com/en-us/content/state-of-ransomware>

SO HILFT COMMVAULT CLOUD

Mit Commvault® Cloud profitieren Sie von proaktiver Cyber-Resilienz: **Die Auto Recovery** von Commvault minimiert die Auswirkungen von Datenbedrohungen auf alle Workloads und fördert die Geschäftskontinuität. Commvault Auto Recovery bietet automatisierte proaktive Cyber-Recovery, die auf einem mehrschichtigen Datenschutzkonzept basiert und die Wiederherstellungszeit bei Cyberangriffen und anderen Katastrophenfällen reduziert. Mit einem RTO von nahezu Null und RPOs unter einer Minute schafft es Commvault Auto Recovery, die Folgen von Datenbedrohungen für Cloud-, On-Premises- und SaaS-Workloads weitgehend zu minimieren und so für Geschäftskontinuität zu sorgen.

Commvault® Cloud Cleanroom™ Recovery bietet eine kostengünstige, saubere, sichere und isolierte Wiederherstellungsumgebung auf Abruf, um Cyber-Recovery-Pläne zu testen, sichere forensische Analysen durchzuführen und ununterbrochene Geschäftskontinuität zu gewährleisten.

Anhaltende Cyberbedrohungen sowie Ransomware führen zu existenziellen Risiken und sorgen für Verwirrung und Angst im Unternehmen. Cleanroom Recovery verfügt über eine einzigartige Testumgebung zur Validierung der Effektivität von Cyber-Recovery-Plänen, -Technologien und -Prozessen.



Cleanroom Recovery verfügt über eine sichere Umgebung, in der Daten und kritische Assets isoliert und vor Angriffen geschützt werden. Sicherheits- und IT-Experten können wertvolle Einblicke in unbekannte Bedrohungsakteure gewinnen, ihre Strategien ausbauen und eine ununterbrochene Geschäftskontinuität ermöglichen.

DISASTER RECOVERY

HERAUSFORDERUNG

Disaster Recovery für Geschäftskontinuität und Standortwiederherstellung bei Naturkatastrophen oder Ausfällen.

LÖSUNG

Commvault® Cloud Auto Recovery ist die flexibelste und kosteneffizienteste Datenreplikationsplattform.

- RPOs unter einer Minute
- RTO von nahezu Null für sofortige Datenwiederherstellung
- Datentransformation während der Replikation
- Ein-Klick-Orchestrierung von der Produktion zur DR und umgekehrt
- DR-Notfallübungen zur Überprüfung der Recovery-Bereitschaft

CYBER RECOVERY

HERAUSFORDERUNG

Cyber Recovery zur Wiederherstellung von Daten und von durch Malware betroffenen Anwendungen nach einem Cyber-Vorfall

LÖSUNG

Commvault® Cloud Cleanroom™ Recovery bietet eine einfache, sichere und schnelle Wiederherstellung von Anwendungen.

- Einrichtung und Automatisierung von Reinräumen für die Wiederherstellung
- Logische Gruppierung heterogener Workloads
- Sichere Scans mit integrierten und konfigurierbaren Tools
- Recovery-Abhängigkeit und benutzerdefinierte Aktionen
- Zugriff auf die Commvault Control-Plane am bereinigten Standort
- Recovery-orientiertes Monitoring, Reporting, Auditing

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 Ihr Unternehmen schützen kann, und testen Sie eine Demo von Commvault® Cloud Cleanroom™ Recovery.

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

