eBOOK

WIE SICH ECHTE CYBERRESILIENZ UNTER DRUCK BEWAEHRT

CYBERANGRIFFE WERDEN SCHNELLER, INTELLIGENTER UND SCHWIERIGER ZU ERKENNEN. UM JEDERZEIT VORBEREITET ZU SEIN, BRAUCHEN SIE MEHR ALS NUR EINEN PLAN – SIE BRAUCHEN ECHTE CYBERRESILIENZ.

Commvault®

Inhalt

Vorbereitung vs. Echte Cyberresilienz

Jeder Anbieter spricht von Resilienz, und die meisten Unternehmen glauben, gut vorbereitet zu sein. Doch wenn ein echter Angriff erfolgt, werden Schwachstellen in der Vorbereitung schnell sichtbar.

Viele Wiederherstellungsstrategien wurden für vorhersehbare Störungen entwickelt – nicht für die intelligenten, adaptiven Bedrohungen durch KI der nächsten Generation. Fortschrittliche KI-Modelle können innerhalb weniger Stunden die gesamte Angriffsfläche eines Unternehmens autonom kartieren, Sicherheitslücken aufdecken, die jahrzehntelang unentdeckt geblieben sind, und Angreifern ermöglichen, sich schneller zu bewegen und anzupassen, als jeder Patch-Zyklus Schritt halten kann.

Cyberangriffe entwickeln sich heute schneller, bleiben länger unentdeckt und richten sich zunehmend gegen genau die Systeme, auf die Unternehmen für ihre Wiederherstellung angewiesen sind. Dadurch entstehen neue Herausforderungen:

- **Backups sind keine garantierte Rückfallebene mehr:** Angreifer nehmen Backup-Systeme zunehmend ins Visier, um Wiederherstellungsoptionen zu schwächen. In manchen Fällen werden Backup-Daten verschlüsselt, gelöscht oder kompromittiert, sodass es deutlich schwieriger wird, einen vertrauenswürdigen Wiederherstellungspunkt zu identifizieren.
- **Angreifer können lange unentdeckt bleiben:** Bedrohungsakteure können sich über längere Zeiträume in IT-Umgebungen aufhalten, sich lateral bewegen und Persistenz aufbauen. Dadurch wird es schwierig festzustellen, wann ein Angriff begonnen hat und welche Daten sicher wiederhergestellt werden können.
- **Die Wiederherstellung kann Risiken erneut einführen:** Ohne geeignete Validierung können bei der Wiederherstellung unbeabsichtigt Schadsoftware oder kompromittierte Konfigurationen erneut in Betrieb genommen werden, wodurch sich die Auswirkungen eines Vorfalls verlängern.

Vorbereitung setzt voraus, dass die Wiederherstellung sauber, schnell und zuverlässig abläuft. Die Realität wird jedoch zunehmend komplexer. Da KI der nächsten Generation Geschwindigkeit und Umfang von Angriffen weiter erhöht, benötigen Unternehmen mehr Transparenz und schnellere Reaktionsmöglichkeiten über ihre gesamte IT-Landschaft hinweg.

92%

der IT-Sicherheitsverantwortlichen geben an, dass KI-gestützte Cyberbedrohungen sie dazu zwingen, ihre Sicherheitsmaßnahmen erheblich auszubauen.[1]

[1] The State of AI Cybersecurity 2026, Darktrace

Cyberresilienz Für Eine Neue Realität

Cyberangriffe beeinträchtigen nicht nur Systeme – sie kompromittieren Daten, gefährden Identitäten und untergraben das Vertrauen. Angreifer bewegen sich häufig unbemerkt durch IT-Umgebungen, etablieren Persistenz und breiten sich über verschiedene Systeme aus, bevor sie entdeckt werden. Bis ein Sicherheitsvorfall erkannt wird, ist oft nur schwer festzustellen, welche Daten unversehrt geblieben sind und welche sicher wiederhergestellt werden können.

KI der nächsten Generation verschärft diese Herausforderung zusätzlich. Dieselben KI-Funktionen, die Verteidiger unterstützen können, werden auch eingesetzt, um Angriffe über den gesamten Angriffszyklus hinweg zu entwickeln und zu beschleunigen – von der Aufklärung bis hin zur Ausnutzung von Schwachstellen. Da die Zeitspanne zwischen der Entdeckung einer Schwachstelle und ihrer Ausnutzung immer kürzer wird, benötigen Unternehmen Cyberresilienzstrategien, die weit über das reine Patch-Management hinausgehen.

Die neue realität von heute:

- **KI beschleunigt Geschwindigkeit und Umfang von Angriffen:** Automatisierte Techniken ermöglichen es Angreifern, schneller zu agieren und sich in Echtzeit anzupassen.
- **Hybride und Multi-Cloud-Umgebungen erhöhen die Komplexität:** Daten, Anwendungen und Identitäten sind über verschiedene Umgebungen verteilt, wodurch Transparenz und Kontrolle während der Wiederherstellung schwieriger werden.
- **Die Wiederherstellung muss unter enormem Zeitdruck erfolgen:** Unternehmen müssen ihre Geschäftsabläufe schnell wiederherstellen – selbst wenn Umfang und Auswirkungen eines Angriffs noch nicht vollständig absehbar sind.

Resilienz ist heute kein ambitioniertes Ziel mehr, das nur besonders leistungsstarke Unternehmen anstreben. Sie ist zu einer unverzichtbaren Fähigkeit für jede Organisation geworden. Um mit der KI der nächsten Generation Schritt zu halten, benötigen Unternehmen eine Resilienz, die:

- **Kontinuierlich ist:** jederzeit getestet und einsatzbereit
- **Validiert ist:** auf vertrauenswürdigen, sauberen Daten basiert
- **Vereinheitlicht ist:** über Daten, Identitäten und Workloads hinweg

Ohne diese Fähigkeiten wird die Wiederherstellung unsicher – ausgebremst durch Komplexität, Risiken und mangelndes Vertrauen in das Ergebnis. Echte Cyberresilienz erfordert daher einen disziplinierten, operativen Ansatz, der sicherstellt, dass Wiederherstellung nicht nur möglich, sondern auch vertrauenswürdig ist.

Was Ist Echte Cyberresilienz?

Wenn Ihre Wiederherstell-ungsstrategie den heutigen Anforderungen nicht gerecht wird, ist sie keine echte Cyberresilienz.

KI erfordert einen neuen Ansatz – einen, der den Zustand Ihrer Daten kontinuierlich überwacht und sie bei Bedarf sofort wiederherstellen kann. Commvault Cloud ist die einzige einheitliche Plattform, die den Schutz von Cloud-, On-Premises- und SaaS-Workloads mit Identitätsschutz, Risikoanalysen und Cyber Recovery kombiniert. So trägt sie dazu bei, Cyberresilienz zu automatisieren und zu einem operativen Bestandteil Ihrer Sicherheitsstrategie zu machen.

So Sieht Echte Cyberresilienz Aus:

Echt Sauber

Wiederherstellungen, die keine zweite Wiederherstellung benötigen.

FRÜHER

Zurück zum Zustand vor dem Angriff – und damit alles verlieren, was danach entstanden ist.

HEUTE

Commvault Threat Scan unterstützt Sie dabei, kompromittierte Daten zu identifizieren und eine saubere Version Ihrer Dateien wiederherzustellen. So lässt sich das Risiko einer erneuten Infektion reduzieren.

Echt Vollständig

Sauber wiederherstellen. Schnell wiederherstellen. Mehr wiederherstellen.

FRÜHER

Ihre Daten sind wieder da – doch Anwendungen, Konfigurationen und Cloud-Infrastruktur müssen weiterhin von Grund auf neu aufgebaut werden. Datenwiederherstellung und Geschäftswiederherstellung sind nicht dasselbe.

HEUTE

Commvault unterstützt Sie dabei, Ihr Unternehmen über Workloads, Cloud-Umgebungen und Identitäten hinweg wiederherzustellen – mit einer einzigen Plattform, die für das Ausmaß heutiger Cyberangriffe entwickelt wurde.

Echt Schnell

**Kontinuierlich testen.
Mit Vertrauen wiederherstellen.**

FRÜHER

Jedes Unternehmen hat einen Wiederherstellungsplan … den niemand jemals testet. Damit gehen Sie genau im entscheidenden Moment ein Risiko ein.

HEUTE

Mit Commvault können Sie ganz einfach einen isolierten Cleanroom bei Bedarf bereitstellen, der Sie dabei unterstützt, Ihre Wiederherstellungsfähigkeit kontinuierlich zu validieren.

Commvault®

Von Wiederher-stellungsplänen Zu ResOps

(Resilience Operations)

Traditionelle Wiederherstellung konzentriert sich auf einzelne Vorfälle. Moderne Resilienz erfordert einen kontinuierlichen Ansatz, da KI der nächsten Generation das Tempo von Cyberbedrohungen weiter erhöht.

Resilience Operations (ResOps) umfassen:

01 **ERKENNEN**
Verschaffen Sie sich einen Überblick über Ihre kritischen Daten, Systeme und Identitäten.

02 **SCHÜTZEN**
Sichern und isolieren Sie Daten mit wirksamen Schutzmaßnahmen.

03 **ERKENNEN**
Identifizieren Sie Bedrohungen, Anomalien und kompromittierte Ressourcen.

04 **WIEDERHERSTELLEN**
Stellen Sie saubere Daten wieder her und bauen Sie Systeme neu auf.

05 **VALIDIEREN**
Testen Sie Ihre Wiederherstellungsbereitschaft kontinuierlich.

06 **OPTIMIEREN**
Verbessern Sie Prozesse auf Grundlage realer Erkenntnisse und Erfahrungen.

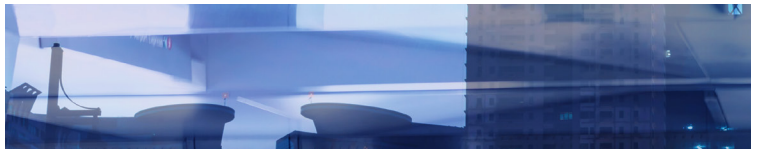
Dieser kontinuierliche Zyklus macht die Wiederherstellung von einem reaktiven Prozess zu einer proaktiven operativen Disziplin, die Unternehmen dabei unterstützt, ihre Cyberresilienz in einer sich schnell wandelnden Bedrohungslandschaft zu stärken.

Beginnen Sie Mit Der Wiederherstellung Durch Minimum Viability

In einem Modell echter Cyberresilienz beginnt die Wiederherstellung nicht mit allem – sie beginnt mit dem, was am wichtigsten ist. Minimum Viability ist ein grundlegendes Konzept der Cyberresilienz. Es priorisiert die Wiederherstellung der kritischsten Systeme, Daten und Prozesse, die erforderlich sind, um den Geschäftsbetrieb aufrechtzuerhalten.

Im Falle eines Angriffs hilft Ihnen Minimum Viability dabei:

- **Kritische Geschäftsprozesse zu priorisieren:** : Identifizieren Sie die Systeme und Daten, die für die Geschäftskontinuität unverzichtbar sind, damit sich die Wiederherstellung auf die Bereiche mit der größten geschäftlichen Wirkung konzentriert.
- **Vertrauenswürdige, saubere Daten wiederherzustellen:** Focus on recovering validated data to help reduce the risk of reinfection and avoid restoring compromised systems.
- **Den Geschäftsbetrieb unter Zeitdruck wieder aufzunehmen:** Bring key services back online quickly while broader recovery efforts continue in parallel.
- **Die Komplexität der Wiederherstellung zu reduzieren:** Begrenzen Sie den Umfang der ersten Wiederherstellungsphase, damit Teams schneller und fundierter Entscheidungen treffen können.



Minimum Viability ist nicht das Endziel der Wiederherstellung – sondern ihr Ausgangspunkt. Es bietet einen kontrollierten und praxisorientierten Ansatz, um den Geschäftsbetrieb wiederherzustellen und gleichzeitig das Vertrauen in Ihre Daten zu bewahren.

Erfahren Sie mehr über die einzelnen Schritte zur Wiederherstellung Ihres Geschäftsbetriebs und unsere bewährten Vorgehensweisen im Ultimativen Leitfaden Zur Minimalen Betriebsfähigkeit.

Wie Commvault Echte Cyberresilienz Ermöglicht

Commvault unterstützt Sie dabei, echte Cyberresilienz zu erreichen, indem Schutz, Wiederherstellung und Validierung in Ihrer gesamten IT-Umgebung zusammengeführt werden.

Commvault® Cloud

Commvault Cloud vereint Daten, Anwendungen und Infrastrukturen aus Cloud-, SaaS-, Hybrid- und On-Premises-Umgebungen auf einer einzigen Plattform. Dieser einheitliche Ansatz trägt dazu bei, Fragmentierung zu reduzieren und einen konsistenten Schutz sowie eine konsistente Wiederherstellung über Ihre gesamte Datenlandschaft hinweg zu ermöglichen.

Commvault Cloud Threat Scan

Die KI-gestützte Bedrohungserkennung hilft dabei, Anomalien zu identifizieren und potenziell kompromittierte Daten in Backup-Umgebungen zu erkennen. Dadurch lässt sich das Risiko einer erneuten Infektion während der Wiederherstellung reduzieren. Dank einer besseren Transparenz über Bedrohungen können Teams fundiertere Entscheidungen darüber treffen, welche Daten sicher wiederhergestellt werden können. Automatisierte Workflows koordinieren Reaktions- und Wiederherstellungsmaßnahmen über Systeme und Anwendungen hinweg, reduzieren den manuellen Aufwand und unterstützen Teams dabei, Wiederherstellungen effizienter durchzuführen.

Commvault Cleanroom™

Cleanroom stellt eine sichere, isolierte Umgebung bereit, in der Wiederherstellungsszenarien getestet, die Datenintegrität validiert und forensische Analysen durchgeführt werden können. Dadurch können Unternehmen ihre Wiederherstellungspläne kontinuierlich testen und das Vertrauen in die Ergebnisse unter realen Bedingungen stärken. Darüber hinaus kann Cleanroom dazu beitragen, **die Häufigkeit von Wiederherstellungstests um das 30-Fache zu erhöhen**.

Commvault Cloud Rewind™

Cloud Rewind unterstützt Unternehmen dabei, vertrauenswürdige, saubere Daten wiederherzustellen und Anwendungen nach einem Sicherheitsvorfall schnell neu aufzubauen. Durch die Orchestrierung von Wiederherstellungsprozessen trägt die Lösung dazu bei, Ausfallzeiten zu reduzieren und kritische Services schneller wieder bereitzustellen. Unternehmen haben bereits mehr als **800 Cloud-Ressourcen und über 200 TB Daten in weniger als 10 Stunden wiederhergestellt** – mit einer durchschnittlichen Wiederherstellungszeit von nur wenigen Minuten pro Objekt.

eBOOK

Testen Sie Ihre Resilienz, Bevor Es Ein Angreifer Tut

Cyberbedrohungen entwickeln sich kontinuierlich weiter. Wiederherstellung bedeutet heute weit mehr, als Systeme einfach wieder in Betrieb zu nehmen. Es geht darum, vertrauenswürdige Daten schnell und zuverlässig wiederherzustellen – selbst dann, wenn Backups und IT-Umgebungen kompromittiert wurden.

Die entscheidende Frage ist nicht, ob Sie sich erholen können.
Sondern ob Sie sauber, schnell und mit Vertrauen wiederherstellen können.

MACHEN SIE DEN RESILIENZTEST

commvault.com/de/cyber-resilience
commvault.com/minimum-viability/assessment

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

Commvault®