O'REILLY®
Report

# Cyber-Resilienz am Wendepunkt

## Eine neue Strategie, um gegenüber Bedrohungen durch agen5sche KI zu bestehen

**Govind Rangasamy**

Commvault®

# KI-BEDROHUNGEN NICHT NUR ÜBERSTEHEN, SONDERN GESTÄRKT DARAUS HERVORGEHEN.

Erfahren Sie, wie Sie sich mit Commvault nach einem Angriff schnell wieder erholen und dauerhaft handlungsfähig bleiben.

Besuchen Sie commvault.com

# Cyber-Resilienz am Wendepunkt

*Eine neue Strategie, um gegenüber Bedrohungen durch agentische KI zu bestehen*

*Govind Rangasamy*

O'REILLY®

**Cyber-Resilienz am Wendepunkt**
von Govind Rangasamy


Veröffentlicht von O'Reilly Media, Inc., 141 Stony Circle, Suite 195, Santa Rosa, CA 95401.

O'Reilly-Bücher können zu Bildungs-, Geschäfts- oder Verkaufszwecken erworben werden. Für die meisten Titel sind auch Online-Editionen erhältlich (*https://oreilly.com*). Weitere Informationen erhalten Sie von unserer Vertriebsabteilung für Unternehmen/Institutionen: 800-998-9938 oder corporate@oreilly.com.

**Akquisition:** Simina Calin
**Entwicklung:** Michele Cronin
**Produktion:** Jonathon Owen
**Korrektorat:** Paula L. Fleming

**Cover Design:** Susan Brown
**Cover-Illustration:** Ellie Volckhausen
**Buchgestaltung:** David Futato
**Buchillustration:** Kate Dullea

September 2025: Erste Ausgabe

**Revisionshistorie für die erste Ausgabe**
19.09.2025: Erste Ausgabe



Das Werk ist Teil einer Zusammenarbeit zwischen O'Reilly und Commvault. Siehe unsere Erklärung zur redaktionellen Unabhängigkeit.

979-8-341-65986-5

[LSI]

# Inhaltsverzeichnis

# Danksagung

Ich möchte Katherine Demacopoulos für ihr Engagement rund um dieses Buch danken sowie Anna Griffin, die den Bedarf für dieses Buch erkannt und es gesponsert hat. Danke auch an Chris DiRado für seine Sicherheitsexpertise und Unterstützung.

Ein Dankeschön an meine Frau Bhuvana und unsere wunderbaren Söhne Pranav und Sanjit. Ihr erinnert mich jeden Tag daran, was wirklich zählt. Eure Liebe, die Neugier, eure Späße und Umarmungen gaben mir die Motivation und Energie, weiterzumachen.

KAPITEL 1

# Ein Cyberangriff steht bevor. Wie verlässlich ist Ihre Recovery- Strategie?

Das Herzstück eines Unternehmens sind seine Netzwerke, Anwendungen und Datenspeicher. Diese überlebensnotwendigen Systeme sind angesichts immer häufiger auftretender und komplexer werdender Cyberangriffe zunehmend bedroht. Cyberkriminelle bedienen sich bereits modernster, KI-gestützter Tools, doch eine weitaus gefährlichere Bedrohung zeichnet sich ab. Agentische Künstliche Intelligenz (KI), die autonom denkt, plant und handelt, wird die Methoden der Cyberkriminalität revolutionieren und Angriffe skalierbarer und effizienter machen.

Im Gegensatz zu herkömmlicher Ransomware, die vorprogrammierten Skripten folgt, kann die agentische KI ihre Strategie in Echtzeit anpassen, aus Abwehrreaktionen lernen und Angriffe schneller weiterentwickeln, als menschliche Verteidiger reagieren können.

Prominente Vorfälle zeigen, dass keine Branche oder Region davor sicher ist. Beispiele reichen von der Vergiftung einer Wasseraufbereitungsanlage in Florida und der 11-tägigen Stilllegung der Colonial Pipeline bis hin zur Lahmlegung ganzer Schulbezirke durch Ransomware-Angriffe und der vollständigen Verschlüsselung von Hotel- und Casino-Systemen.

Selbst der beste Perimeterschutz und die modernsten Threat-Intelligence- Programme, wie das Financial Services Information Sharing and Analysis Center (FS-ISAC) und die US Cybersecurity & Infrastructure Security Agency (CISA), sind nur ein Baustein von vielen. Die Gegner von heute verfügen über umfangreiche Finanzmittel, sind außerordentlich geduldig und konzentrieren sich darauf, die Resilienzfähigkeit des Zielunternehmens auszuhebeln.

## Verstehen, wie moderne Cyberbedrohungen funktionieren: Die Industrialisierung der Cyberkriminalität

Noch vor wenigen Jahren wurden Ransomware-Angriffe größtenteils von einer Handvoll spezialisierter Hacker-Gruppen durchgeführt. Heute stehen für jeden einigermaßen geschickten Kriminellen im Dark Web Ransomware as a Service (RaaS)-Plattformen zur Verfügung. Das RaaS-Geschäftsmodell funktioniert wie herkömmliche SaaS-Plattformen (Software as a Service) und bietet Abonnements und Ertragsbeteiligungsregelungen, wodurch Cyberkriminalität für jeden Zahlungswilligen zugänglich wird.

Diese kriminellen Netzwerke bieten sofort nutzbaren Zugang zu professionellen Erpressungsmodellen, einschließlich Call-Centern zur Opferunterstützung, Verhandlungshilfe für Lösegelder und sogar „Garantien“ für die Löschung von Daten, wenn Opfer sich weigern zu zahlen. Dieser industrialisierte Ansatz hat zu einer Explosion von Angriffen geführt. Kriminelle müssen keine eigene Malware mehr entwickeln. Sie können einfach aus einem Menü wählen: LockBit, REvil, Darkside, Conti, BlackCat, und vielem mehr.

Jede Entwicklung bietet spezielle Funktionen, die maximalen Schaden anrichten und größtmöglichen Druck ausüben. Moderne Ransomware-Varianten exfiltrieren routinemäßig Daten vor der Verschlüsselung, um eine Veröffentlichung androhen zu können, zerstören gezielt und systematisch Sicherungssysteme, um Wiederherstellungsoptionen zu eliminieren, und stellen Payloads bereit, die ganze Netzwerke oder Cloud-Konten innerhalb von Minuten löschen können.

## KI-gesteuerte Ransomware: Wenn Angriffe denken, lernen und sich anpassen

Das Aufkommen agentischer KI markiert einen grundlegenden Wandel abseits herkömmlicher RaaS-Plattformen. Im Gegensatz zur generativen KI, die bei Aufgaben hilft, ist die agentische KI proaktiv und kann komplexe Probleme lösen sowie autonom Entscheidungen treffen. Diese KI-Agenten führen nicht einfach vorprogrammierte Angriffe durch. Sie lernen und passen ihre Strategien an die jeweilige Umgebung an.

In kontrollierten Tests haben Forscher der Unit 42 beispielsweise einen gesamten Angriff vom ersten Eindringen bis zur Daten-Exfiltration in nur 25 Minuten abgewickelt. Der Geschwindigkeitsunterschied ist gigantisch: Menschliche Angreifer brauchten im Durchschnitt zwei Tage, um die Daten zu exfiltrieren während KI-gestützte Angriffe dasselbe Ziel 100-mal schneller erreichten.

## Doppelte Erpressung etc.: Angriffe mit Tiefenwirkung

Moderivn|eInRhalntsvoemrzweicahrnei-sAngriffe umfassen oft zwei Phasen:

1. Die Exfiltration sensibler Daten.
2. Die Verschlüsselung wichtiger Systeme.

Selbst wenn ein Opfer über externe Backups in einer zweiten Cloud-Region verfügt, ist der Druck durch die Gefahr, dass sensible Daten veröffentlich werden könnten, enorm hoch. Ende 2024 waren durch das Datenleck bei LastPass die verschlüsselten Tresordaten von Millionen von Nutzern in Gefahr, und obwohl die Master-Passworte sicher waren, verursachte die Tatsache, dass ein Angreifer eine Kopie aller Tresore besaß, eine Vertrauenskrise.

Staatliche Akteure hingegen setzen Ransomware nicht aus Profit-, sondern aus strategischen Gründen ein, indem sie zum Beispiel die Kernprozesse von Pipelines, Versorgungsunternehmen, Gesundheitssystemen und Regierungsdiensten in großem Umfang lahmlegen, was sich direkt auf deren operative Technologie auswirkt.

Ein gutes Beispiel dafür ist der WannaCry Ransomware-Angriff von 2017. Er verursachte einen umfassenden Ausfall der Krankenhaussysteme des britischen National Health Service, was dazu führte, dass medizinische Eingriffe abgebrochen und Krankenwagen umgeleitet werden mussten. Dieser Angriff zeigt deutlich, wie Cyberangriffe Leben gefährden, wenn kritische Infrastrukturen ausfallen.

## Alles kann zum Angriffsziel werden

Die Demokratisierung agentischer KI durch leicht zugängliche Plattformen macht jede Illusion, dass bestimmte Branchen vor Angriffen sicher seien, zunichte. Agentische KI kann Angriffe planen und dann autonom durchführen, was sie skalierbarer und effizienter macht. Gleichzeitig sinkt dadurch die Einstiegshürde für Cyberkriminelle:

- *Bildungssektor:* Im Jahr 2022 hielt die Vice Society die Daten des Los Angeles Unified School District unter Verschluss, wovon 1.000 Schulen und 600.000 Schüler betroffen waren.

- *Energiesektor:* Im selben Jahr legte Ransomware die Petro-Card-Kartensysteme von Suncor Energy in Kanada lahm, wodurch viele Autofahrer an Tankstellen im ganzen Land strandeten.

- *Hotelerie:* Im Jahr 2024 griff BlackCat die MGM Resorts an und legte Spielautomaten sowie Reservierungssysteme in 30 Hotels lahm.

- *Handel und Dienstleistung:* Im April 2025 musste Marks & Spencer in Großbritannien die Geschäfte schließen, nachdem DragonForce seine Geschäftssysteme verschlüsselt hatte und Mailchimp sowie SendGrid wurden Opfer globaler Phishing-Kampagnen.

Die Moral der Geschichte ist klar: Unsere Gegner haben sowohl das Werkzeug als auch die Anreize, überall zuzuschlagen. Mit der Beschleu-nigung der digitalen Transformation und immer mehr vernetzten Geräten, Prozessen und Partnern, nimmt die Angriffsfläche zu. Die Zeiten, in denen die IT-Abteilung „kritische Systeme" hinter einer Festung aus Firewalls abschotten konnte, sind vorbei. Jeder Endpoint, jedes Cloud-Service und jede Drittanbieter-Integration ist ein potenzieller Einstiegspunkt.

Darüber hinaus kann der Mensch selbst, sei es durch einen überzeugenden KI- Deepfake-Anruf oder einen Mitarbeiter, der ein privates Gerät für die Arbeit verwendet, zu einem effektiven Einfallstor für Angreifer werden.

## Warum Unternehmen immer noch von Angriffen überrascht werden

Trotz zunehmender Belege für ein erhöhtes Cyberbedrohungs-Risiko, werden viele Unternehmen kalt erwischt. Diese anhaltende Schwäche beruht auf tief verwurzelten Denkweisen in Bezug auf die Cyber-Sicherheit, die nicht mehr der heutigen Realität entsprechen. Drei kritische Schwachstellen – eine rein präventionsorientierte Denkweise, isolierte Teams und Runbooks sowie der Glaube an die umfassende Sicherheit der Cloud – machen selbst gut geschützte Unternehmen verwundbar.

## Die rein präventionsorientierte Denkweise: Trügerische Sicherheitsebenen

In der Vergangenheit entwickelte sich die Cyber-Sicherheit in unterschiedlichen Wellen. Jedes Mal glaubten Cyber-Sicherheitsexperten, dass sie es endlich geschafft hätten, ihre Unternehmensdaten allumfassend zu schützen. Tabelle 1-1 stellt diese Entwicklung dar.

*Tabelle 1-1. Entwicklung der Cyber-Sicherheit in unterschiedlichen Wellen*

| Ära | Fokus | Falsches Versprechen | Realität |
|---|---|---|---|
| 1990er | Perimeter schutz | Firewalls und Border-Router sollten unbefugten Zugriff verhindern. | Angriffe umgingen Firewalls mittels Phishing, Social Engineering und Insidern. |
| 2005+ | E-Mail-Sicherheit | Scans sollten schädliche Nachrichten eliminieren. | Malware versteckte sich in legitimen Datenströmen und Anhängen |
| 2005+ | Netzwerk-sicherheit | Durch Überwachung sollten Anomalien erkannt werden. | Komplexe Bedrohungen schienen harmlos, bis sie |
| 2010+ | End-point-Schutz | Antivirus-Programme sollten die Ausführung blockieren. | Sicherheitsverletzungen auslösten. |
| 2015+ | Identitäts-sicherheit | Zero Trust sollte nur authentifizierten Zugriff zulassen | Dateilose Malware und Zero-Day-Exploits umgingen die Signaturerkennung. Gestohlene Token, API-Schlüssel und falsch konfigurierte Berechtigungen führten zu Lücken. |
| 2020+ | Cloud-security | Anbieter sollten sich um die Sicherheit kümmern. | Angriffe zielten auf falsch konfigurierte Cloud-Berechtigungen und Container-Registries ab |

Trotz der zunehmenden Flut an Cyberbedrohungen bleiben viele Unternehmen in der Präventions-Mentalität verankert. Sie investieren in Firewalls der nächsten Generation, EDR (Endpoint Detection and Response), SIEM-Plattformen (Security Information and Event Management), Threat Feeds und Red-Team-Übungen, nur um festzustellen, dass diese Steuerelemente zwar notwendig, aber nicht ausreichend sind.

Sobald ein Angreifer Fuß fasst, sei es durch den Diebstahl von Anmeldedaten, die Anwendung von Zero-Day-Exploits, Phishing oder die Kompromittierung der Lieferkette, beginnt der Perimeterschutz zu bröckeln. Abbildung 1-1 illustriert die mehrschichtige Abwehrstrategie, auf die die Cybersecurity-Branche vertraut.

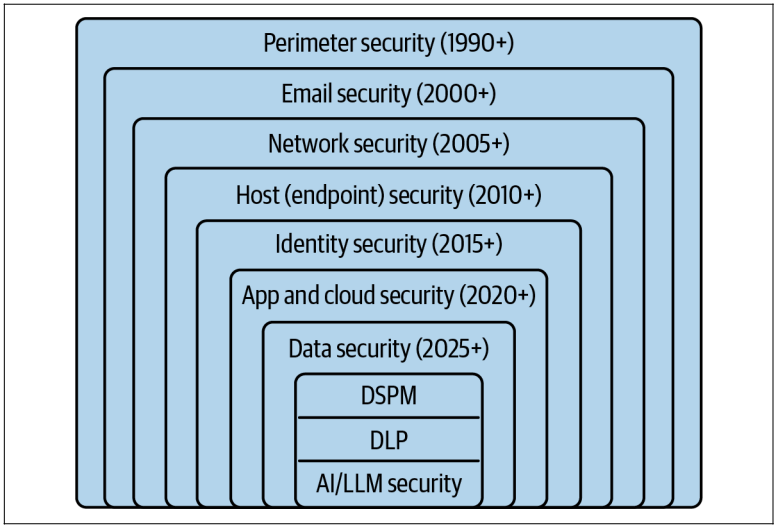


*Abbildung 1-1. Die mehrschichtige Abwehrstrategie der Cybersecurity-Branche*

Das wirft ein Paradoxon auf: Konzentriert man sich zu sehr auf die Prävention, investiert man zu wenig in die Wiederherstellung und insbesondere in Wiederherstellungstests. Backups werden als etwas behandelt, das es zu erfüllen gilt, und nicht als strategische Ressource, und Cyber-Recovery-Tests - sofern sie überhaupt durchgeführt werden – werden wie eine jährliche Disaster Recovery (DR)-Übung gehandhabt.

Im Ernstfall greift man hastig auf provisorische Runbooks zurück, nur um festzustellen, dass sie veraltet, unvollständig, ungetestet und für die heutigen dynamischen Umgebungen nicht zu gebrauchen sind.

## Isolierte Teams und Runbooks

Die Teams für Cybersicherheit, Cloud-Operation, Anwendungsentwicklung, Unternehmensarchitektur und Business Continuity arbeiten oft getrennt voneinander und haben eigene Prozesse, Tools und Prioritäten.

Das Resultat? Richtlinien und Runbooks füllen PowerPoint-Präsenta-tionen, Word-Dokumente und Ticketsysteme und werden im Notfall selten bis gar nicht verwendet. Verbindungen und Abhängigkeiten zwischen Anwendungen, Netzwerkkonfigurationen, Identitätssystemen, GitHub-Repositories, Container Registries, Datenbankservern und Daten-sicherungskopien werden selten dokumentiert.

Der erste Rebuild-Versuch ist der schlechteste Zeitpunkt, um fehlende Komponenten zu entdecken.

## Cloud Resilienz als Illusion

Viele CIOs, CTOs und CISOs glaubten, dass der Umstieg auf die Cloud unter dem Vorwand der digitalen Transformation das Wiederherstellungsproblem für die Unternehmen auf magische Weise lösen würde. Hyperscale-Anbieter werben für Multi-Zonen- und -Regionen-Lösungen, Snapshots, replizierte Kopien und native Backup-Tools, die eine drastische Verkürzung der Wiederherstellungszeiten versprechen. Um eine gute Resilienz zu erreichen, müssen Teams oft über ein Dutzend Tools und Services kombinieren.

Eine Skalierung verstärkt das Problem. Unternehmen verfolgen ihre Backup- Strategie nicht über alle Cloud-Konten hinweg. Der „Shift Left"-Ansatz, der Entwicklern eine größere operative Verantwortung überträgt, hat wohl mehr Risiken verursacht als verhindert.

Hyperscale-Anbieter veröffentlichen immer mehr Dienste und Tools, um das Self-Service-Modell zu vereinfachen. Doch gerade dieses Modell hat zu fehlerhaften Prozessen geführt, wodurch Unternehmen letztlich einem noch größeren Risiko ausgesetzt sind.

Diese Schwächen zeigen sich, wenn es ernst wird. Kürzlich versuchte ein Finanzdienstleistungsunternehmen nach einem simulierten Verstoß ein Failover in eine zweite Region durchzuführen, stellte jedoch fest, dass die Datenverschlüsselungscodes und Identitätsrollen nicht repliziert worden waren. Das Skript „Region-Failover" schlug fehl und ließ den Recovery-Standort in einem unbrauchbaren Zustand zurück.

Die Cloud allein ist kein Allheilmittel. Sie erfordert vollständig getestete Rebuilds in der gesamten Anwendungsumgebung, um sicherzustellen, dass jede Konfiguration, alle Zugangsdaten und jedes Objekt vorhanden sind.

### Resilienz funktioniert nicht ohne Wiederherstellung

Es ist harte Realität, dass die meisten Unternehmen ihre gesamte Cyber-Sicherheitsstrategie auf einer gefährlichen Illusion aufgebaut haben: Dass sie jeden Angriff verhindern können. Diese präventionsorientierte Denkweise erzeugt ein falsches Sicherheitsgefühl, das in dem Moment zusammenbricht, in dem ein Angreifer den Perimeter durchdringt.

Ohne die nachgewiesene Fähigkeit einer schnellen und vollständigen Wiederherstellung sind selbst die komplexesten Abwehrmaßnahmen sinnlos. Denn bei Resilienz geht es nicht darum, Ausfälle zu vermeiden, sondern darum, sich wieder davon zu erholen.

### Resilienz heißt „Vertrauen aufbauen"

Wenn Resilienz etwas bedeutet, dann Vertrauen. Vertrauen darauf, dass Sie die Lichter wieder einschalten können, wenn sie ausgehen. Bei Cyber-Resilienz geht es weder um das Vorhandensein von Firewalls noch um Patch-Frequenzen. Sie beschreibt die Fähigkeit, geschäftskritische Anwendungsservices (z. B. Kundenportale, Zahlungssysteme, Produktionslinien oder elektronische Patientenakten) innerhalb von Minuten oder Stunden, statt Tagen oder Wochen wiederherzustellen.

*Für die Devise „Ein Rebuild ist unverzichtbar" braucht es drei fundamentale Veränderungen:*

• *Vom Backup zum vollständigen Rebuild der Anwendungsumgebung: Der Fokus muss sich über das Erstellen von Dateikopien und Block-Snapshots hinaus auf die Möglichkeit verlagern, jede Anwendungskomponente (d. h. Netzwerk, Rechenleistung, Speicher, Identität und insbesondere deren Abhängigkeiten) neu aufbauen zu können, um alle wichtigen Dienste wieder zum Laufen zu bringen.*

• *Von gelegentlichen DR-Übungen hin zu regelmäßigen Wiederherstellungstests: Anstatt einmal pro Jahr Failover-Übungen durchzuführen, müssen Teams monatlich automatisierte „Rebuild-Übungen" in von der Produktion isolierten Cloud-Konten durchführen.*

• *Von isolierten Playbooks hin zu funktionsübergreifender Recovery as Code (RaC): Sicherheits-, Cloud-, Architektur-, Entwicklungs- und DR-Teams müssen gemeinsam Runbooks erstellen, die als Code versioniert und zusammen getestet werden.*

*Wie wäre es, wenn RaC automatisch erstellt und regelmäßig aktualisiert werden könnte?*

## Der Preis der Selbstzufriedenheit

Wenn ein Ausfall von Minuten ein Unternehmen Tausende Euros kostet, ist es ernüchternd zu erkennen, was ein ganzer Tag offline wirklich bedeutet. Schon ein einziger Tag kann verheerende Folgen haben: Millionen an entgangenen Einnahmen, erdrückende Geldstrafen und schwere (oft irreparable) Reputationsschäden.

Einzelhändler müssen schließen und können nichts verkaufen, Produzenten sind eingeschränkt und können nichts versenden, Krankenhäuser sind lahmgelegt und können nicht auf wichtige Patientenakten zugreifen. Jede verlorene Minute bedeutet einen wütenden Kunden, einen im Stich gelassenen Partner und eine schwer beschädigte Marke.

Im Gegensatz dazu berichten Unternehmen, die konsistente Rebuild-Strategien anwenden, von einer Verkürzung der durchschnittlichen Wiederherstellungszeit von 48 Stunden (ca. 2 Tage) auf weniger als 2 Stunden und davon, dass selbst die ausgeklügeltsten Angriffe sie nicht dauerhaft außer Gefecht setzen können.

Und der zusätzliche Nutzen eines Rebuild: sie sparen nicht nur Geld, sondern sichern sich auch Vertrauen. Im nächsten Kapitel geht es um die Entwicklung einer Rebuild-Funktion. erholen.

KAPITEL 2

# Der Anschein von Sicherheit: Warum herkömmliche Recovery-Methoden fehlschlagen und warum das NIST Cybersecurity Framework auf Rebuild setzen muss

*Du kannst einen Waldbrand nicht mit einer Tasse Wasser löschen.*
— in Anlehnung an eine Feuerwehr-Weisheit

Im späten 19. Jahrhundert bauten Ingenieure hohe Deiche zwischen Grenzstädten und dem Mississippi, zuversichtlich, dass die schiere Größe jede Überschwemmung verhindern würde. Familien picknickten auf deren Böschungen und glaubten, dass der Kampf gegen das Wasser gewonnen sei. Doch als das Frühlingstauwetter noch nie dagewesene Sturzfluten entfesselte, zersprangen die Deiche wie Eierschalen, und die Wasserfluten überschwemmten die Stadt.

Was lernen wir von diesen zerstörten Bauwerken: Keine Schutzmaßnahme, so großartig sie auch sein mag, ist unüberwindbar, wenn sie auf fehlerhaften Annahmen beruht.

Die digitale Infrastruktur von heute steht vor einer ähnlichen Krise der falschen Sicherheit. Die Cybersecurity- und Backup-Industrie hat ihre eigenen Deiche gebaut und ist von der Zweckdienlichkeit ihrer Lösung überzeugt:

- Die Cybersecurity-Branche errichtet Barrieren: Perimeter, Firewalls, Endpoint-Schutz, Cloud-Sicherheit und Identitäts-Frameworks.
- Die Backup-Branche konzentriert sich auf Datentresore, Bandarchive, Snapshots und Replikationsstrategien.

Doch prominente Sicherheitsverletzungen und Ransomware-Vorfälle haben diese Illusion zerstört. Egal, wie hoch die Mauern, Angreifer werden ein Schlupfloch finden. Auch traditionelle Backup-Methoden erweisen sich als äußerst unzureichend, wenn es darum geht, vollständig kompromittierte Ökosysteme nach modernen Ransomware-Angriffen wiederherzustellen. In diesem Kapitel wird erläutert, warum herkömmliche Backup-Ansätze nicht ausreichen und warum eine Rebuild-Funktion die Wiederherstellungsergebnisse erheblich verbessern kann.

# Die trügerische Sicherheit von Backups und Datenschutz

Seit über 50 Jahren glauben wir, dass der Schutz von Daten ausreichen würde. Bei Datenschutzsystemen wurde der Fokus auf eine kostengünstige, langfristige Aufbewahrung gelegt, nicht auf den Schutz des gesamten Anwendungs-Ökosystems. Wenn Unternehmen daher nach einem Ransomware-Ereignis eine Wiederherstellung versuchen, entdecken sie häufig unzählige kritische Fehler, die ihre Backups nahezu nutzlos machen.

So werden Dateien beispielsweise in Bandtresoren gesichert, die Wiederherstellung von Servern dauert jedoch Tage. Festplattenbasierte Sicherungen beschleunigen das Ganze, befinden sich jedoch in anfälligen Netzwerken. Disaster Recovery-Standorte versprechen ein nahtloses Failover, schlagen jedoch aufgrund von veralteten Verfahren, Konfigurationsabweichungen und Wissenslücken ständig fehl.

Der grundlegende Fehler liegt nicht im Datenschutz an sich, sondern in der Illusion, dass das Sichern von Daten der Möglichkeit entsprechen würde, funktionierende Systeme wiederherzustellen. Echte Wiederherstellung erfordert nicht nur die Offline-Sicherung von Daten, sondern auch umfassende Systemwiederherstellungsfunktionen, die die meisten Sicherungsstrategien nicht bieten.

## Moderne Ransomware: Das Ende von „Backup and Restore“

Ransomware-Angriffe stoßen nicht zufällig auf Backups, sondern suchen gezielt danach, um sicherzustellen, dass Ihr Plan B schon vor Beginn der 2. Phase unbrauchbar ist.

Sobald die Angreifer sich Domain-Administratorrechte gesichert haben, zerstören sie systematisch die Wiederherstellungsfunktionen des Unter- nehmens, indem sie Snapshots deaktivieren oder löschen, die Aufbewahrungsrichtlinien für Backups manipulieren und scheinbar unveränderliche Tresore beschädigen. Sie unterwandern sogar die Orchestrierungsebenen, die diese Systeme verwalten, und verwandeln jeden potenziellen Wiederherstellungspfad in eine Sackgasse.

Doch die Bedrohung geht über die einfache Zerstörung hinaus. Angreifergruppen, die auf doppelte Erpressung setzen, haben einen strategische Vorgehensweise perfektioniert: Sie stehlen zuerst sensible Daten, um mit deren Veröffentlichung drohen zu können, und verschlüsseln dann alles Übrige, um den Betrieb lahmzulegen. Dieser zweigleisige Angriff maximiert die Hebelwirkung, da Unternehmen sowohl mit Betriebsstillständen als auch mit dem Verlust der Reputation konfrontiert sind.

## Das Trugbild der unveränderlichen Speicher

Ein unveränderlicher Speicher ist so konzipiert, dass Snapshots nach dem Schreiben nicht mehr geändert werden können. Doch Angreifer haben raffinierte Gegenstrategien entwickelt, die die Grenzen der Technologie aufzeigen. Cyberkriminelle dringen in die Verwaltungs- oder Kontroll-ebene ein und ändern vor dem Fertigstellen der Snapshots die Richtlinien und Einstellungen zur Unveränderlichkeit, wodurch der Schutz ausgeschaltet wird, bevor er in Kraft treten kann. Außerdem nutzen sie Sicherheitslücken in der Konfiguration dazu, sich selbst die Befugnis zu erteilen, Archive zu löschen oder erneut zu verschlüsseln, wodurch sie die unternehmenseigenen Sicherheitsmaßnahmen gegen das Unternehmen selbst richten.

Selbst wenn die Tresore technisch gesehen sicher bleiben, ist ihr Schutzbereich stark eingeschränkt. Sie schützen zwar die Daten, doch Netzwerkkonfigurationen, Microservices-Meshes und Identitäts-Hierarchien sind einem Angriff schutzlos ausgesetzt.

## Datensicherheitstools: Hilfreich, aber unvollständig

Die jüngsten Fortschritte im Sicherheitsbereich haben ausgeklügelte Tools wie Data Security Posture Management (DSPM) für umfassende Datentransparenz, Data Loss Prevention (DLP) zur Überwachung der Datenbewegung und KI- gestützte Sicherheitstools gebracht, die eine intelligente Erkennung und Reaktion auf Bedrohungen ermöglichen.

Diese Technologien stellen zwar einen bedeutenden Fortschritt im Bereich der Cybersecurity dar, konzentrieren sich jedoch in erster Linie auf Prävention und Erkennung und nicht auf umfassende Wiederherstellung. Das macht Unternehmen anfällig, wenn es Angreifern gelingt, ihre Abwehrmaßnahmen zu durchbrechen.

### Der verführerische Ruf der Cloud Recovery und ihre verborgenen Schwächen

Anbieter von Hyperscale-Cloud-Lösungen versicherten unbegrenzte Kapazität, sofortige, regional replizierte Snapshots und Self-Service-Disaster-Recovery. Viele Unternehmen, denen man versprach, dass ihre Daten dadurch sicherer seien, migrierten innerhalb weniger Wochen mehrere Terabytes. Diese Versprechen verschleierten jedoch grundlegende Lücken, die sich erst dann bemerkbar machten, als Unternehmen ihre Wiederherstellungsfähigkeiten am dringendsten benötigten.

## Mehr als ein herkömmliches Backup

Herkömmliche Methoden können die komplexen Abhängigkeiten, die Cloud- Services beinhalten, nicht erfassen; die unvermeidlichen Konfigurationsabweichungen, die in Netzwerk- und Identitäts-Domänen auftreten, und die Malware oder die Fehlkonfigurationen, die sich in Containern, serverlosen Funktionen oder Anwendungsbibliotheken verstecken. Ohne „Goldene Kopien“ (vollständig gescannte, saubere, Multi-Komponenten-, Point- in-Time Anwendungs- und Datenkopien) entbehren Wiederherstellungen jeder Grundlage.

Den alten „Hoffentlich funktioniert das Backup“-Ansatz zu verfolgen, ist genauso riskant wie auf einen einzigen, ungetesteten Fallschirm zu setzen.

### Das fehlende Element: Regelmäßige, umfassende Rebuild- Tests

Anbieter von Hyperscale-Cloud-Lösungen versicherten unbegrenzte Sowohl eine Abwehrmaßnahmenbasierte Cybersecurity als auch herkömmliche Backup-Strategien sind im Grunde genommen unvollständig. Die Lösung besteht in regelmäßigen, praxisnahen Tests aller Wiederherstellungsfunktionen.

*Rebuild-Tests* stellen einen Paradigmenwechsel dar, von der Hoffnung auf funktionierende Backups, hin zu Tests auf ihre Effektivität inklusive einer umfassenden Validierung. Dieser Ansatz rekonstruiert die gesamte digitale Umgebung genau so, wie sie zu einem bekannten bereinigten Zeitpunkt existierte, und liefert einen ganzheitlichen Wiederaufbau der Umgebung, der weit über eine einfache Datenwiederherstellung hinausgeht.

Der Prozess umfasst das „Zurückdrehen" aller Infrastrukturebenen des Unternehmens – nicht nur der Daten, sondern auch der Netzwerkkonfigurationen, Rechenressourcen, Identitäts-Frameworks, Container, serverlosen Konfigurationen, und API-Gateways, damit die wiederher-gestellte Umgebung exakt wie das Original aussieht.

Besonders wichtig ist, dass Rebuild-Tests umfassende Scans auf Malware, Sicherheitslücken, Konfigurationsabweichungen und unbefugte Änderungen umfassen, die möglicherweise vor der Erstellung des Snapshots in die Umgebung gelangt sind.

Dieser Validierungsschritt verwandelt die Wiederherstellung von Backups von einem Sprung ins Unbekannte in einen verifizierten, sicheren Wiederherstellungsprozess, auf den Unternehmen vertrauen können, wenn ihr Überleben davon abhängt.

## Die Schwachstelle des NIST Cybersecurity Frameworks

Das Cybersecurity Framework des National Institute of Standards and Technology (NIST) gliedert sich in sechs Kernfunktionen: Identifizieren, Schützen, Erkennen, Reagieren, Wiederherstellen und Steuern. Seine Wiederherstellungsfunktion wird jedoch missverstanden und schafft eine bedrohliche Schwachstelle, die Unternehmen angreifbar macht, auch wenn sie glauben, dass sie geschützt sind.

### Wiederherstellen versus Neu Aufbauen: Zwei unterschiedliche Funktionen

Die Wiederherstellungsfunktion des NIST konzentriert sich auf eine Wiederherstellung, die die Systeme nach einem Vorfall wieder in einen betriebsbereiten Zustand bringt. Bei diesem Ansatz wird die Wiederherstellung als Schadensbegrenzung behandelt, wobei es vor allem um die Geschwindigkeit und nicht um die Validierung geht. Unternehmen nutzen Backups für die Wiederherstellung, führen DR-Skripte aus und feiern, wenn Anwendungen scheinbar wieder funktionieren, oft ohne die Unversehrtheit oder Vollständigkeit des Wiederhergestellten zu überprüfen.

Im Gegensatz dazu stellt der Rebuild einen Paradigmenwechsel hin zu einem sicheren Wiederaufbau dar. Anstatt verlorene Elemente wiederherzustellen, dient die Rebuild-Funktion dazu, aus zweifelsfrei funktionierenden Komponenten eine verifizierte, saubere Anwendungs-umgebung zu erstellen. Es ist wie der Gegensatz zwischen dem Ausbessern einer beschädigten Wand und dem Bau einer neuen Wand ausgehend von vertrauenswürdigen Bauplänen. Beide Wände erscheinen vielleicht funktionstüchtig, aber nur eine kann die Systemintegrität erhalten.

### Wo die Wiederherstellung zu kurz greift

In der Praxis besteht die Wiederherstellung oft nur aus einer Reihe von oberflächlichen Compliance-Maßnahmen, die eine minimale Sicherheit für die tatsächliche Wiederherstellungsfähigkeit bieten. Unternehmen führen jährlich theoretische DR-Übungen durch, bei denen man Verfahren auf dem Papier testet, aber nie die tatsächliche Systemwiederherstellung validiert wird. Sie führen sporadische Datenbankwiederherstellungen durch und testen regelmäßig Virtual Machine (VM) Spins, die nur Fragmente ihrer Infrastruktur umfassen, während sie die komplexen Abhängigkeiten, die moderne Anwendungen erfordern, ignorieren.

Leider führen Unternehmen nur selten vollständige Anwendungswiederherstellungen mit regelmäßiger Validierung durch, um zu überprüfen, ob alle Komponenten mit den Snapshot-Daten übereinstimmen und als Gesamtsystem funktionieren.

Tabelle 2-1 zeigt, wo das derzeitige NIST Framework hinter den modernen Anforderungen zurückbleibt, und wie Rebuild-Funktionen diese gefährlichen Lücken beheben.

Indem wir mit „Rebuild“ eine weitere Säule hinzufügen– eine lebendige Erweiterung der Wiederherstellungs-Funktion – schwören wir die Verteidiger auf eine deutlich strengere Überprüfung der Cyber-Resilienz ein: Die Möglichkeit, zu einem bestimmten Zeitpunkt zurückzukehren, eine sichere goldene Kopie auszuwählen und bei Bedarf die Anwendung von der Netzwerk- bis zur Datenebene neu aufzubauen.

*Tabelle 2-1. Lücken im derzeitigen NIST-Framework und wie die Rebuild-Funktion diese Lücke schließt*

| Funktion | Traditionelle Stärke | Aktuelle Lücke | Wie Rebuild die Lücke schließt |
|---|---|---|---|
| Identifizieren | Asset- Listen, BIAs | Keine verlässliche Wiederherstellu ngssicherheit | Historisches Archiv mit „goldenen Kopien“ |
| Schützen | Identitäts- und Zugriffsmanage- ment (IAM), Verschlüsselung, Firewalls | Zero-Day- oder Insiderangriffe können nicht gestoppt werden | Unveränderliche Snapshots für Rebuild-Artefakte |
| Erkennen | SIEM-, XDR-, UEBA | Alarm-bereitschaft ≠ Wieder- herstellung | Automatisierte Rebuild- Tests, die durch Ereignisströme ausgelöst werden |
| Reagieren | IR-Playbooks, Quarantäne | Playbooks validieren nur selten die vollständige Wiederherstellung | Der integrierte Rebuild wird als Teil der Reaktion ausgeführt |
| Wiederherstellen | Backup- und Failover-Skripte | Teilweise, manuelle Wiederherstellun g; nicht getestete Runbooks | Code-basierte Orchestrierung eines Rebuilds für die komplette Umgebung |
| Neu Aufbauen (Rebuild) | | | Regelmäßige, automatisierte zeitpunktgenaue Rebuild-Übungen |

## Das erweiterte Framework

Zur Sicherung der Resilienz müssen wir die Rebuild-Funktion in das NIST- Framework aufnehmen. Die Wiederherstellungs-Funktion bleibt der Grundsatz, der Plan und das Notfall-Szenario – der strategische Rahmen, der definiert, was im Fall einer Katastrophe geschehen soll. Die Rebuild-Funktion ist der lebendige Motor, der die Wiederherstellung zu einer gesicherten Realität und nicht zu einer theoretischen Möglichkeit macht, wie in Abbildung 2-1 dargestellt.

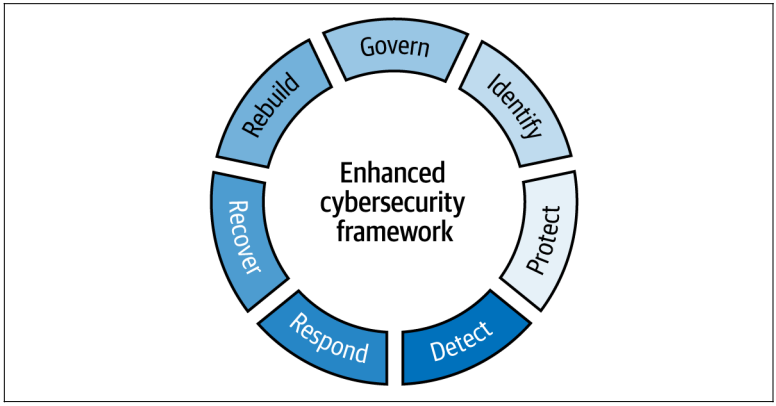


*Abbildung 2-1. Das NIST-Framework mit der zusätzlichen Funktion „Neu Aufbauen" (Rebuild)*

Die Rebuild-Funktion umfasst eine Reihe von Elementen:

*Zeitpunktgenaue Infrastrukturwiederherstellung*
: Dabei werden umfassende Point-in-Time-Snapshots der Infrastrukturkomponenten erfasst, einschließlich Netzwerkkonfigurationen, Rechenressourcen, Anwendungs-Images und deren Abhängigkeiten. Im Gegensatz zu herkömmlichen Backups, die sich auf Daten konzentrieren, sind diese Snapshots so konzipiert, dass sie den Infrastrukturkontext, den Anwendungen benötigen, um ordnungsgemäß zu funktionieren, neu erstellen können.

*Goldene Kopien*
: Dabei handelt es sich um zeitpunktgenaue Images, die einem umfassenden Scan auf Malware, Fehlkonfigurationen und Sicherheitslücken unterzogen wurden und somit validierte, saubere Wiederherstellungspunkte bieten. Es geht hier nicht nur um Datenkopien, sondern um verifizierte, saubere Snapshots ganzer Anwendungs-Stacks, denen man bedingungslos vertrauen kann. So muss man nicht befürchten, dass durch die Wiederherstellung die Probleme, die man hinter sich lassen möchte, erneut entstehen.

*Wiederherstellung als Code (Recovery as Code)*
: RaC wandelt Ad-hoc-Wiederherstellungsverfahren in automatisierte, versionierte und wiederholbare Prozesse um. Anstatt sich auf veraltete Runbooks zu verlassen, behandelt RaC

Rebuild-Verfahren als lebendige Software, die sich mit Ihrer Infrastruktur weiterentwickelt, sodass sich die Wiederherstellungsfunktionen im Laufe der Zeit verbessern, anstatt sich durch Nichtanwendung zu verschlechtern.

Der Rebuild verwandelt „Hoffentlich funktioniert das Backup“ in „Ich weiß, dass dieser Rebuild klappt“. Das liegt daran, dass er getestet und weiterentwickelt wurde und dutzende Male bewiesen hat, dass er funktioniert, bevor Sie ihn tatsächlich benötigen.

KAPITEL 3

# Die Rebuild-Vorteile nutzen: Unerwartete Szenarien in der Cloud testen

Im frühen 20. Jahrhundert verbesserte sich die Fahrzeugsicherheit enorm, nicht nur, weil die Autos stabiler wurden, sondern weil Crashtests ein zentraler Punkt bei der Fahrzeugentwicklung waren und Sicherheit von bloßer Hoffnung in ein gesichertes Ergebnis verwandelten. Ähnlich glaubten die Piloten in den Anfängen der Luftfahrt, dass stärkere Flugzeuge weniger Probleme beim Fliegen bedeuteten.

Doch wenn es in der Luft zu einem Notfall kam, war es nicht allein die Stärke des Flugzeugs, die Leben rettete, sondern vielmehr die Fähigkeit des Piloten, sich von unerwarteten Ereignissen nicht aus der Bahn werfen zu lassen. Egal, wie gut das Flugzeug konstruiert war, das Überleben hing oft von intensiven Schulungen ab, bei denen jeder denkbare Notfall simuliert wurde.

Heute steht die digitale Resilienz vor einer ähnlichen Transformation. Unternehmen dürfen nicht mehr davon ausgehen, dass Backups und Cybersecurity-Maßnahmen funktionieren. Was fehlt, ist das vielleicht wichtigste Element überhaupt: regelmäßige Tests. Kontinuierliches Testen ermöglicht es Unternehmen, ihre digitalen Umgebungen nach Totalausfällen zuverlässig wieder aufzubauen. In diesem Kapitel wird erläutert, wie Unternehmen regelmäßige Rebuild-Tests implementieren können.

## Wahre Geschichten über nicht funktionierende Backups und fehlgeschlagene Wiederherstellungspläne

Jüngste Vorfälle zeigen, wie anfällig unsere digitalen Ökosysteme, trotz beträchtlicher Investitionen der Unternehmen in Cybersecurity und Daten- Backups, sind. Umfang und Intensität von Ransomware-Angriffen haben in den letzten Jahren dramatisch zugenommen. Das zeigt, dass selbst umfassende Disaster Recovery-Pläne fehlschlagen, wenn sie nicht mit realen Szenarien moderner Cyberbedrohungen getestet wurden.

Viele große Unternehmen haben in den letzten Jahren sehr gelitten, wenn ihre Wiederherstellungspläne trotz sorgfältiger Dokumentation und erheblicher Investitionen spektakulär fehlschlugen.

*MGM Resorts und Caesars Entertainment*
: Diese Unternehmen sahen sich Ende 2023 zermürbenden Angriffen ausgesetzt, die zu umfangreichen Ausfällen führten. Trotz ihrer umfassenden DR-Pläne hatten beide Unternehmen Schwierigkeiten, wichtige Geschäftsfunktionen rasch wiederherzustellen. Es gab eine solide Dokumentation, aber die tatsächliche Wiederherstellung scheiterte aufgrund nicht getesteter Abhängigkeiten, veralteter Konfigurationen und fehlender Integrationen zwischen Daten- Backups und der Wiederherstellung von Anwendungen.

*National Health Service (NHS), London, Großbritannien*
: Ein Angriff mit der Qilin Ransomware im Jahr 2024 offenbarte die harte Wahrheit: Fast eine Million Patientendatensätze und kritische Gesundheitsdatensysteme wurden trotz zuverlässiger Backups kompromittiert. Das NHS musste auf die harte Tour lernen, dass die Wiederherstellung von Datenbanken allein nicht ausreichte; ohne verifizierte Wiederherstellungsverfahren für Anwendungen, Identitäten und Netzwerkarchitekturen erwiesen sich die Backups als nutzlos.

*AWS S3-Bucketangriffe*
: In diesem ernüchternden Szenario von 2025 nahm die Codefinger Ransomware die Cloud-Speicher-Buckets des Unternehmens ins Visier und ließ herkömmliche Cloud-Backup-Strategien ins Leere laufen. Viele Unternehmen mussten trotz regelmäßiger

Cloud-Backups feststellen, dass diese von der Ransomware verschlüsselt und nicht mehr zugänglich waren. Solche Vorfälle verdeutlichen die Notwendigkeit eines völlig neuen Testansatzes für Wiederherstellungsverfahren.

Diese Geschichten offenbaren eine beunruhigende Realität: Unsere bisherigen Annahmen in Bezug auf Datenschutz und Cybersecurity greifen zu kurz. Der exponentielle Anstieg modernster Ransomware-Angriffe in Verbindung mit immer häufiger auftretenden Ausfällen von Cloud-Regionen macht einen neuen Ansatz für digitale Resilienz notwendig: regelmäßige, umfassende und gründliche Rebuild-Tests der gesamten Umgebung.

# Wiederherstellung neu gedacht: Die moderne Herausforderung von Cloud-Rebuilds

Der Neuaufbau von Cloud-Umgebungen erfordert viel mehr als nur die Wiederherstellung von Daten aus Backups. Moderne Anwendungen arbeiten in hochdynamischen Ökosystemen, die aus zahlreichen Cloud-nativen Services bestehen, welche sich über mehrere, parallellaufende DevOps-Pipelines fortlaufend ändern. Diese Pipelines sind zunehmend KI-gesteuert.

## Verborgene Abhängigkeiten und Konfigurationsabweichungen

Jede DevOps-Pipeline kann unabhängig Konfigurationen aktualisieren, Microservices bereitstellen und Sicherheitsrichtlinien anpassen, was das Risiko von Konfigurationsabweichungen und der Verschleierung kritischer Abhängigkeiten erhöht. Teams, die Tools zur koninuierlichen Integration und Bereitstellung (CI/CD) wie AWS CodeDeploy CodePipeline und CodeBuild verwenden, ändern Umgebungen häufig, ohne die Auswirkungen ihrer Änderungen klar im Blick zu haben. So schaffen sie oft verborgene Schwachstellen oder unbemerkte Abhängigkeiten, was im Notfall einen vollständigen und akkuraten Neuaufbau erschwert.

## Die Strategie der Mindestbetriebsfähigkeit: Rebuild möglich machen

Die meisten Unternehmen müssen sich in der Praxis der Realität stellen, dass ein gleichzeitiger Wiederaufbau der gesamten Umgebung

weder praktikabel noch notwendig ist. Hier wird das Konzept der Mindest-betriebsfähigkeit (oder der „Minimal Viable Company“) zur strategischen Brücke zwischen theoretischem Rebuild und erfolgreicher Umsetzung.

Der Minimum-Viability-Ansatz erkennt an, dass Unternehmen wissen müssen, was ihre wichtigsten Ressourcen sind und wie sie diese wieder betriebsfähig machen können. Anstatt sich mit der überwältigenden Aufgabe zu befassen, vollständige Umgebungs-Rebuilds zu testen, können Unternehmen die Rebuild- Funktion schrittweise implementieren, indem sie sich auf das konzentrieren, was für das Unternehmens überlebensnotwendig ist.

Unternehmen können die Rebuild-Funktion wirksam implementieren, indem sie ihre Anwendungen und Services mithilfe etablierter Frameworks wie ISO 22301 (Business Continuity Management Systems) oder der NIST-Leitlinien zur Business Impact-Analyse nach Bedeutung abstufen. Diese Frameworks helfen Organisationen dabei, Systeme basierend auf ihrer operativen Bedeutung zu kategorisieren:

- *Unternehmenskritisch:* Systeme, auf die Sie nicht verzichten können (z. B. Active Directory, Auftragsmanagementsystem, Patientenversorgungs-systeme). Diese Anwendungen bilden die Grundlage für eine Mindestbetriebsfähigkeit – ohne sie funktioniert das Unternehmen nicht.

- *Geschäftskritisch:* Systeme, die für die vollständige Wiederherstellung von Betriebsabläufen benötigt werden (z. B. E-Mail, Buchhaltung, Liefer- kettenmanagement). Diese ermöglichen eine erweiterte Betriebskapazität, die über das grundlegende Überleben hinausgeht.

- *Nicht kritisch:* Alle anderen Systeme, die für eine volle Funktionalität notwendig sind, aber für eine sofortige Business Continuity nicht unerlässlich sind.

Dieser mehrstufige Ansatz verwandelt die Rebuild-Funktion von einer überwältigenden Herausforderung, bei der alles funktionieren muss, in einen strategischen, stufenweisen Wiederherstellungsprozess. Unternehmen können eine Mindestbetriebsfähigkeit erreichen, indem sie sich bei Rebuild-Tests zunächst auf geschäftskritische Systeme

konzentrieren und dann systematisch auf unternehmenskritische und nicht kritische Anwendungen ausweiten.

Dieser Ansatz reduziert die ursprünglichen Recovery Time Objectives (RTOs) für essentielle Geschäftsfunktionen drastisch und hat gleichzeitig eine vollständige Umgebungswiederherstellung als Ziel.

## Ein vollständige Rebuild: Metadata, Automatisierung und Orchestrierung

Ein effektiver Rebuild umfasst die Erfassung aller relevanten Metadaten – nicht nur der Anwendungsdaten, sondern auch detaillierter Konfigurationen, Ressourcenabhängigkeiten, IAM-Richtlinien (Identitäts- und Zugriffs- management), Netzwerktopologien und API-Endpunkte.

Unternehmen müssen diese umfassenden Metadaten sicher und unveränderlich über mehrere Cloud-Regionen oder isolierte Konten hinweg replizieren, um Single Points of Failure zu minimieren und den Schutz vor Ransomware und unbefugten Änderungen zu erhöhen.

Beim Neuaufbau muss die automatisierte Infrastructure as Code (IAC)-Technik genutzt werden, bei der bislang fragmentierte Wiederherstellungsprozesse zu ausführbaren Automatisierungs-Pipelines zusammengeführt werden. Dieser Ansatz ermöglicht, dass Resilienzprozesse anpassungsfähig, konsistent und überprüfbar bleiben.

Durch die Zentralisierung und kontinuierliche Aktualisierung des Wiederherstellungscodes können Teams die Resilienz proaktiv managen, anstatt rückwirkend auf Vorfälle zu reagieren. Daher bedeutet ein umfassender Rebuild- Prozess nicht nur die Wiederherstellung von Daten, sondern auch die nahtlose und konsistente Orchestrierung der gesamten Cloud-Umgebung.

### Operationalisierung der Rebuild-Funktion: Zeitpunktgenaue Wiederherstellung der Infrastruktur und Recovery as Code

Commvault Cloud Rewind (ehemals Appranix) behebt kritische Schwachstellen herkömmlicher DR-Verfahren mit zwei innovativen Konzepten für den bedarfsgerechten Wiederaufbau von Anwendungsumgebungen: die zeitpunktgenaue Wiederherstellung der Infrastruktur

(Point in Time Recovery PITR) und Recovery as Code (RaC).

In der Vergangenheit hatten Unternehmen Probleme mit fragmentierten Recovery-Runbooks, wobei die Sicherheits-, Anwendungs-, Architektur- und Backup-Teams Runbooks unabhängig voneinander verwalteten. Bei Notfällen nahm schon die Zusammenstellung dieser verstreuten Wiederher- stellungsdokumente viel Zeit in Anspruch, was zu längeren Ausfallzeiten führte.

Die Point-in-time Infrastructure Rrecovery löst dieses Problem durch die Bereit- stellung eines automatisierten, umfassenden Snapshots eines gesamten digitalen Ökosystems – nicht nur der Daten, sondern des kompletten Anwendungs-Stacks, der Microservices, serverlosen Funktionen, Identitäts- und Zugriffskonfigurationen, Netzwerktopologien und deren Abhängigkeiten.

Durch die regelmäßige Erfassung dieser vollständigen Point-in-Time-Zustände auf Grundlage der vorhandenen Richtlinien ermöglicht PITR (Abbildung 3-1) Unternehmen, validierte, umfassende „goldene Kopien" zu pflegen, die sowohl für die Wiederherstellung der Mindestbetriebsfähigkeit als auch für den Neuaufbau des vollständigen Anwendungs-Stacks jederzeit verfügbar sind.

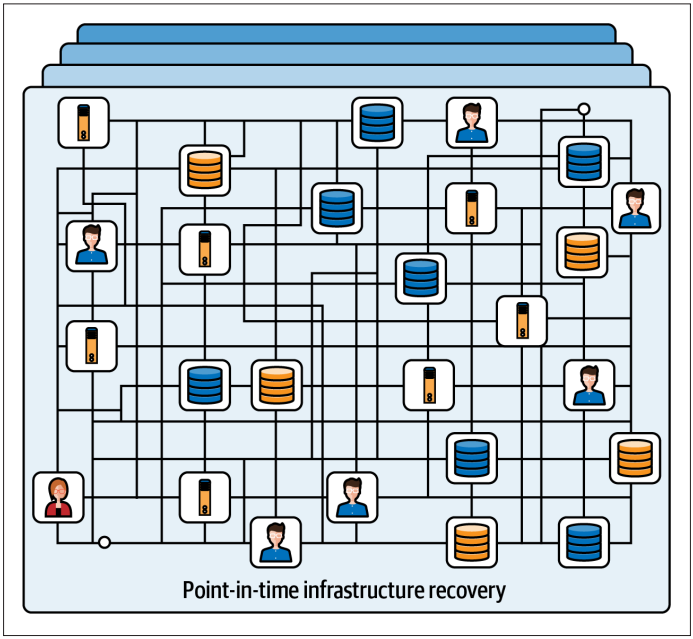


*Abbildung 3-1. Zeigt wie PITR einen umfassenden Snapshot des gesamten Cloud-Anwendungs-Ökosystems liefert*

Die Fähigkeit von PITR, mehrstufige Snapshots zu erfassen, ist für Strategien zur Mindestbetriebsfähigkeit besonders wertvoll. Unternehmen können Richtlinien konfigurieren, die geschäftskritische Anwendungen für häufigere Snapshots priorisieren, unternehmenskritische Systeme mit verifizierten Wiederherstellungspunkten versehen und für nicht kritische Anwendungen den Basisschutz aufrechterhalten.

Dieser mehrstufige Ansatz ermöglicht die schnelle Wiederherstellung der wichtigsten Betriebsprozesse bei gleichzeitiger Aufrechterhaltung eines umfassenden Schutzes in der gesamten Umgebung.

Durch die Nutzung von Hyperscale Cloud-Plattformen wie AWS, Azure oder Google Cloud wird diese Funktion weiter verbessert. Dank der umfangreichen, flexiblen Rechenressourcen und der integrierten Isolierungsfunktionen von Hyperscale Clouds können Unternehmen häufige und umfangreiche Tests problemlos und effizient durchführen. Diese Plattformen vereinfachen komplexe Überprüfungen der Wiederherstellungsprozesse und verwandeln teure und sporadische Disaster Recovery-Übungen in routinemäßige, kosteneffektive Rebuild-Tests.

Als Ergänzung zu PITR verwandelt Recovery as Code die Wiederherstellung in einen einheitlichen, automatisierten Prozess, der die Rebuild-Funktion in die operative Praxis umsetzt. Anstatt separate, umständliche Runbooks zu verwalten, bettet RaC alle notwendigen Wiederherstellungsschritte direkt in ausführbare Automatisierungs-Pipelines ein (Abbildung 3-2).

Versionsgesteuerter Code, bei dem eine einheitliche Vorgehensweise für Sicherheitsteams, Architekten, Anwendungsentwickler und Backup-Spezialisten etabliert wird, dient als zentrale Informationsquelle für die Wiederherstellung. Dieser Code-basierte Ansatz integriert regelmäßige Rebuild-Tests nahtlos in die täglichen DevOps-Workflows und reduziert den operativen Aufwand enorm.

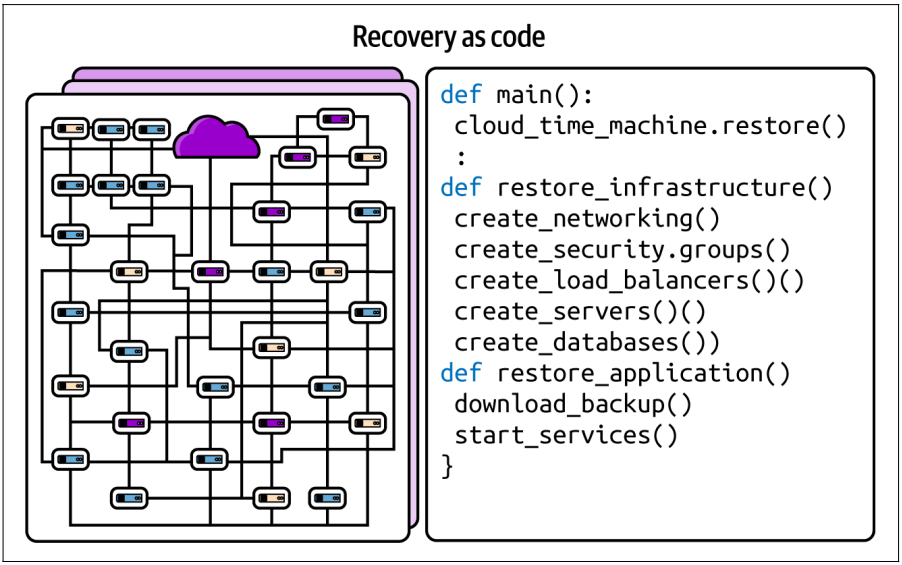


*Abbildung 3-2. PITR kombiniert mit RaC, der alle Wiederherstellungs- schritte in ausführbare Automatisierungs-Pipelines einbettet*

## Den Rebuild strategisch nutzen

RaC kann so strukturiert werden, dass er Workflows zur Mindestbetriebsfähigkeit unterstützt, mit separaten Automatisierungs-Pipelines für geschäftskritische, unternehmenskritische und nicht kritische Anwendungs- ebenen. So können Unternehmen den Mindestbetrieb schnell wiederherstellen und gleichzeitig die vollständige Wiederherstellung der Umgebung vorbereiten, was die Rebuild-Funktion sowohl zu einer strategischen als auch praktisch nutzbaren Komponente macht.

Gemeinsam verändern PITR und RaC die Unternehmens-Resilienz grundlegend. Dank dieser Innovationen können Unternehmen, statt ungewiss im reaktiven Krisenmanagement zu verharren, einen proaktiven und überprüfbaren Ansatz nutzen, der die Wiederherstellungszeiten erheblich verkürzt, Compliance-Anforderungen vereinfacht und ein beispielloses Vertrauen bei den Stakeholdern schafft. Regelmäßige Rebuild-Tests werden somit nicht nur praktikabel, sondern entwickeln sich auch zu einer strategischen Notwendigkeit für moderne digitale Resilienz.

# Der geschäftliche Nutzen regelmäßiger Rebuild-Tests inklusive Kostenoptimierung

Regelmäßige Rebuild-Tests mit PITR und RaC beeinflussen die Resilienz eines Unternehmens grundlegend, da sie die Rebuild-Funktion sowohl rentabel als auch strategisch wertvoll machen. Anstatt sich auf unsichere Wiederherstellungspläne und angstbestimmtes Krisenmanagement zu verlassen, verfügen Unternehmen über klare, messbare und belegbare Wiederherstellungsmöglichkeiten.

Nehmen wir an, eine Gesundheitseinrichtung wird Opfer eines Ransomware- Angriffs. Anstatt auf die vollständige Wiederherstellung der Infrastruktur zu warten, ermöglicht die Planung der Mindestbetriebs-fähigkeit die schnelle Wiederherstellung von Patientenversorgungs-systemen, des Notaufnahmebetriebs und wichtiger Kommunikationskanäle. Die Einrichtung kann ihre Administrationssysteme, Terminplanungs-plattformen und Reporting-Tools später wiederherstellen, ohne die Patientenversorgung zu stören.

Dieser mehrstufige Ansatz bietet zahlreiche messbare Geschäftsvorteile.

## Verbesserte Betriebsprozesse und Kundenvertrauen

Da die Planung der Mindestbetriebsfähigkeit umsatzgenerierende Systeme priorisiert, können Unternehmen ihre Kerngeschäfte schnell wieder aufnehmen und gleichzeitig das Vertrauen der Kunden bewahren. Dieses Vertrauen wird zu einem Wettbewerbsvorteil, insbesondere in Branchen, in denen sich die digitale Zuverlässigkeit direkt auf die Kundenbeziehungen auswirkt.

## Regulatorische und Compliance-Vorteile

Die Planung der Mindestbetriebsfähigkeit hilft Unternehmen dabei, die gesetzlichen Anforderungen zu erfüllen, wenn es um die Aufrechterhaltung wichtiger Services bei Betriebsausfällen geht. Automatisierte Rebuild-Tests vereinfachen Compliance-Prozesse, da regelmäßig umfassende Nachweise generiert werden, was die Vorbereitung von Audits effizienter macht.

Einrichtungen können so mit minimalem manuellem Aufwand die Einhaltung gesetzlicher Standards wie dem Health Insurance Portability and Accountability Act (HIPAA) und branchenspezifischen

Richtlinien wie SOC 2, ISO 27001 sowie dem Digital Operational Resilience Act (DORA) nachweisen und Prüfern sofortigen Einblick in ihre Resilienz-Fähigkeiten verschaffen.

### Kosten- und Zeitersparnis

Durch die Automatisierung von Rebuilds sinken Komplexität und Kosten erheblich. Herkömmliche Disaster Recovery-Tests sind kostspielig, betriebs- störend und anfällig für menschliche Fehler. Durch die Einführung von RaC können Unternehmen mithilfe von Programmier- und Bereitstellungs-modellen in der Hyperscale Cloud ganz nach Bedarf effektiv Rebuilds und Tests durchführen.

Sie können komplexe Rebuild-Prozesse automatisieren und unstrukturierte, manuelle Runbooks in optimierte, wiederholbare, codebasierte Abläufe verwandeln. Diese Automatisierung reduziert nicht nur den administrativen Aufwand und beseitigt die Kosten für manuelle Tests, sondern fördert auch mit jedem Test die Konsistenz und Zuverlässigkeit.

### Zuversicht und Vertrauen innerhalb des Unternehmens

Wichtig ist außerdem, dass regelmäßige Rebuild-Tests beispiellose Zuversicht und Vertrauen innerhalb des Unternehmens erzeugen. Regel-mäßig validierte Wiederherstellungsfähigkeiten bieten Führungsteams klare und belegbare Gewissheit, dass sie auf Betriebsausfälle vorbereitet sind.

Aufsichtsbehörden, Kunden und Partner können darauf vertrauen, dass das Unternehmen Risiken proaktiv mindert und sich nach Cyberangriffen oder Cloud-Ausfällen schnell erholen kann. Dieses Vertrauen wird zu einem strategischen Vorteil, durch den sich widerstandsfähige Unternehmen in einer Welt, die zunehmend von digitalen Bedrohungen und Ausfällen geprägt ist, von den anderen abheben.

## Rebuild-Tests praxisnah gestalten: Infrastruktur und Validierungsmethoden

Nach der Festlegung des strategischen Rahmens für eine Mindestbetriebsfähigkeit stellt sich die Frage: Wie führen Unternehmen Rebuild-Tests im großen Maßstab für kritische

Anwendungen durch? Es gibt zwei Schlüsselfaktoren, die häufige Tests erschwinglich und auch realistisch machen:

- Erstens bieten Hyperscale-Cloud-Plattformen die flexible Infrastruktur, die man braucht, um bei Bedarf ganze Testumgebungen hochzufahren.

- Zweitens helfen Chaos-Engineering-Prinzipien bei diesen Tests, reale anstelle von vorhersehbaren Ausfallszenarien zu simulieren.

Gemeinsam verwandeln diese Ansätze Rebuild-Tests von einer kostspieligen jährlichen Übung in einen funktionsfähigen Routineablauf.

## Cloud-Plattformen als leistungsstarke Testumgebung nutzen

Cloud-Plattformen wie AWS, Azure und Google Cloud bieten aufgrund ihrer unübertroffenen Flexibilität, Skalierbarkeit und Erschwinglichkeit eine ideale Umgebung für regelmäßige Rebuild-Tests. Im Gegensatz zu herkömmlichen Rechenzentren ermöglichen Hyperscale-Clouds Unternehmen, auf Knopfdruck vollständig isolierte Sandbox-Umgebungen bereitzustellen, umfassende Tests durchzuführen und diese, ohne den laufenden Betrieb zu stören, wieder abzubauen.

Diese Flexibilität beseitigt die lästigen Hürden herkömmlicher Disaster Recovery-Tests und ermöglicht so häufigere und aussagekräftigere Tests.

Ein wesentlicher Vorteil dieser Plattformen sind die riesigen bedarfsorientieren Rechen- und Speicherkapazitäten, mit denen Unternehmen Ressourcen entsprechend den spezifischen Testanforderungen schnell nach oben oder unten skalieren können. Die strategische Nutzung von Spot-Instanzen ermöglicht eine skalierbare Rechenkapazität zu drastisch reduzierten Kosten – oft 70% bis 80% unter den herkömmlichen On-Demand-Preisen – und erlaubt eine höhere Testfrequenz ohne das Budget zusätzlich zu belasten.

Die Cloud-Umgebung ermöglicht außerdem die Simulation von partiellen Infrastrukturausfällen, das Testen von regionenübergreifenden Failover- Funktionen für geschäftskritische Systeme und die Validierung, dass Verfahren zur Wiederherstellung

der Mindestbetriebsfähigkeit bei unterschiedlichen Ausfallszenarien funktionieren – und das alles in kosteneffizienten, isolierten Testumgebungen.

Regelmäßige Rebuild-Tests, die früher als komplex und kostspielig galten, sind jetzt praktisch und leicht zugänglich, was sie zukünftig von einer sporadischen Compliance-Maßnahme zu einer Kernfunktion von Unternehmen macht.

## Chaos-Test: Resiliente Systeme durch gezielt herbeigeführte Ausfälle

Il test del caos è la pratica di introdurre deliberatamente interruzioni Bei Chaos-Tests wird ein System gezielt herbeigeführten Ausfällen ausgesetzt, um verborgene Schwachstellen aufzudecken und die Widerstandsfähigkeit unter realistischen Bedingungen zu validieren. Bei diesem Ansatz werden absichtlich Ausfallszenarien wie Infrastrukturausfälle, Netzwerklatenz oder unerwartete Ressourcenspitzen simuliert, um zu testen, ob Systeme unter Belastung zuverlässig funktionieren.

Im Gegensatz zu Standard-DR-Tests, bei denen häufig vorhersehbare Szenarien simuliert werden, setzen Chaos-Tests auf Unvorhersehbarkeit, das laufende Hinterfragen von Annahmen und die Aufdeckung von verborgenen Schwachstellen in Bezug auf die Resilienz von Anwendungen und Infrastrukturen.

Im Kontext von Rebuild-Tests sind Chaos-Tests besonders wichtig, da sich Produktionsumgebungen ständig weiterentwickeln, neue Services bereitgestellt werden, Konfigurationen sich ändern und Workloads fluktuieren. Herkömmliche statische Rebuild-Tests sind schnell veraltet.

Cloud-Plattformen ermöglichen es Unternehmen, adaptive Rebuild-Tests durchzuführen, die die Dynamik moderner Anwendungen widerspiegeln. Durch die Integration von Chaos-Engineering-Prinzipien in Rebuild-Verfahren werden Tests proaktiv weiterentwickelt, bilden die Komplexität der Produktionsumgebung ab und passen sich kontinuierlich an Änderungen an.

Chaos-Tests gewinnen zusätzlich an Bedeutung, wenn sie unter dem Gesichtspunkt der Mindestbetriebsfähigkeit durchgeführt werden.

Anstatt zufällige Ausfallszenarien über ganze Umgebungen hinweg zu testen, können Unternehmen sich bei den Chaos-Tests auf geschäftskritische Systeme konzentrieren, um zu verstehen, wie Ausfälle sich auf andere Systeme auswirken und die Wiederherstellung der Mindestbetriebsfähigkeit beeinflussen können.

So könnte ein Chaos-Test während einer Übung zur Wiederherstellung der Mindestbetriebsfähigkeit beispielsweise absichtlich Active Directory-Dienste deaktivieren, um zu verifizieren, ob Backup-Systeme zur Authentifizierung wichtige Geschäftsabläufe aufrechterhalten können. Oder er könnte Fehler bei der Netzwerksegmentierung zwischen kritischen Mikro-Services simulieren, um zu überprüfen, ob für den Mindestbetrieb notwendige Anwendungen auch dann funktionsfähig bleiben, wenn abhängige Dienste nicht verfügbar sind.

# Regelmäßige Rebuild-Tests durchführen: Von der Theorie zu konkreten Ergebnissen

Die Einführung regelmäßiger Rebuild-Tests verwandelt die Resilienz eines Unternehmens von einer theoretischen Zuversicht in konkret messbare Fähigkeiten. So wie bei der Entwicklung von Software mittlerweile regelmäßig Qualitätssicherungsmaßnahmen (QS) gesetzt werden, müssen auch für die digitale Resilienz regelmäßige Rebuild-Tests durchgeführt werden. CIOs und CISOs können greifbare Ergebnisse erwarten: Nachweisbare Wiederherstellungsfähigkeit, messbare Risikoreduktion und klare Abstimmung zwischen den Teams für Cyber-Sicherheit, Cloud- Operation und Wiederherstellung.

## Mehrstufige Testansätze implementieren

Ein strukturierter Ansatz beginnt mit der Planung monatlicher oder vierteljährlicher Rebuild-Testtage, die sowohl Szenarien für die Wiederherstellung der Mindestbetriebsfähigkeit als auch der gesamten Umgebung umfassen. Diese Termine müssen sorgfältig geplant werden und sollten regelmäßige Wiederherstellungsübungen, Tests zur Mindestbetriebsfähigkeit und kontrollierte Chaos-Tests umfassen.

### Testtage zur Mindestbetriebsfähigkeit

Unternehmen sollten separate Übungen durchführen, die sich speziell auf die Wiederherstellung geschäftskritischer Systeme innerhalb definierter Zeitfenster konzentrieren. Diese Tests überprüfen, ob wichtige Geschäftsfunktionen schnell wiederhergestellt werden können, am besten innerhalb weniger Stunden und nicht Tage.

Zu den Erfolgskennzahlen für diese Tests gehören die Dauer für die Wiederherstellung von Identitäts-Diensten, die Zeitspanne, um wichtige Geschäftsanwendungen wieder online zu bringen, und die Verifizierung, dass die Mindestbetriebsfähigkeit aufrechterhalten werden kann, während die vollständige Wiederherstellung fortgesetzt wird.

### Tests zur vollständigen Wiederherstellung der Umgebung

Auch die Durchführung umfassender Tests zur vollständigen Wiederherstellung der Infrastruktur sind essentiell, um zu bestätigen, dass unternehmenskritische und nicht kritische Systeme erfolgreich wiederhergestellt werden können, nachdem die Mindestbetriebsfähigkeit gewährleistet ist. Diese Tests überprüfen die Fähigkeit des Unternehmens, die volle Betriebskapazität wiederaufzunehmen.

## Rollen und Zuständigkeiten definieren

Eine klare Definition von Rollen und Verantwortlichkeiten ist für effiziente Tests von entscheidender Bedeutung, insbesondere wenn Mindestbetriebsfähigkeit und vollständige Wiederherstellung der Umgebung miteinander in Einklang gebracht werden sollen.

### Sicherheitsteams

Die Sicherheitsteams stellen sicher, dass wiederhergestellte Umgebungen rigoros gescannt und von Sicherheitslücken, Ransomware-Signaturen und Fehlkonfigurationen befreit werden. Während der Wiederherstellung der Mindestbetriebsfähigkeit konzentrieren sich diese Teams auf die Validierung geschäftskritischer Systeme und führen gleichzeitig umfassende Sicherheitsbewertungen der Gesamtumgebung durch.

### Cloud-Operation- und Anwendungsteams

Diese Teams konzentrieren sich auf die Bereitstellung der Infrastruktur, die Konfigurationsabstimmung und die Orchestrierung umfassender Rebuilds aus den PTIR der Umgebungen. Sie überwachen die technische Ausführung der Wiederherstellung für die Mindestbetriebsfähigkeit sowie für jene der Gesamtumgebung und bestätigen, dass Abhängigkeiten in der Infrastruktur korrekt aufeinander abgestimmt sind und dass die wiederhergestellten Services den funktionalen Anforderungen entsprechen.

### Recovery-Teams

Die Wiederherstellungsteams überwachen den gesamten Rebuild-Prozess und sorgen für eine gruppenübergreifende Koordination und eine genaue Dokumentation der Ergebnisse. Sie steuern den Übergang von der Mindestbetriebsfähigkeit zur vollen Betriebskapazität und koordinieren verschiedene Testszenarien.

## Erfolg messen und Nutzen aufzeigen

Um die Effektivität zu beurteilen und den Nutzen von Rebuild-Tests zu demonstrieren, müssen klare Kennzahlen festgelegt und kommuniziert werden. Diese Kennzahlen gehen über einfache Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) hinaus. Sie umfassen:

*Kennzahlen für die Mindestbetriebsfähigkeit*
: Die Dauer für die Wiederherstellung geschäftskritischer Systeme und damit verbundener Abhängigkeiten, die Erfolgsquote der Verfahren zur Erlangung der Mindestbetriebsfähigkeit bei Belastungstests und die Fähigkeit, wichtige Betriebs- abläufe im Zuge der vollständigen Wiederherstellung aufrecht zu erhalten.

*Kennzahlen für die umfassende Wiederherstellung*
: Die Zeitspanne bis zur vollständigen Wiederherstellung ganzer Umgebungen, die Erfolgsrate der Verfahren zur vollständigen Wiederherstellung und die Überprüfung der korrekten Funktion aller Systeme nach der Wiederherstellung.

*Kennzahlen für Resilienz-Tests*
: Die Häufigkeit und Gründlichkeit der durchgeführten Chaos-Tests, die Anzahl der bei den Tests erkannten und behobenen Schwachstellen oder Fehlkonfigurationen sowie die langfristige Verbesserung der Wiederherstellungsleistung.

*Kennzahlen zu den geschäftlichen Auswirkungen*
: Die Reduzierung potenzieller Umsatzverluste bei Cybervorfällen, Kennzahlen zur Verbesserung des Kundenvertrauens und der Nachweis der Einhaltung gesetzlicher Vorschriften durch regelmäßige Tests.

CIOs und CISOs sollten regelmäßig Berichte mit Fokus auf diese Kennzahlen erhalten. Sie liefern langfristig Transparenz und konkrete Nachweise für Verbesserungen.

Durch regelmäßige Rebuild-Tests erhalten alle Beteiligten konkrete Nachweise zu den Wiederherstellungs-Fähigkeiten des Unternehmens – von Sicherheitsteams, die ein reduziertes Bedrohungsrisiko überprüfen möchten, bis hin zu Führungskräften, die ihre operationale Resilienz demonstrieren wollen.

Bislang als Best Practice angesehen, nehmen regelmäßige Rebuild-Tests nun im Unternehmen eine Kernfunktion im Risikomanagement ein. Durch die Integration von Prinzipien zur Mindestbetriebsfähigkeit in umfassende Tests können Unternehmen eindeutig nachweisen, dass sie wichtige Geschäftsfunktionen schnell wiederherstellen und gleichzeitig eine vollständige digitale Resilienz gewährleisten können. Diese Fähigkeit ist aufgrund der sich ständig weiterentwickelnden und zunehmenden Cyber-Bedrohungen für das Überleben von Unternehmen unerlässlich geworden.

KAPITEL 4

# Ihr Schlüssel zum Erfolg: Die Rebuild-Funktion: Grundlage echter Cyber-Resilienz

Echte Cyber-Resilienz hängt von einer wichtigen Fähigkeit ab, die über herkömmliche Cyber-Sicherheitskonzepte hinausgeht. Wie in Kapitel 2 festgestellt, benötigt das NIST Cybersecurity Framework eine siebte Funktion: „Neu Aufbauen" oder „Rebuild". Diese Funktion verwandelt Ungewissheit in Sicherheit und macht den „Hoffentlich funktioniert das Backup"-Ansatz überflüssig, indem die Wiederherstellungsfähigkeiten durch regelmäßige Tests überprüft.

Der Ansatz der in Kapitel 3 dargelegten Mindestbetriebsfähigkeit macht diese Umstellung möglich. Anstatt alles gleichzeitig zu testen, können Unternehmen den Rebuild systematisch implementieren, beginnend bei geschäftskritischen Systemen bis hin zu ganzen Umgebungen. Dieses strategische Framework verwandelt eine erdrückende Herausforderung in einen überschaubaren, schrittweisen Prozess, der einen unmittelbaren Nutzen bringt und gleichzeitig auf eine umfassende Resilienz hinarbeitet.

## Die Bedrohung durch agentische KI: Warum sich die Recovery-Anforderungen mit der Geschwindigkeit der Angriffe ändern

Experten prognostizieren, dass wir schon in diesem Jahr eine Welle KI- gestützter Angriffe erleben könnten, da KI-Agenten viel billiger als professionelle Hacker sind und Angriffe schneller und weitaus umfangreicher als Menschen koordinieren können, was sie für Cyberkriminelle äußerst attraktiv macht.

KI-gesteuerte Ransomware besteht aus mehreren KI-Bots, die alle Schritte für einen erfolgreichen Ransomware-Angriff ausführen, aber schneller und besser als menschliche Akteure. Diese Systeme beschleunigen vorhandene

Angriffsmethoden nicht nur, sondern ändern die Spielregeln grundlegend, indem sie mit maschineller Geschwindigkeit arbeiten und Funktionen für maschinelles Lernen nutzen.

Die Folgen für Wiederherstellungsprozesse sind enorm. In fast jedem fünften Fall findet der Datendiebstahl nun in der ersten Stunde nach der Kompromittierung statt. Herkömmliche Backup- und Wiederherstellungs- ansätze, die auf von Menschen gesteuerte Bedrohungen ausgelegt sind, und die einen Vorlauf von Tagen oder Wochen boten, sind obsolet, wenn bei einem Angriff von der Erkundungsphase bis zur Verschlüsselung nur wenige Minuten vergehen.

Im Zeitalter der agentischen KI gewinnt die schnelle, automatisierte Rebuild- Funktion zunehmend an Bedeutung. Nur durch regelmäßige, automatisierte Tests können Unternehmen Gegnern, die mit übermenschlicher Geschwindigkeit lernen und sich anpassen, einen Schritt voraus sein.

## Ihr strategischer Fahrplan: Von der Mindestbetriebsfähigkeit zur vollständigen Resilienz

Der Weg zum sicheren Rebuild folgt dem Ansatz der Mindestbetriebsfähigkeit, der die Durchführung umfassender Tests möglich macht. Unternehmen beginnen damit, geschäftskritische Systeme zu identifizieren, die im Notfall für einen Mindestbetrieb unerlässlich sind. Anschließend implementieren sie PITR- Snapshots und RaC-Automatisierung für diese Prioritätssysteme.

Erfolge beim Mindestbetrieb schaffen die Grundlage für eine Erweiterung. Unternehmen können in der Folge die Rebuild-Funktionen auf unternehmenskritische Systeme wie die Buchhaltung und das Lieferketten- Management erweitern, gefolgt von nicht kritischen Anwendungen. Jede Erweiterung baut auf geprüften

Prozessen und wachsendem Unternehmens- Know-how auf, und letztendlich wird eine umfassende Rebuild-Fähigkeit für das gesamte digitale Ökosystem erreicht.

Die in Kapitel 3 erörterten Hyperscale-Cloud-Plattformen machen diesen Fortschritt wirtschaftlich tragbar. Laut der offiziellen AWS- und Azure- Dokumentation senken Spot-Instanzen im Vergleich zu On-Demand-Preisen die Testkosten um bis zu 90%, während die flexible Infrastruktur eine häufige Validierung ohne Beeinträchtigung der Produktionssysteme ermöglicht.

Chaos-Tests sorgen dafür, dass Testszenarien reale Ausfallszenarien widerspiegeln und ein echtes Vertrauen in die Wiederherstellungsfunktionen entsteht.

## Herausforderungen bei der Implementierung meistern

Das Konzept der Mindestbetriebsfähigkeit überwindet systematisch unternehmensinterne Barrieren bei der Umsetzung der Rebuild-Funktion. Äußern Führungskräfte Bedenken hinsichtlich der Kosten, spricht der wirtschaftliche Nutzen klar dafür. Die schnelle Wiederherstellung umsatzgenerierender Systeme lohnt sich beim ersten Vorfall, der damit verhindert werden kann.

Denken Sie nur an das Praxisbeispiel aus Kapitel 3. MGM Resorts und Caesars Entertainment besaßen umfassende DR-Pläne, doch beide Unternehmen hatten Schwierigkeiten bei der Wiederherstellung, da ihnen keine getesteten Rebuilds zur Verfügung standen. Der Ansatz der Mindestbetriebsfähigkeit hätte die schnelle Wiederherstellung der wichtigsten Casino- und Hotelsysteme erleichtert, während die vollständige Wiederherstellung parallel verlaufen wäre, wodurch Geschäftsausfälle und Auswirkungen auf die Kunden minimiert hätten werden können.

In ähnlicher Weise zeigte die Erfahrung des NHS in London mit der Qilin Ransomware, dass zuverlässige Backups ohne verifizierte Wiederherstellungsverfahren für Anwendungen, Identitäten und Netzwerkarchitekturen nutzlos sind. Eine Strategie zur Mindestbetriebsfähigkeit hätte die Wiederherstellung des Patientenversorgungssystems priorisiert, wodurch wichtige Gesundheitsdienstleistungen fortgesetzt werden hätten können, während gleichzeitig ein umfassender Rebuild der Backoffice- und Support- Systeme möglich gewesen wäre.

## Budget- und Ressourceneinschränkungen

Durch die RaC-Automatisierung werden unstrukturierte Runbooks in einheitlichen, versionsgesteuerten Pipelines zusammengefasst. Sicherheits-, Cloud-Operations-, Anwendungs- und Wiederherstellungsteams arbeiten auf Basis desselben Codes zusammen, anstatt einzelne, isolierte Dokumentationen zu pflegen. Durch diese Konsolidierung entfallen separate Übungen über mehrere Teams hinweg, während Konsistenz gewährleistet und der manuelle Aufwand reduziert wird.

Der ROI spricht für sich, sobald Unternehmen die Zeiten für die Wiederherstellung der Mindestbetriebsfähigkeit messen. Die Reduzierung des RTO von 48 auf 2 Stunden für geschäftskritische Systeme bringt sofortigen Nutzen. Durch die automatisierte Erfassung von Compliance-Nachweisen für SOC 2, ISO 27001 und DORA reduziert sich der Audit-Aufwand und gleichzeitig können die Wiederherstellungsfunktionen kontinuierlich validiert werden.

## Rückhalt im Management und Unternehmensausrichtung

Nichts überzeugt Führungskräfte so sehr wie belegbarer Erfolg. Unternehmen können Rebuild-Kennzahlen in Echtzeit auf Dashboards anzeigen, Führungskräften Auditberichte zur Verfügung stellen und eine vollständige Wiederherstellung in weniger als einer Stunde anstatt in Tagen oder Wochen demonstrieren.

Der Ansatz der Mindestbetriebsfähigkeit macht die geschäftlichen Auswirkungen sofort sichtbar. Erkennt die Führungskraft, dass die wichtigsten umsatzgenerierenden Systeme schnell und zuverlässig wiederhergestellt werden können, folgen die Finanzierung und die organisatorische Unterstützung ganz von selbst. Jeder erfolgreiche Test der Mindestbetriebsfähigkeit schafft Vertrauen für eine erweiterte Umsetzung des Rebuilds.

# Ausblick: Wenn der Rebuild zum Standard wird

Die Zukunft der Cyber-Resilienz zeichnet sich bereits ab, angetrieben von der Realität KI-gesteuerter Bedrohungen. Mit zunehmender Leistungsfähigkeit der KI-Agenten werden Sicherheitsteams weitere Aufgaben mit minimalem Aufwand an autonome Agenten delegieren,

sodass Systeme und Netzwerke mit sich ständig weiterentwickelnden Bedrohungstaktiken Schritt halten können. In fünf Jahren wird die Rebuild-Funktion für die Cyber-Sicherheit genauso wichtig sein wie die Funktionen des aktuellen NIST-Frameworks. Die Planung der Mindestbetriebsfähigkeit wird allgemeiner Standard, wobei Unternehmen sich so strikt an getestete Wiederherstellungsverfahren für unternehmenskritische Systeme halten werden wie an Finanzkontrollen.

Diese Transformation wird die Art und Weise verändern, wie Unternehmen digitale Resilienz angehen:

- *KI-gestützte Rebuild-Funktionen:* Zukünftige Rebuild-Systeme nutzen KI, um Konfigurationsabweichungen automatisch zu erkennen, potenzielle Ausfallszenarien vorherzusagen und systematische Chaos-Tests durchzuführen, die neue Angriffsvektoren vorhersehen, bevor diese eingesetzt werden. Diese agentischen Wiederherstellungssysteme werden Hand in Hand mit menschlichen Akteuren arbeiten, um Routineaufgaben autonom durchzuführen, menschliche Entscheidungen zu verbessern und Workflows zu automatisieren.
- *Reaktion mit angepasster Geschwindigkeit:* Mit zunehmender Beschleunigung der Angriffe müssen auch die Rebuild-Fähigkeiten entsprechend angepasst werden. Unternehmen werden KI-basierte Wiederherstellungssysteme implementieren, die eine vollständige Wiederherstellung der Umgebung schneller durchführen, als Angreifer ihre Strategien anpassen können.
- *Wettbewerbsvorteil:* Unternehmen, die eine schnelle und zuverlässige Wiederherstellung vorweisen können, werden erhebliche Wettbewerbsvorteile erzielen. Kunden und Partner bevorzugen Anbieter, die eine zuverlässige Betriebskontinuität aufzeigen können. In regulierten Branchen werden belegbare Rebuild-Fähigkeiten zur Voraussetzung für die Beibehaltung von Lizenzen und Zertifizierungen werden.

Unternehmen, die die Rebuild-Funktion schon heute nutzen – beginnend bei der Mindestbetriebsfähigkeit bis hin zum Ausbau einer vollständigen Abdeckung – werden nicht nur die Angriffe von morgen überstehen, sondern auch stärker daraus hervorgehen. Sie werden Cyber-Vorfälle nicht mehr als geschäftsbedrohliche Katastrophen, sondern als überschaubare operative Herausforderungen sehen.

# Ihr Weg in die Zukunft: Von der Hoffnung zur Gewissheit

Die Entscheidung, die jedes Unternehmen treffen muss, ist klar: entweder weiter hoffen, dass herkömmliche Backup- und Recovery-Methoden gegen moderne Bedrohungen ausreichen, oder mit dem Aufbau einer nachweisbaren Rebuild- Fähigkeit beginnen, die echte Sicherheit bietet.

Das Konzept der Mindestbetriebsfähigkeit hilft bei der Umsetzung dieser Entscheidung. Beginnen Sie mit einem einzigen geschäftskritischen System. Implementieren Sie PTIR-Snapshots und RaC-Automatisierung. Führen Sie Chaos-Tests durch, um die Wiederherstellung im Notfall zu validieren. Messen und präsentieren Sie die Ergebnisse.

Erfolge bei einem System bilden die Grundlage für eine Erweiterung auf andere Systeme. Jedes zusätzliche System profitiert vom wachsenden Unternehmens- Know-how, bewährten Prozessen und etablierter Automatisierung. Der Weg von der Backup-Hoffnung zur Sicherheit eines Rebuilds beschleunigt sich mit zunehmenden Fähigkeiten.

Testen Sie zuerst Ihre Mindestbetriebsfähigkeit, und gehen Sie dann systematisch eine Erweiterung an. Vertrauen Sie auf eine zuverlässige Wiederherstellung dank bewährter Rebuild-Fähigkeiten. Sichern Sie Unternehmenswachstum, indem Sie Resilienz zu einem Wettbewerbsvorteil machen.

Die Cyberbedrohungen von morgen werden ausgeklügelter, hartnäckiger und verheerender sein als die heutigen Angriffe. Unternehmen, die auf perfekte Lösungen oder ideale Bedingungen warten, stehen unvorbereitet da, wenn das Überleben von der Geschwindigkeit und Zuverlässigkeit der Wiederherstellung abhängt.

Beginnen Sie mit dem Definieren Ihrer geschäftskritischen Systeme und folgen Sie dem Ansatz der Mindestbetriebsfähigkeit. Die Technologie existiert bereits. Die Methoden sind erprobt. Die einzige Frage ist, ob Sie gleich jetzt beginnen oder warten, bis der nächste Angriff Sie dazu zwingt.

Entscheiden Sie sich für Sicherheit, für den Rebuild und dafür, auch in unsicheren Zeiten erfolgreich zu agieren.

## Über den Autor

**Govind Rangasamy** ist Gründer und CEO von Appranix, das jetzt zu Commvault gehört, und Autor des Forbes Technology Council. Als Mehrfachunternehmer mit umfassender Erfahrung im Management von Enterprise-Clouds gründete Govind Appranix, um infrastrukturorientierte Resilienzmodelle zu revolutionieren, die seiner Ansicht nach für die heutigen verteilten, dynamischen Cloud- Anwendungen unzureichend sind. Er schreibt regelmäßig für Forbes und ist häufiger Gast in Podcasts sowie Konferenzredner zum Thema Cloud-Resilienz.