IBM Resiliency Orchestration mit Cyber Incident Recovery

Schutz von Daten und Plattformkonfigurationen mit zweckgerichteter Funktionalität für die schnelle, zuverlässige und skalierbare Wiederherstellung nach Cyberattacken

Highlights

- Durch einen Air-Gap geschützten und nicht veränderbaren Speicher für Daten und Plattformkonfigurationsdateien.
- Schnelle Erkennung von Anomalien in Windows- oder Linux-System-konfigurationen wie Windows-Registrierungen, Anwendungs-konfigurationen und Gerätekonfigurationen.
- Weniger Auswirkungen von Störungen durch eine Cyberattacke oder einen anderen Ausfall durch die schnelle, koordinierte Wiederherstellung von Daten und Plattformkonfigurationen.
- Häufigere Tests ohne Auswirkungen auf die Geschäftssysteme durch eine automatisierte Test- und Überprüfungsplattform.
- Erfüllung von Compliance-Anforderungen durch hohe Prozesstransparenz und Berichterstellungsfunktionen.

Cyberattacken stellen nach wie vor eine Gefahr für Unternehmen aller Größenordnungen dar. Während die IT-Sicherheitsgruppen immer besser Cyberattacken verhindern, stellt sich bei solchen Angriffen nach wie vor die Frage nach dem „Wann“ (falls nicht bereits passiert) und nicht nach dem „Ob“. Eine durch Cyberattacken verursachte Betriebsunterbrechung, durch die Ihre kritischen Daten und Systemkonfigurationen beschädigt werden, kann ebenso schädlich für die finanzielle Situation und den Ruf eines Unternehmens sein wie Datendiebstahl oder ein kompletter IT-Ausfall.

Dies gilt insbesondere dann, wenn es bei den Cyberattacken um Datenverschlüsselung oder Malware geht, die speziell auf Daten-sicherungen abzielt. Durch kontinuierliche Netzwerklücken bei Sicherungs- und Disaster-Recovery-Standorten (DR) kann Malware die dort befindlichen Daten beschädigen oder verschlüsseln. Dadurch werden sowohl Primärdaten als auch Sicherungsdaten unbrauchbar, sodass der Produktionsbetrieb nur mit erheblichen Verzögerungen wieder aufgenommen werden kann.

Häufig tritt der Schaden dadurch auf, dass bestehende DR-Lösungen nicht für die Wiederherstellung nach Cyberattacken ausgelegt sind oder es immer wieder zu Problemen bei der DR-Funktionalität kommt. Hierzu gehören beispielsweise hohe Abhängigkeit von manuellen Prozessen, veraltete Runbooks und unzureichende Tests. Dadurch dauert die Wiederherstellung zu lange, die Daten-wiederherstellungspunkte sind zu alt oder die Wiederherstellung selbst schlägt fehl.

Eine zweckgerichtete Lösung für höhere Cyberausfallsicherheit

Cyber Incident Recovery, unterstützt von IBM Resiliency Orchestration, wurde entwickelt, um Daten und Plattformkonfigurationen bei einem Cyber-bedingten Ausfall sehr schnell wiederherzustellen. Als speziell für die Wiederherstellung nach einer Cyberattacke konzipierte Lösung bietet Cyber Incident Recovery zahlreiche Vorteile:

- Einfache Testfunktionalität ohne Auswirkungen auf die Produktionsumgebungen.
- Schnellere Erkennung von fehlerhaften Daten und schnelle Reaktion zur Reduzierung von Ausfallzeiten.
- Effiziente, zeitpunktgesteuerte Wiederherstellung für bessere RPO-Ergebnisse.
- Hohe Skalierbarkeit für die schnelle Verarbeitung komplexer Erkennungs- und Wiederherstellungsprozesse auf Siteebene innerhalb von Minuten.
- Bessere Transparenz und Berichterstellung zur Einhaltung gesetzlicher Bestimmungen.

Die technologischen Bausteine, auf denen Cyber Incident Recovery basiert, bilden eine Plattform für Rechen- und Datenebenen von Produktions- und DR-Umgebungen. Somit ist ein agiler Wiederherstellungsansatz nach einer Cyberattacke gewährleistet. Diese Architektur umfasst Folgendes:

Nicht veränderbarer Speicher. Nicht veränderbarer Speicher für Konfigurationsdaten oder WORM-Speicher (Write Once Read Many) für Anwendungsdaten trägt dazu bei, Beschädigungen zu verhindern und eine korrekte Wiederherstellbarkeit zu gewährleisten, da Änderungen an gesicherten Konfigurationsdaten nach dem Speichern nicht mehr vorgenommen werden können. Bei Anwendungsdaten hilft dieser Ansatz, die Speicherkosten zu senken, weil nur neue Kopien von inkrementellen PIT-Änderungen in den Speicher geschrieben werden.

Air-Gap-basierter Schutz. In isolierten Netzwerken werden Produktionsumgebungen vom WORM-Speicher getrennt, der die geschützten Sicherungsdaten an einem Remote- oder DR-Standort enthält. Der Zugriff auf den WORM-Speicher ist zudem auf die Zeiten beschränkt, in denen Daten für Sicherungen zur Verfügung stehen. Durch diesen Ansatz, in Kombination mit nicht veränderbarem Speicher, wird verhindert, dass geschützte Daten durch Malware beschädigt werden, die Netzwerke durchdringt oder speziell Sicherungsdaten im Visier hat.

Überprüfung von Konfigurationsdaten. Diese Überprüfung trägt dazu bei, dass die zu schützende Konfiguration oder die Daten sauber und wiederherstellbar sind. Dieser in Resiliency Orchestration integrierte Prozess erkennt automatisch, wenn Ihre Systemkonfigurationen geändert wurden und nicht mit den „goldenen“ Versionen übereinstimmen. Zudem lässt sich Resiliency Orchestration in vom Kunden bereitgestellte Scripts zur Anwendungsgültigkeit integrieren, um Tests auf Anwendungs- und Datenebene zu ermöglichen.

Automatisierung und Orchestrierung. Durch die Automatisierung des End-to-End-Wiederherstellungsprozesses (E2E) für Daten, Anwendungen, Switches und Recheninfrastrukturen ermöglicht Resiliency Orchestration die schnelle Wiederherstellung Ihrer IT-Umgebung. Resiliency Orchestration ersetzt dabei die traditionellen manuellen Prozesse durch vordefinierte, getestete und validierte Workflows. So können Sie mit einem Klick einen ganzen Geschäftsprozess, eine Anwendung, eine Datenbank oder ein einzelnes System wiederherstellen. Über diese Workflows werden die verschiedenen erforderlichen Schritte organisiert, um miteinander verbundene Systeme und Daten wiederherzustellen und Benutzerfehler zu begrenzen. Resiliency Orchestration beschleunigt die Implementierung von Lösungen, indem eine umfangreiche Bibliothek mit mehr als 450 vordefinierten Mustern zum Einsatz kommt, die für den Aufbau von Workflows kombiniert werden können.

Cyber Incident Recovery für Plattformkonfigurationen

Geschäfte rund um die Uhr setzen die kontinuierliche Verfügbarkeit der IT-Infrastruktur voraus, die die Grundvoraussetzung für geschäftskritische Anwendungen ist: physische Server, VM-Instanzen (virtuelle Maschinen), Speichersysteme und Netzwerkgeräte. Cyberattacken können Geschäftsprozesse zum Erliegen bringen, wenn Konfigurationsdaten dieser Plattformen beschädigt werden.

Das Plattformkonfigurationsfeature von Cyber Incident Recovery (siehe Abbildung 1) erlaubt die schnelle Wiederherstellung von Services. Dies erfolgt durch die Replizierung einer „Golden Copy“ von Server- und Gerätekonfigurationsdaten in durch Air-gap geschützten, nicht veränderbaren Speicher in einem Cloudobjektspeicher oder einem IBM Rechenzentrum. Produktionsgeräte werden im Detail untersucht, um Änderungen an den Konfigurationsdaten zu erkennen. Das System analysiert dann die Änderung, um festzustellen, ob es eine gültige Änderung ist. Alerts (Benachrichtigungen) werden ausgegeben, wenn es sich um eine verdächtige Änderung an den Konfigurationsdaten handelt. Die Alerts können auch relevante Tickets aus der Änderungsmanagementsoftware bereitstellen.

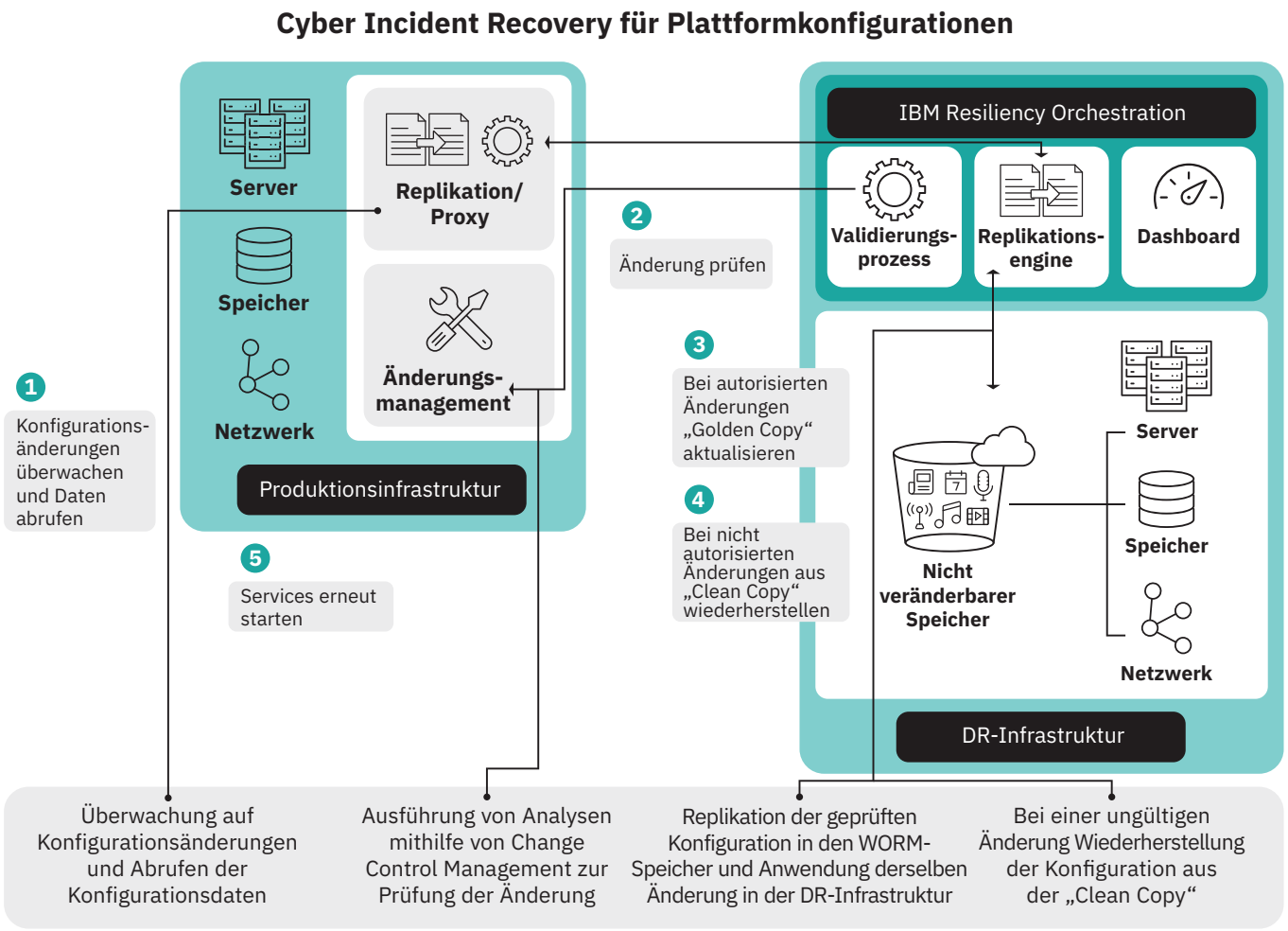

Abbildung 1. Cyber Incident Recovery für Plattformkonfigurationen unterstützt beim Schutz von Konfigurationsdaten von physischen und virtuellen Servern sowie von Speicher- und Netzwerkgeräten.

Handelt es sich um eine gültige Änderung, werden die Konfigurationsdaten durch die Replizierung einer neuen „Golden Copy“ im nicht veränderbaren Speicher geschützt. Wird eine ungültige Änderung festgestellt, wird die neueste Reinkopie der Gerätekonfigurationen von Resiliency Orchestration schnell wieder in die Produktionsinfrastruktur eingespielt. Dies erfolgt auf Basis von Richtlinienvorgaben und mit Zustimmung des Managements. Dedizierte und VM-Konfigurationen werden auf einer sauberen Produktions-infrastruktur wiederhergestellt.

Cyber Incident Recovery für Daten

Das Datenfeature von Cyber Incident Recovery ermöglicht eine äußerst zuverlässige und schnelle Wiederherstellung nach Cyberattacken, durch die die Daten selbst beschädigt wurden. Dabei werden die Daten durch eine Air-Gap und nicht veränderbaren Speicher geschützt. Gleichzeitig kann eine schnelle Wiederherstellung am DR-Standort des Kunden erfolgen.

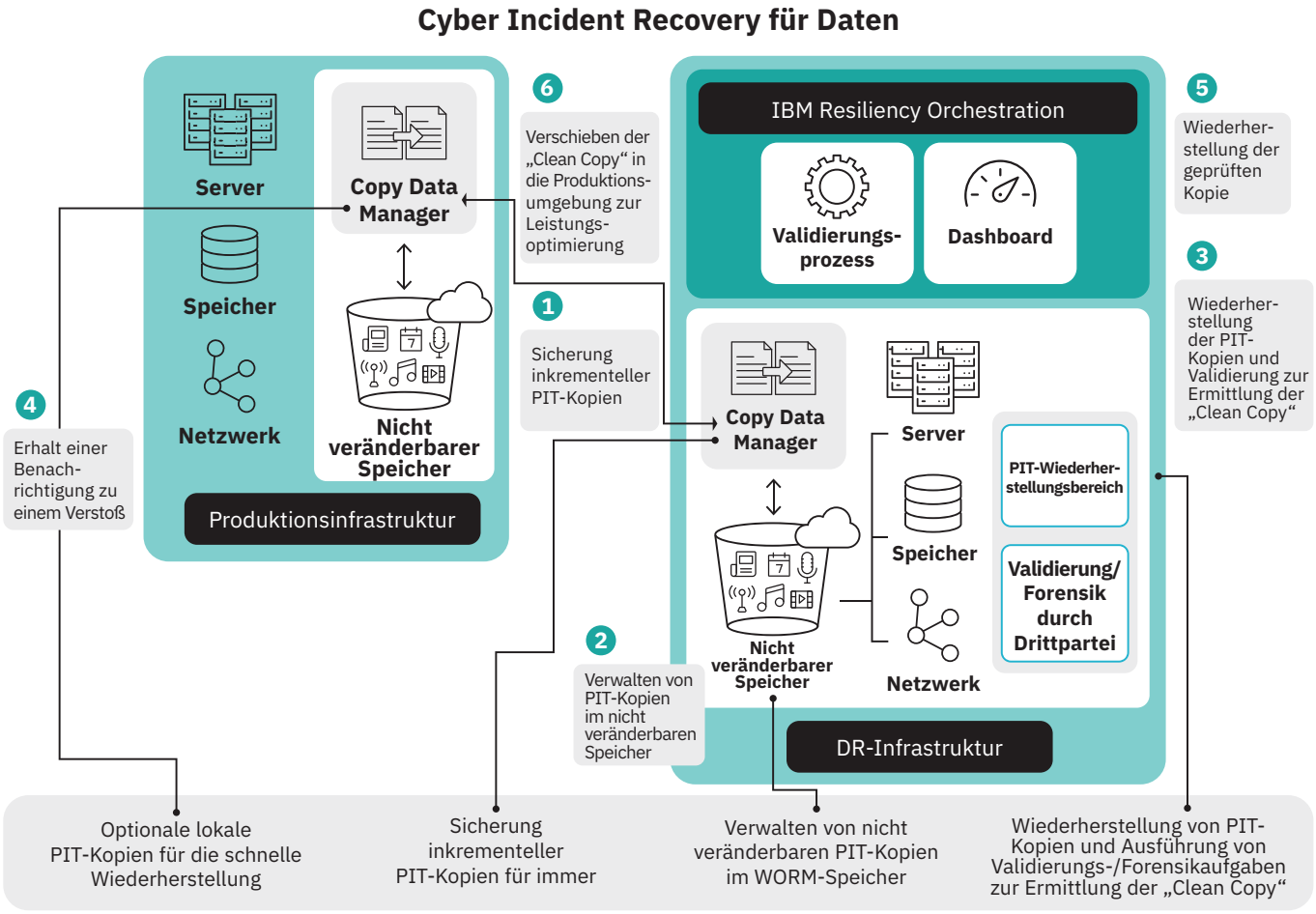

Abbildung 2. Cyber Incident Recovery für Daten ermöglicht die effiziente Sicherung großer Datenmengen sowie unterbrechungsfreie Tests und schnelle Wiederherstellung.

Cyber Incident Recovery ist für die Verarbeitung großer Mengen von Anwendungsdaten ausgelegt. Hierfür kommen Copy Data Management-Technologien zum Einsatz, um inkrementelle PIT-Kopien der Daten zu erstellen und zu verwalten. Da diese Kopien in nicht veränderbarem Speicher wie Cloud-objektspeicher oder Speicher mit WORM-Funktionalität aufbewahrt werden, handelt es sich um „ewige“ Kopien, die nicht geändert werden können. Wie in Abbildung 2 zu sehen, repliziert die Copy Data Management-Software Daten an einen DR-Standort oder alternativen Standort. Dabei werden die PIT-Kopien erstellt. Optional können PIT-Kopien auch am Produktionsstandort erstellt und gespeichert werden, damit eine schnelle Wiederherstellung vorgenommen werden kann.

Wenn ein DR-Manager eine Benachrichtigung zu einer Datenschutzverletzung oder einer Infizierung durch eine Verschlüsselungsmalware erhält, wird am DR-Standort ein automatisiertes Testen von PIT-Kopien durchgeführt, um die Wiederherstellbarkeit der Daten zu überprüfen. Die beim Test- und Prüfprozess ermittelte aktuellste „Clean Copy“ wird dann in der DR-Infrastruktur über den Prozess für schnelle Wiederherstellung der Copy Data Management-Software wiederhergestellt. Die Tests können auch häufiger am DR-Standort erfolgen. So wird die Wiederherstellbarkeit der Daten ohne Beeinträchtigung der Geschäftsoperationen sichergestellt. Mit Resiliency Orchestration lassen sich Plattformen schneller und parallel wiederherstellen.

Einfacheres Management durch Dashboards und Berichte

Cyber Incident Recovery beinhaltet ein Dashboard-Feature (siehe Abbildung 3), mit dem Änderungen an der Plattformkonfiguration und an Daten überwacht werden können. Dieses Feature kann auch wichtige Cyber-Recovery-Updates in Echtzeit für das höhere Management oder den Vorstand bereitstellen, sodass fundierte Entscheidungen schneller getroffen werden können.

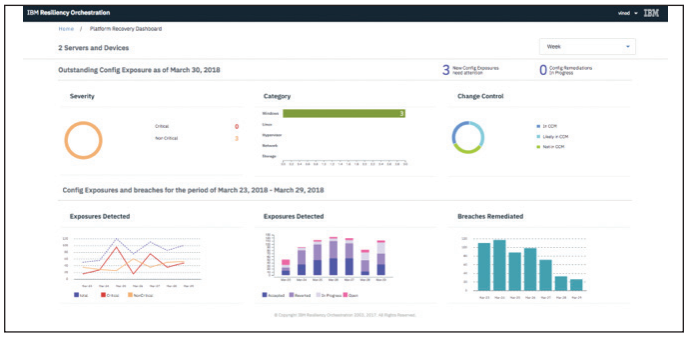

Abbildung 3. Zentrales Dashboard.

Ein Dashboard mit Cybervorfällen enthält Details wie die Anzahl der Sicherheitslücken und den Schweregrad und ermöglicht darüber hinaus die Verfolgung von Sicherheitslücken. Ein Dashboard mit Cyberdaten bietet mehr Einblicke in cyberspezifische RPO-Abweichungen, RTO-Abweichungen, zum Validierungsstatus von Snapshots und zum aktuellen Stand der Cyber-Readiness.

Das integrierte Berichtsmodul bietet eine Vielzahl von Berichten wie zur Ausfallsicherheit bei Cyberattacken oder DR-Daten. Diese Berichte können exportiert und für Compliancezwecke an Regulierungsbehörden weitergeleitet werden. Dies kann auch Diagramme umfassen, die während des normalen Geschäftsbetriebs erfasst werden.

Warum IBM?

Die Spezialisten bei IBM Business Resiliency Services können auf nahezu 60 Jahre Erfahrung zurückblicken, in denen sie Kunden weltweit bei ihren Anforderungen an Sicherung und Wiederherstellung unterstützt haben. Heute profitieren über 9.000 Kunden von unseren DR- und Datenmanagement-Services. Zudem sichern und verwalten wir pro Jahr über 3,5 Exabyte an Daten. Über 300 IBM Resiliency Centers in mehr als 60 Ländern weltweit bieten verwaltete DR- und Datenschutzservices an. Hinzu kommen über 6.000 IBM Experten weltweit, die Sie beim Thema Ausfallsicherheit kompetent unterstützen.

Weitere Informationen

Weitere Informationen zu Cyber Incident Recovery erhalten Sie von Ihrem IBM Ansprechpartner oder auf der folgenden Website: **ibm.com**/services/business-continuity/cyber-resilience

Darüber hinaus hat IBM Global Financing eine Vielzahl von Zahlungsoptionen im Angebot, um Ihnen bei der Anschaffung der richtigen Technologie für mehr Unternehmenswachstum zu helfen. IBM bietet ein vollständiges Lebenszyklusmanagement für IT-Produkte und -Services, vom Kauf bis zur Entsorgung. Weitere Informationen finden Sie unter: **ibm.com**/financing

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustraße 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
ibm.com

Bitte der Wiederverwertung zuführen

89017289-DEDE-02