kyndryl

Ausfallsicherheits-Orchestrierung mit Cyber Incident Recovery

Spezielle Cyber-Resilience-Lösung für die schnelle, zuverlässige und skalierbare Wiederherstellung in Hybrid-Multi-Cloud-Umgebungen

Inhalte

Eine Änderung ist möglicherweise überfällig

Je mehr Ihre Daten und Anwendungen in einer zunehmend vernetzten Infrastruktur, bestehend aus On-Premises-, Public-Cloud- und Multi-Cloud-Umgebungen, übertragen werden, desto mehr Möglichkeiten gibt es für Cyberangreifer, die Kontinuität Ihres Geschäftsbetriebs zu unterbrechen. Die Komplexität von Hybrid-Multi-Cloud-Umgebungen setzt Ihre geschäftskritischen Daten und Systemkonfigurationen einem höheren Risiko als je zuvor aus. Das Risiko ist so hoch, dass die Wahrscheinlichkeit eines erfolgreichen Cyberangriffs zur Gewissheit geworden ist. Ganz gleich, wie wachsam Ihr für die IT-Sicherheit zuständiges Team ist, ein Cyberangriff wird letztendlich zu einer Störung des Geschäftsbetriebs in Form eines Ausfalls, eines Datendiebstahls oder einer Datenkorruption führen, die Ihrem Ruf schadet und finanzielle Folgen hat.

Noch vor nicht allzu langer Zeit konnte man sich darauf verlassen, dass herkömmliche Disaster-Recovery-Lösungen den Schaden der meisten konventionellen Cyberangriffe begrenzten. Doch das war lange, bevor es Hybrid-Multi-Cloud-Umgebungen gab. Während IT-Infrastrukturen komplexer geworden sind, haben auch Cyberangreifer immer ausgeklügeltere Methoden entwickelt. Datenverschlüsselungs- und Malwareangriffe nehmen heute Datensicherungen auf zuvor undenkbare Weise ins Visier. Infolgedessen erhalten die Angreifer Zugang zu Backup- und Disaster-Recovery-Standorten. Dadurch werden sowohl Primär- als auch Sicherungsdaten unbrauchbar und die Wiederherstellung des Produktionsbetriebs verzögert sich erheblich.

Die Kyndryl Ausfallsicherheits-Orchestrierung mit Cyber Incident Recovery minimiert die geschäftlichen Folgen von Cyberangriffen durch die schnelle, zuverlässige und skalierbare Wiederherstellung in Hybrid-Multi-Cloud-Umgebungen.

Spezielle Lösung für die Wiederherstellung nach Cyberangriffen in einer Hybrid-Multi-Cloud-Welt
Die Kyndryl™ Ausfallsicherheits-Orchestrierung mit Cyber-Incident-Recoverykann Ihre Daten und Plattformkonfigurationen bei einem Ausfall infolge eines Cyberangriffs schnell wiederherstellen. Die Lösung sorgt für eine intelligente Automatisierung von Datensicherungs- und Disaster-Recovery-Abläufen und ermöglicht Wiederherstellungs-Tests, die Unveränderbarkeit von Daten, die Erkennung von Anomalien sowie Überwachung, Management und Berichterstellung in Hybrid-Multi-Cloud-Umgebungen. Die Lösung erlaubt die automatisierte, zuverlässige und schnelle Wiederherstellung physischer und virtueller Arbeitslasten, einschließlich Geschäftsprozessen, Anwendungen, Systemen und Datenbanken, nach Cyberangriffen.

Cyber Incident Recovery bietet:
- Einfache Testfunktionalität ohne Auswirkungen auf Produktionsumgebungen
- Schnellere Erkennung von Datenkorruption und schnelle Reaktion zur Reduzierung von Ausfallzeiten
- Effiziente zeitpunktgenaue Wiederherstellung, die RPOs (Recovery Point Objectives) optimiert
- Skalierbarkeit für die umfangreiche Erkennung und Wiederherstellung auf Standortebene innerhalb von Minuten
- Vereinfachte Transparenz und Berichterstellung zur Einhaltung gesetzlicher Bestimmungen

Die Kyndryl Ausfallsicherheits-Orchestrierung mit Cyber-Incident-Recovery ermöglicht die automatisierte, zuverlässige und schnelle Wiederherstellung physischer und virtueller Arbeitslasten nach Cyberangriffen.

Eine Architektur, die eine agile Herangehensweise an Cyber-Resilience ermöglicht

Die technologischen Bausteine, aus denen Cyber Incident Recovery besteht, bieten eine Plattform, die Rechen- und Datenebenen von sowohl Produktions- als auch Disaster-Recovery-Umgebungen umfasst. Dies ermöglicht eine agile Herangehensweise an die Wiederherstellung Ihrer virtuellen und physischen Workloads.

Nicht veränderbarer Speicher
Nicht veränderbarer Speicher für Konfigurationsdaten oder WORM-Speicher (Write Once Read Many) für Anwendungsdaten trägt dazu bei, Datenkorruption zu verhindern und die Wiederherstellbarkeit von Daten zu gewährleisten, da nach dem Speichern keine Änderungen mehr an den gesicherten Daten vorgenommen werden können. Bei Anwendungsdaten lassen sich mit diesem Ansatz die Speicherkosten senken, da nur neue Kopien von zeitpunktgenauen inkrementellen Änderungen in den Speicher geschrieben werden.

Air-Gap-Schutz
Die Netzwerkisolation trennt Produktionsumgebungen vom WORM-Speicher, der die geschützten Sicherungsdaten an einem Remote- oder Disaster-Recovery-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.

Anomalieerkennung
Die Kyndryl Ausfallsicherheits- Orchestrierung beinhaltet eine Anomalieerkennungsfunktion, die regelbasierte Heuristik-Identifikation, erweitert durch künstliche Intelligenz (KI), verwendet.Sie ist auf verschiedene Änderungsmuster bekannter Malware trainiert, erfasst und vergleicht die Änderungsmuster in gesicherten Daten, um die Datenanomalien mit hoher Genauigkeit vorherzusagen. Mit dieser Funktion für die Anomalieerkennung am Disaster-Recovery-Standort können anomale gesicherte Snapshots ermittelt und aus „sauberen“ Kopien wiederhergestellt werden.

Überprüfung von Konfigurationsdaten
Diese Komponente nutzt die integrierte, KI-basierte Funktion für die Anomalieerkennung, um sicherzustellen, dass die gesicherte Konfiguration oder die gesicherten Daten fehlerfrei und wiederherstellbar sind. Dieser in die Ausfallsicherheits-Orchestrierung integrierte Prozess erkennt automatisch, wann Ihre Systemkonfigurationen geändert wurden. Die Ausfallsicherheits-Orchestrierung kann zudem mit den vom Kunden bereitgestellten Scripts zur Anwendungsvalidität kombiniert werden, um Tests auf Anwendungs- und Datenebene zu ermöglichen.

Automatisierung und Orchestrierung
Durch die Automatisierung des gesamten Wiederherstellungsprozesses für Daten und Anwendungen 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 Arbeitsabläufe werden die verschiedenen erforderlichen Schritte koordiniert, um miteinander verbundene Systeme und Daten wiederherzustellen und Benutzerfehler zu begrenzen. Resiliency Orchestration beschleunigt die Implementierung von Lösungen mit einer umfangreichen Bibliothek mit mehr als 800 vordefinierten Mustern, die für die Erstellung von Arbeitsabläufen kombiniert werden können.

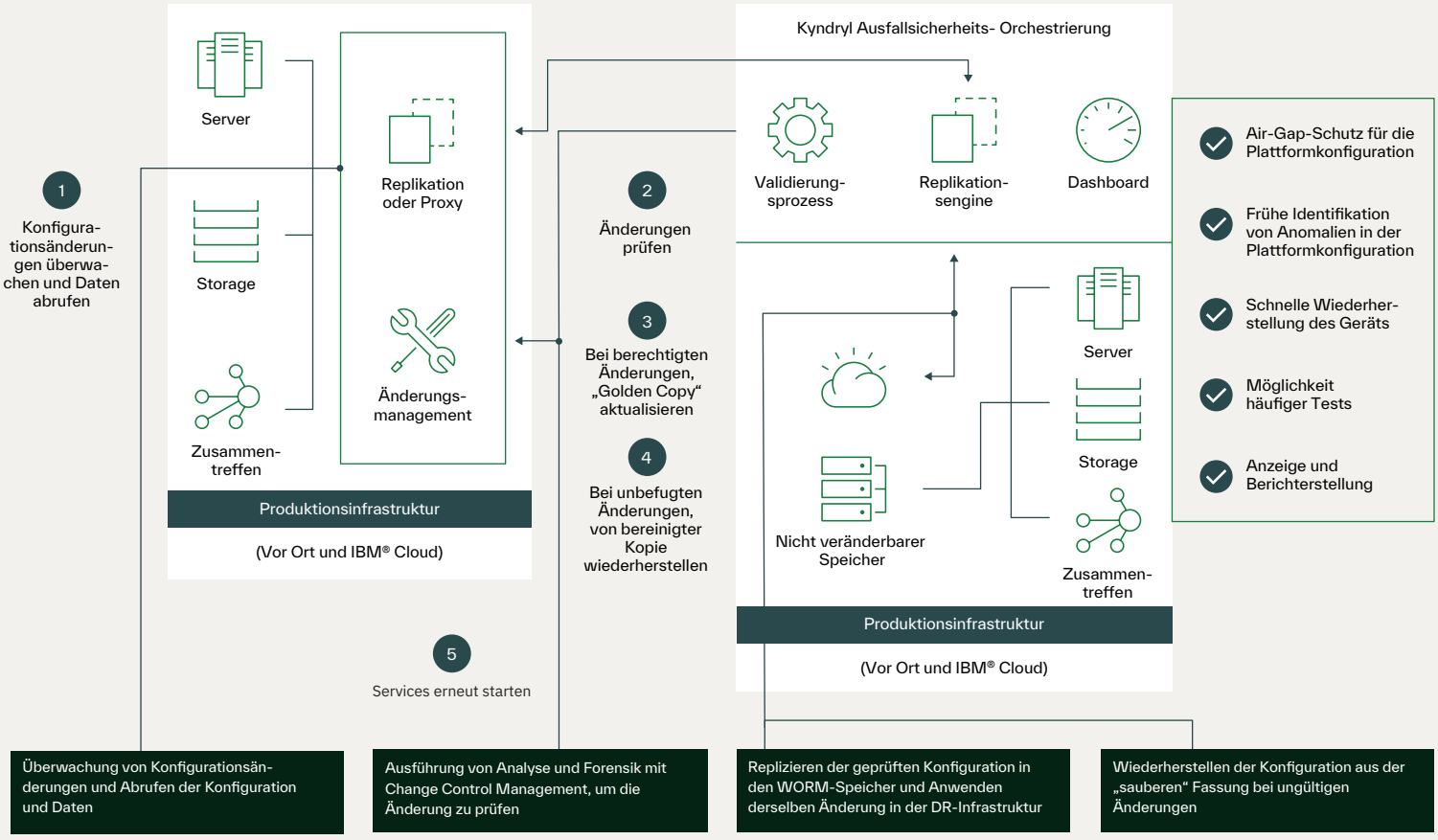
Cyber Incident Recovery für die Plattformkonfiguration

Häufig ändert Malware die Konfigurationen, bevor sie die Daten selbst beschädigt. Deshalb ist es von entscheidender Bedeutung, jegliche Konfigurationsänderungen zu erkennen, bevor die eigentlichen Daten infiziert werden. Das Feature für die Plattformkonfiguration von Cyber Incident Recovery schützt Konfigurationsdaten virtueller und physischer Workloads, Anwendungen, Speichersysteme und Netzwerkgeräte in On-Premises-, Public-Cloud-, Hybrid-Cloud- und Multi-Cloud-Umgebungen.

Aufrechterhaltung des Geschäftsbetriebs mit einer „Golden Copy“
Diese Komponente nutzt die integrierten Technologien, um Änderungen in Endgerätekonfigurationen in der Produktionsumgebung zu erkennen, und benachrichtigt den Benutzer bei jeder berechtigten und nicht berechtigten Änderung. Die Benachrichtigungen (Alerts) können auch relevante Tickets aus der Change-Control-Management Software bereitstellen. Um eine schnelle Wiederherstellung von Services zu ermöglichen, repliziert Cyber Incident Recovery eine „Golden Copy“ der Server- und Gerätekonfigurationsdaten in nicht veränderbarem Speicher mit Air-Gap-Schutz.

Reaktion auf ungültige und gültige Konfigurationsänderungen
Im Falle einer gültigen Änderung werden die Konfigurationsdaten durch Replikation einer neuen „Golden Copy“ auf unveränderliche Speicher geschützt. Wird eine ungültige Änderung identifiziert, werden die zuletzt sauberen Kopien der Gerätekonfigurationen durch Resiliency Orchestration schnell auf der Produktionsinfrastruktur wiederhergestellt, basierend auf vorher festgelegten Richtlinien und mit der entsprechenden Management Zustimmung. Dedizierte und VM-Konfigurationen werden in einer sauberen Produktionsinfrastruktur wiederhergestellt. Im Fall gültiger Änderungen wird eine neue „Golden Copy“ in einem nicht veränderbaren Speicher erstellt.

Kyndryl Cyber-Wiederherstellung als Service
Cyber Incident Recovery für Plattformkonfigurationen



*Air-Gap wird nicht unterstützt für unveränderlichen Speicher, der in der Cloud gehostet wird

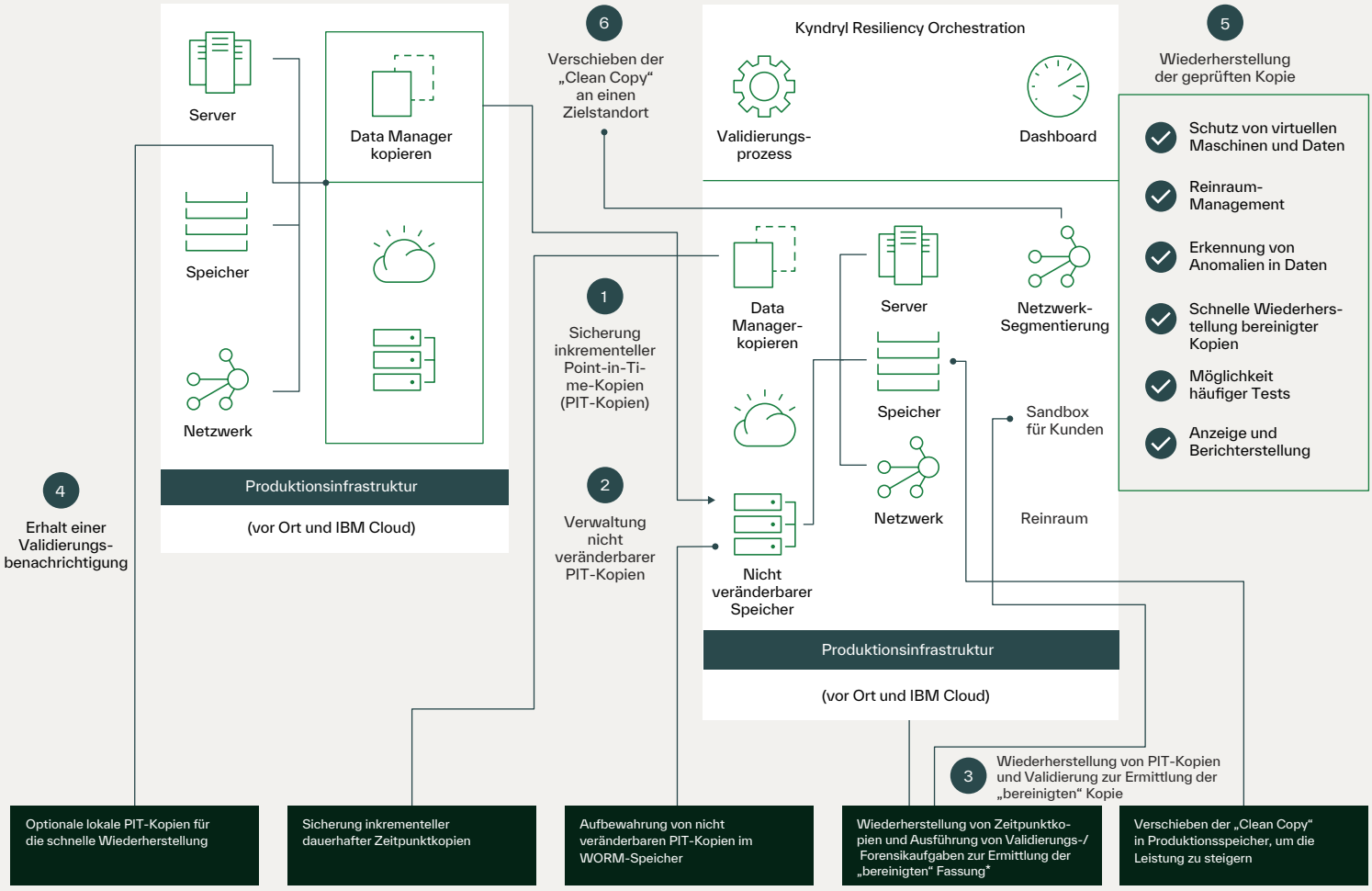
Cyber Incident Recovery für Daten

Das Datenfeature von Cyber Incident Recovery ermöglicht eine äußerst zuverlässige und schnelle Wiederherstellung nach Cyberattacken, durch die die Daten selbst beschädigt wurden. Es schützt die Daten mit Air-Gap-Schutz und nicht veränderbarem Speicher und koordiniert die schnelle Wiederherstellung am Disaster-Recovery-Standort.

Schutz großer Datenmengen in jeder Umgebung
Cyber Incident Recovery ist für die Verarbeitung großer Mengen von Anwendungsdaten ausgelegt, unabhängig davon, wo diese sich befinden. Die Lösung nutzt Copy-Data-Management-Technologie, um inkrementelle zeitpunktgenaue Datenkopien (Point-in-Time-Kopien) 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 dauerhafte Kopien, die nicht geändert werden können. Die Copy-Data-Management-Software repliziert Daten an einem Disaster-Recovery- oder alternativen Standort und erstellt dabei die Point-in-Time-Kopien (PIT-Kopien). PIT-Kopien können auch am Produktionsstandort erstellt und gespeichert werden, um eine schnelle Wiederherstellung zu ermöglichen.

Schnelle Reaktion auf Cyberangriffe zur Aufrechterhaltung des unterbrechungsfreien Geschäftsbetriebs
Wenn ein Disaster-Recovery-Manager über eineDatensicherheitsverletzung oder eine Infektion mit Verschlüsselungs-Malware informiert wird, werden am Disaster-Recovery-Standort automatisierte Tests der PIT-Kopien durchgeführt, um die Wiederherstellbarkeit der Daten zu überprüfen. Die bei diesem Test- und Prüfprozess ermittelte neueste „saubere“ Kopie (Clean Copy) wird dann in der Disaster-Recovery-Infrastruktur durch die Resiliency Orchestration-Software wiederhergestellt. Die Tests am Disaster-Recovery-Standort können auch regelmäßig durchgeführt werden. So lässt sich die Wiederherstellbarkeit der Daten ohne Beeinträchtigung des Geschäftsbetriebs sicherstellen. Mit Resiliency Orchestration lassen sich Plattformen schnell und parallel wiederherstellen.

Kyndryl Cyber Recovery as a Service
Cyber Incident Recovery für Daten



Dashboards und Berichte für ein einfacheres Management

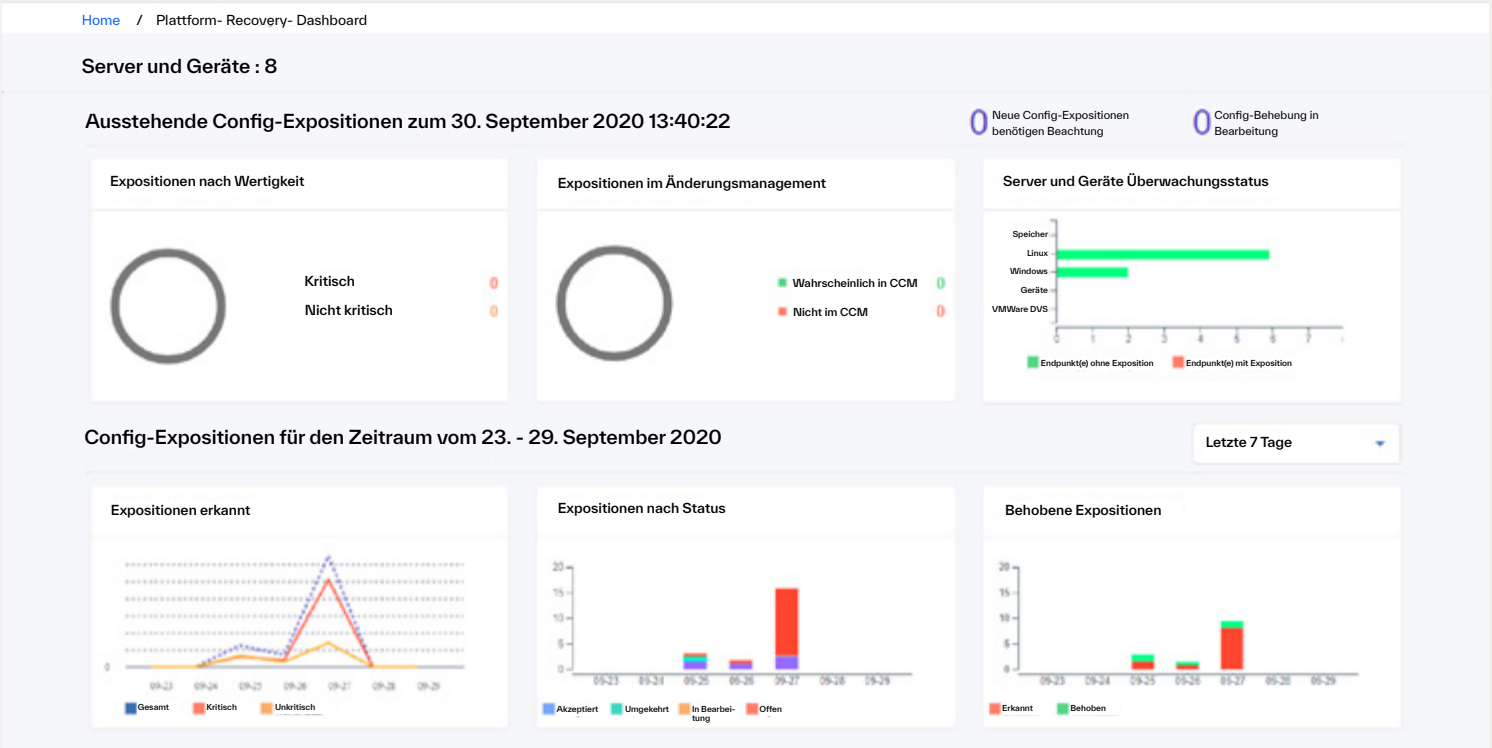
Das in Cyber Incident Recovery enthaltene Dashboard vereinfacht das Management der Wiederherstellung nach Cyberangriffen und die Überwachung von Änderungen an der Plattformkonfiguration und an Daten. Es bietet Einblick in Echtzeit in Abweichungen bei RPOs (Recovery Point Objectives) und RTOs (Recovery Time Objectives), den Snapshot-Prüfstatus und wichtige Updates zur Wiederherstellung nach Cyberangriffen.

Währenddessen kann die Geschäftsleitung oder der Vorstand wichtige Updates zur Wiederherstellung nach Cyberangriffen in Echtzeit erhalten und so schneller fundiertere Entscheidungen treffen.

Bessere Verfolgung von Sicherheitslücken und größere Transparenz
Das Dashboard in Cyber Incident Recovery zeigt Ihnen die Anzahl der Sicherheitslücken in Ihren Umgebungen und ihren jeweiligen Schweregrad an. Sie können offene Sicherheitslücken überwachen und Entscheidungen auf der Basis von Informationen zu RPO- und RTO-Abweichungen bei Cyberangriffen, zum Snapshot-Prüfstatus und zum aktuellen Stand der Vorbereitungen auf Cyberangriffe treffen.

Zuverlässige Berichtsfunktionalität
Das integrierte Berichtsmodul bietet eine Vielzahl von Berichten, darunter zum Cyber-Resilience- oder Disaster-Recovery-Status. Diese Berichte können zu Compliance-Zwecken exportiert und Regulierungsbehörden zur Verfügung gestellt werden, neben Diagrammen, die während des normalen Geschäftsbetriebs erfasst werden.

Cyber Incident Recovery liefert Einblick in Echtzeit in RPO- und RTO-Abweichungen, den Snapshot-Prüfstatus und wichtige Updates



Kyndryl Business Resiliency Services hilft Kunden in aller Welt, ihre Sicherungs- und Wiederherstellungsbedürfnisse zu erfüllen, und kann sich dabei auf jahrzehntelange Erfahrung stützen.

Kyndryl Vorteil
- Kompetenz im Bereich des gesamten Lebenszyklus der Ausfallsicherheit
- Automatisierte Wiederherstellung physischer, virtueller und Cloud-basierter Workloads
- Mehr als 800 vordefinierte Muster für eine schnellere, effiziente Implementierung und Skalierbarkeit
- Auswahl an Clouds, einschließlich AWS, Azure und IBM Cloud zur Skalierbarkeit im Unternehmen

Bewährt
- Über 9.000 Kunden werden durch Kyndryl Disaster-Recovery- und Datenmanagement-Services geschützt
- Kyndryl sichert und verwaltet mehr als 3,5 Exabyte an Daten pro Jahr

Globale Präsenz
- Es gibt über 300 IBM Resiliency-Center in mehr als 50 Ländern
- IBM setzt mehr als 6.000 Experten weltweit speziell für Resilience ein.

Warum Kyndryl?

Kyndryl hat langjährige Erfahrung in der Entwicklung, dem Betrieb und der Verwaltung der modernsten, effizientesten und zuverlässigsten Technologie-Infrastruktur, auf die die Welt täglich angewiesen ist. Wir engagieren uns sehr für die Weiterentwicklung der kritischen Infrastruktur, die den menschlichen Fortschritt antreibt. Wir bauen auf unserem Fundament exzellenter Kompetenz auf, indem wir Systeme auf neue Art und Weise schaffen: Wir holen die richtigen Partner ins Boot, investieren in unser Geschäft und arbeiten Seite an Seite mit unseren Kunden, um Potenziale zu erschließen.

Sie möchten mehr erfahren?

Um weitere Informationen darüber zu erhalten, was Kyndryl Resiliency Orchestration mit Cyber Incident Recovery für Sie tun kann, kontaktieren Sie bitte Ihren Kyndryl-Ansprechpartner oder besuchen Sie www.kyndryl.com.

kyndryl

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

Hergestellt in den USA
Juli 2021