kyndryl

16. Tagung GSE Arbeitskreis
Business Continuity Management

Marlin Stankusch
Senior Lead Consultant Security & Resiliency
Kyndryl Consult

Resiliency Orchestration

05.12.2023

Kyndryl Übersicht

Der größte IT-Service Anbieter der Welt

Als unabhängiges Unternehmen betreibt und modernisiert Kyndryl kritische IT-Infrastrukturen und bietet die fortschrittlichsten Lösungen auf dem Markt an, die auf die jeweilige Situation des Kunden zugeschnitten sind

- Betrieb in 63 Ländern seit mehr als 30 Jahren (Kyndryl war zuvor Teil von IBM-GTS)
- 90 000 Mitarbeiter mit durchschnittlich 10+ Jahren an Erfahrung an
- $18.5 Milliarden Umsatz und “Trusted Advisor” für mehr als 4,000 Kunden

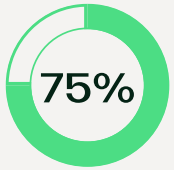
Kyndryl Portfolio

- End-to-End-Unterstützung von der strategischen Beratung bis zur Implementierung mit Kyndryl Consult-Projekten und Full Managed Services von Kyndryl Managed
- Sechs Practices für Technologien:

Cloud Services	Digital Workplace
Core Enterprise Infrastructure	Security & Resiliency
Managed ERP, Data & AI	Network Services & Edge

Unsere Kunden

4,000 ...globale Kunden inkludiert:



... der Fortune 100 und mehr als die Hälfte der Fortune 500

Unsere Kunden in Deutschland:

Deutsche Bank, Allianz, BMW, Volkswagen, symrise, Universitätsmedizin Mainz, Hapag-Lloyd, Lufthansa, Henkel, OSRAM, B|BRAUN

... & viele andere große deutsche Konzerne und Unternehmen des gehobenen Mittelstandes

Unsere Unterscheidungsmerkmale

Lokal & Agil	Die Aufteilung in länderspezifische Kyndryl-Einheiten führt zu schnelleren Entscheidungen und Kundenzentrierung. Das globale Netzwerk ermöglicht es uns, große, komplexe IT-Umgebungen als One-Stop-Shop zu betreiben.
Flexibilität & Zuverlässigkeit	8 von 10 Verträgen, die seit unserer Ausgründung unterzeichnet wurden, beinhalten ein flexibles As-a-Service-Modell mit branchenführenden NPS-Bewertungen.
Umfassendes Ökosystem	Wir bieten jahrzehntelange Erfahrung im Betrieb von IT-Infrastrukturen. Wir sind völlig unabhängig in den Lösungen, die wir implementieren und haben enge Partnerschaften mit Microsoft, AWS, ServiceNow und vielen anderen
Flexible & AI-basierte Lösungen	Bei 83 % unserer Projekte erfolgt die Bereitstellung ohne Eingriffe. Wir arbeiten mit konstant hohen Kundenbewertungen bei der Erbringung unserer Dienstleistungen - 26 % Prozentpunkte höher als der nächste Wettbewerber

Warum Resilienz?

Eine Vielzahl von äusseren Einflüssen erfordert eine a… Geschäftsmodell abge…

- Naturkatastrophen

UMWELT

Flugverkehr lahmgelegt: V… Jahren brachte isländische… tagelangen Stillstand

Von chz/dpa · 13 April, 2020 · Burda

…jallajökull -Gletscher stößt eine riesige Aschewolke aus.

…s/2020-04-13-flugverkehr-lahmgelegt-vor-zehn-jahren-brachte-islandischer-vulkan

Unwetter verursacht Milliardenschäden

Stand: 18.05.2023 17:47 Uhr

Einen Tag nach den schweren Regenfällen in Italien mit mindestens 13 Toten zeichnet sich das Ausmaß der Zerstörung ab. Die Schäden liegen laut Regionalpolitikern in Milliardenhöhe. Das Auswärtige Amt gab eine Reisewarnung heraus.

https://www.tagesschau.de/ausland/europa/italien-schaeden-ueberschwemmung-100.html

STÄRKE 6,8

Schweres Erdbeben erschüttert Taiwan

AKTUALISIERT AM 19.09.2022 - 10:19

In Taiwan hat ein schweres Erdbeben Häuser und Brücken einstürzen lassen und weitere Schäden verursacht. Nach bisherigen Angaben ist ein Mensch ums Leben gekommen.

https://www.faz.net/aktuell/gesellschaft/ungluecke/taiwan-schweres-erdbeben-der-staerke-6-8-18324962.html

Wegen des Erdbebens in Taiwan: Auftragsfertiger TSMC warnt doch vor Produktionsausfällen

Nachdem es zunächst hieß, der Auftragsfertiger sei von der Naturkatastrophe nicht tangiert, muss er nun doch Probleme einräumen. Beim kommenden "iPhone 7" ist TSMC angeblich einziger Chipproduzent.

https://www.heise.de/news/Wegen-des-Erdbebens-in-Taiwan-Auftragsfertiger-TSMC-warnt-doch-vor-Produktionsausfaellen-…

Warum Resilienz?

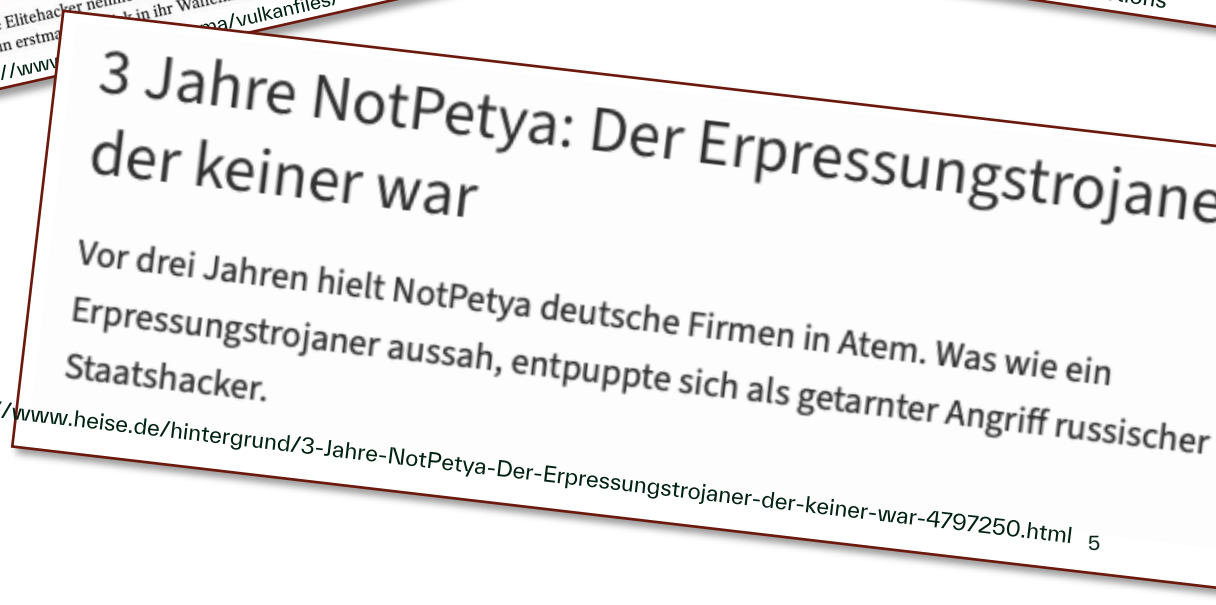
Eine Vielzahl von äusseren Einflüssen erfordert eine auf das Geschäftsmodell abgestimmte Resilienz

- Naturkatastrophen
- Großereignisse

Warum Resilienz?

Eine Vielzahl von äusseren Einflüssen erfordert eine auf das Geschäftsmodell abgestimm

- Naturkatastrophen
- Großereignisse
- Konflikte, Kriegswaffen & Organisiertes Verbrechen



Agenda

01 Einleitung

02 Disaster Recovery vs. Cyber Incident Recovery

03 Recovery Orchestration

04 Ein möglicher Fahrplan zur Umsetzung

05 Ransomware Angriff

kyndryl

Das Risiko disruptiver Cyber-Bedrohungen nimmt zu

Die kontinuierliche Modernisierung und der Zustrom neuer Technologien in den letzten Jahren haben die Angriffsfläche für Unternehmen vergrößert und Sie angreifbarer gemacht.

Die Verwaltung und Sicherung Ihrer Unternehmensdaten und -anwendungen ist eine Herausforderung, da Ihr Unternehmen mit einem erhöhten Risiko von Cyber-Bedrohungen, steigenden Datenschutzkosten und sich ändernden Vorschriften konfrontiert ist.

85%

85 % der Unternehmen wurden im Jahr 2023 durch mindestens einen Cyberangriff kompromittiert, während 39 % mehr als sechsmal kompromittiert wurden.[1]

1. CyberEdge 2023 Cyberthreat Defense Report

All Industry Key Findings

Ransomware-Studie: Nur wenige Unternehmen können Daten nach einer Attacke wiederherstellen, ohne Lösegeld zu zahlen

69%

der Befragten gaben an, dass sie im vergangenen Jahr von einem erfolgreichen Ransomware-Angriff betroffen waren

68%

Unternehmen, die sich nach einem erfolgreichen Ransomware-Angriff für die Zahlung eines Lösegelds entschieden haben

50%

Unternehmen gaben an, dass sie eine Betriebsunterbrechung von einer Woche oder mehr hatten

91%

der Befragten, die im vergangenen Jahr ein Lösegeld gezahlt haben, gaben an, dass Daten exfiltriert wurden, wobei 47 % angaben, dass vertrauliche/geheime Daten exfiltriert wurden

46%

gaben an, dass die Angreifer versuchten, ihre Backups anzugreifen, und in 45 % dieser Fälle waren die Angreifer erfolgreich.

Nur 28%

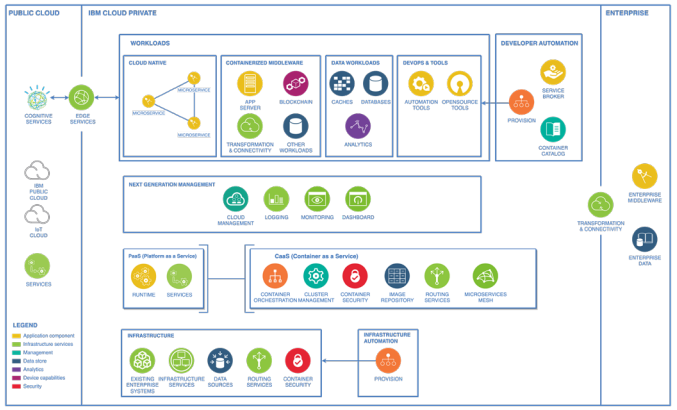
Unternehmen gaben an, dass sie ihre verschlüsselten Daten nach einem Ransomware-Angriff ohne Zahlung eines Lösegelds aus ihrem Backup wiederherstellen konnten

kyndryl

Source: Ransomware Study: Few Organizations Can Recover Data from an Attack Without Paying Ransom, IDC White Paper, sponsored by Kyndryl, based on survey of 928 respondents across industries and geographies (Doc ID : US51195823), November 2023

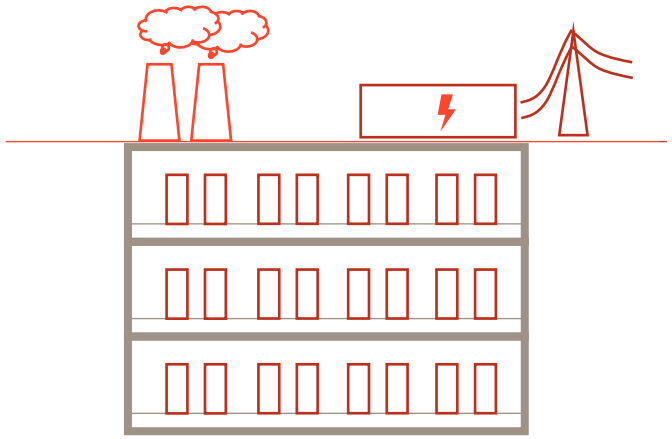
Cyber Incident vs. Diaster

- Desaströse Auswirkungen haben beide
- Cyber Incident betrifft Daten und Software
- Cyber Incident ist nicht lokal oder regional begrenzt
- Disaster betrifft die physische Umgebung
- Disaster ist lokal/regional begrenzt



- **Datastores**
  - Fileserver
  - Backup repositories
  - Disks
  - Removable media
- **Applications**
  - Software packages
  - Installation repositories
  - Build services and code
- **Infrastructure**
  - Virtualization
  - Configuration

CI
DATEN
Wiederherstellen



- **Facilities**
  - Datacenter
  - Offices
  - Production sites
- **Grid/Emergency Power**
- **Cooling**
- **IT Hardware**
  - Server
  - Network
  - Storage
- **People**

DR
INFRASTRUKTUR
Neu aufbauen

kyndryl

Cyber Incident vs. Diaster

Aufgrund der unterschiedlichen Schadensbilder gibt es verschiedene Anforderungen an CI und DR-Standorte

CI-Standorte:

1. „gute“ Backups erkennen
2. unveränderlichem Speicher
3. Abgetrennt vom Produktionsstandort

DR-Standorte:

1. ausreichend Rechenleistung bereitstellen
2. Ausweichbüros bereitstellen
3. Produktionsstandorten permanent verbunden

kyndryl

- **Datastores**
  - Fileserver
  - Backup repositories
  - Disks
  - Removable media
- **Applications**
  - Software packages
  - Installation repositories
  - Build services and code
- **Infrastructure**
  - Virtualization
  - Configuration

CI
DATEN
Wiederherstellen

Cyber Resiliency Architecture

- Air gap
- CIR Handbücher
- Unveränderliche Backup Daten
- Malware und Erkennung von korrupten Daten im Backup
- Laaange Aufbewah-rungszeiten (>90 Tage)

- **Facilities**
  - Datacenter
  - Offices
  - Production sites
- **Grid/Emergency Power**
- **Cooling**
- **IT Hardware**
  - Server
  - Network
  - Storage
- **People**

DR
INFRASTRUKTUR
Neu aufbauen

Disaster Recovery Architecture

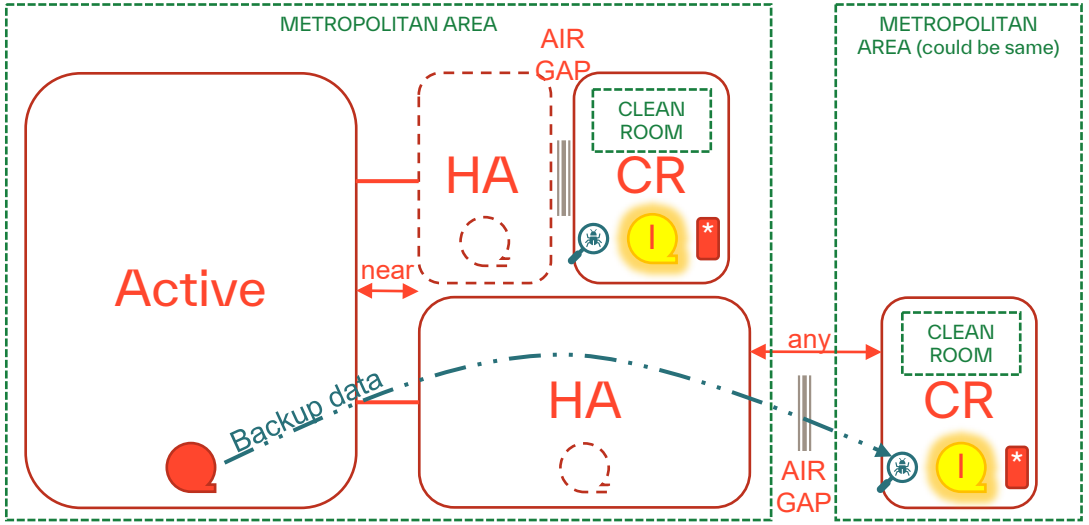
- Ausreichende Rechenleistung für DR relevante Anwendungen
- Ausweichbüros
- DR Handbücher
- Vorbereitete Produktionsdaten (mirroring)

Cyber Incident vs. Diaster

Zusammenfassend:

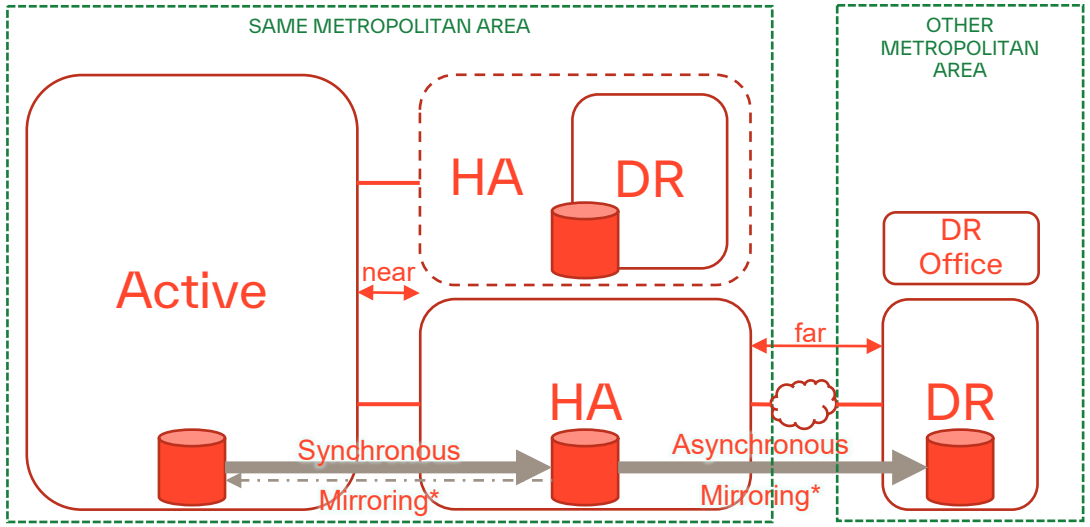
- CI-Standorte sollten via Air-GAP von der Produktionsumgebung getrennt sein
- Datensicherungen auf unveränderlichem Speicher ablegen
- Lange Aufbewahrungszeiten der Backups

CI
DATA
Wiederherstellen



* Separate Backup Infrastruktur zur Analyse der neu erstellten Sicherungen und zur Ablage “unauffälliger” Backups auf unveränderlichem Speicher

DR
INFRASTRUCTURE
Neu aufbauen

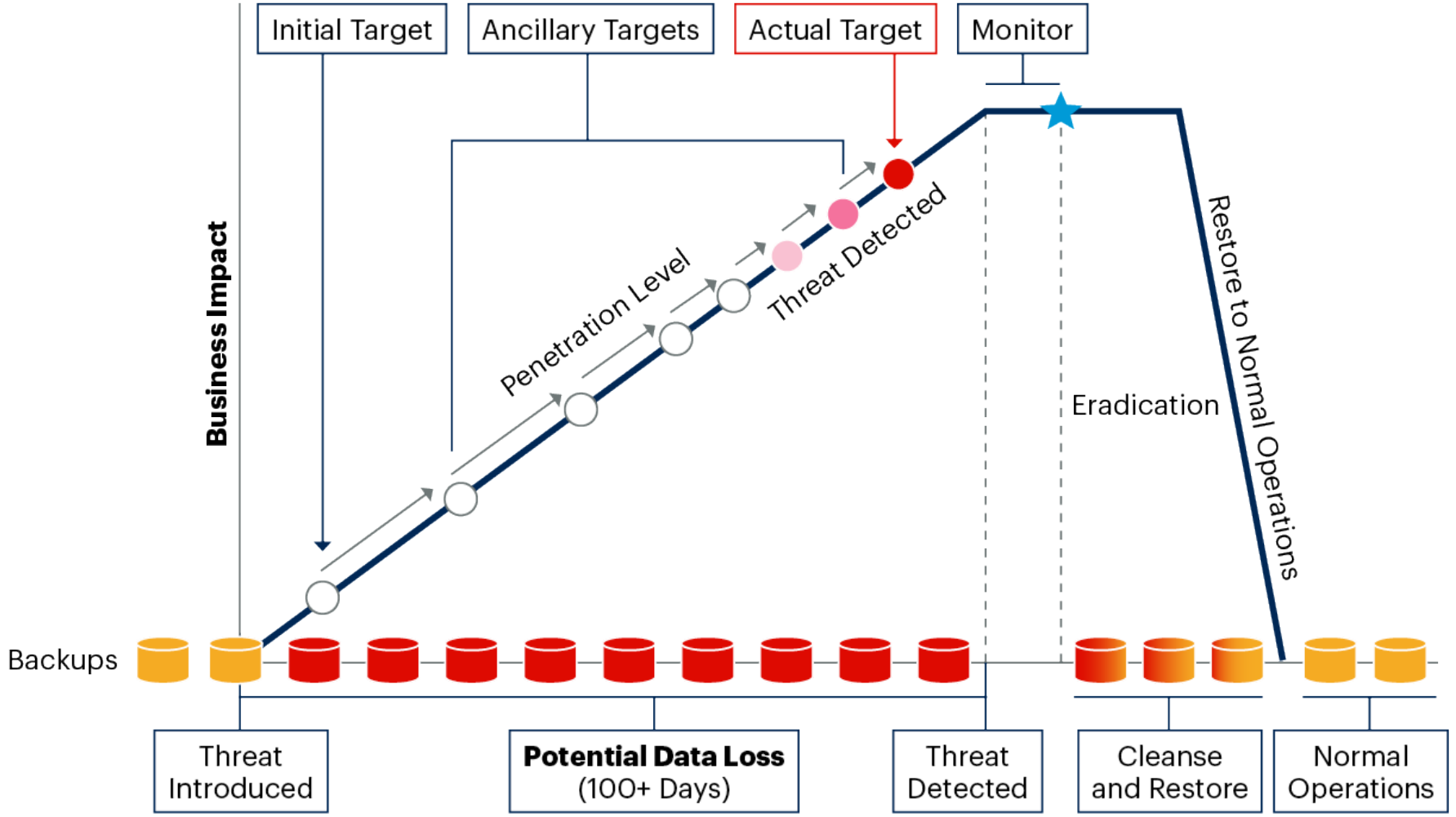


* Synchrone Spiegelung unterbricht die Datenverarbeitung bis der Schreibzugriff auf der entfernten Seite bestätigt ist. Asynchrone Spiegelung unterbricht die Datenverarbeitung bis der Schreibzugriff an die entfernte Seite gesendet wurde.

kyndryl

Ein sauberes Backup ist Schlüssel zum Erfolg

Auswirkungen einer Cyber Attacke auf Datensicherungen



Source: Gartner; 2022

Agenda

01 Einleitung

02 Disaster Recovery vs. Cyber Incident Recovery

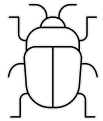
03 Recovery Orchestration

04 Ein möglicher Fahrplan zur Umsetzung

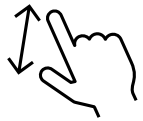
05 Ransomware Angriff

Bisher gelebte DR Ansätze helfen bei einem Cyber Incident nur begrenzt

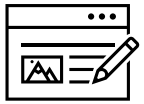
Herausforderung heterogene DR Umgebungen mit unterschiedlichen Replikationsmechanismen in hybriden Infrastrukturen zu managen



Keine Fähigkeiten Cyber Incident Recovery Programme zu managen



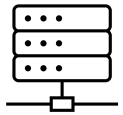
Minimal Sichtbarkeit der RTO und RPO im täglichen Betrieb



Manuelle, fehleranfällige DR Prozesse und run-books

Komplexe Umgebungen und deren Handling führen zu langen Recovery Zeiten und hoher Arbeitsbelastung

Manuelle DR tests/drills und Auswertungen



Traditionelle DR Ansätze haben eine IT Infrastruktur lastige Sichtweise, Recovery aus dem BackUp wird in der Regel nicht getestet

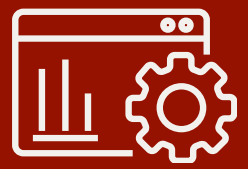
kyndryl

Kyndryl Best Practices

Cyber Resilience ist die Fähigkeit, IT Systeme vor Cyber Angriffen zu schützen und sie nach einem Angriff schnell wieder bereitstellen zu können

Maßnahmen zur Umsetzung von Cyber Resiliency

I
Orchestration and Automation



II
Air-gapped Protection

III
Immutable Storage

IV
PIT copies and Data Verification

V
Regulatory Reporting and Assurance

Kyndryl Best Practices in einem herstellerübergreifenden Umfeld

Kyndryl bietet die Möglichkeit, Best Practices für Cyber Resilience mit einer Vielzahl von Sicherungs- und Speicherlösungen zu implementieren. Orchestrierung/Automatisierung und Berichterstattung werden von der Lösung Resiliency Orchestrator abgedeckt.

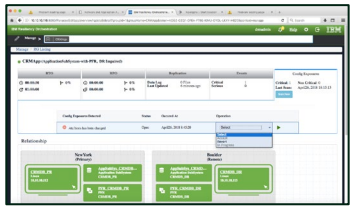
I
Orchestration and Automation

II
Air-gapped Protection

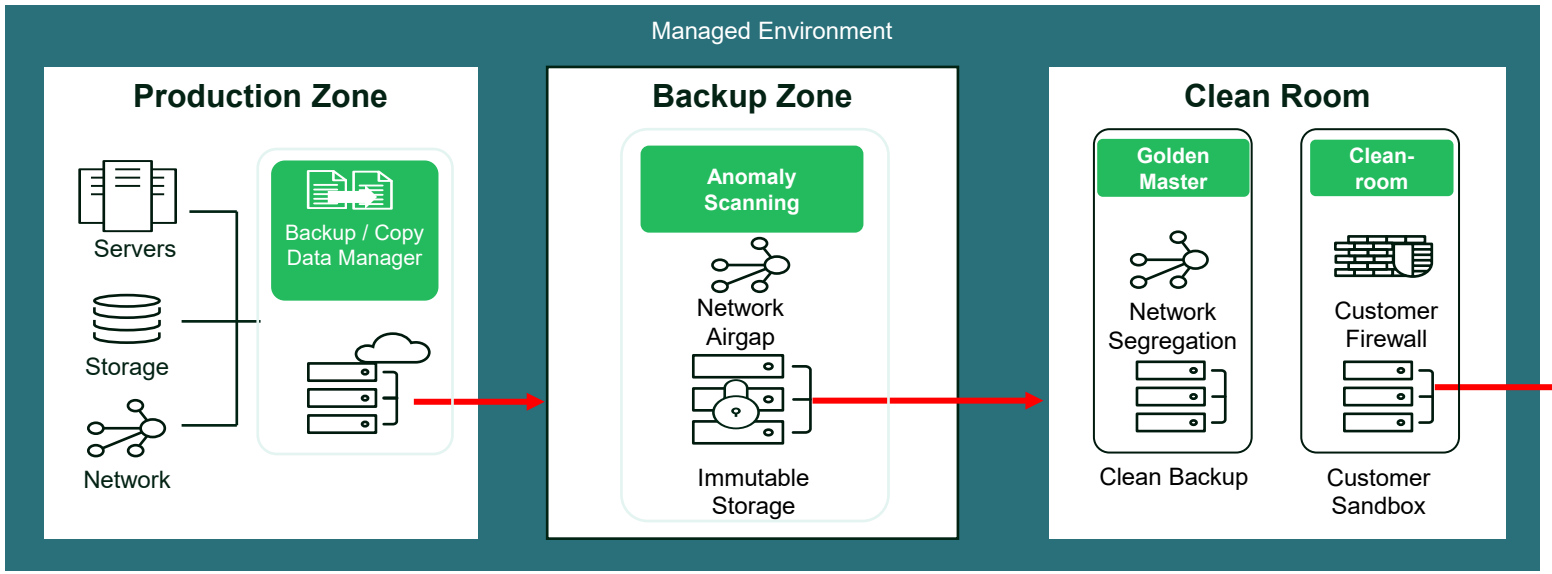
III
Immutable Storage

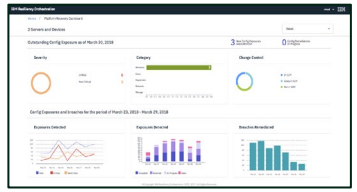
IV
PIT copies and Data Verification

V
Regulatory Reporting and Assurance



Workflow Engine



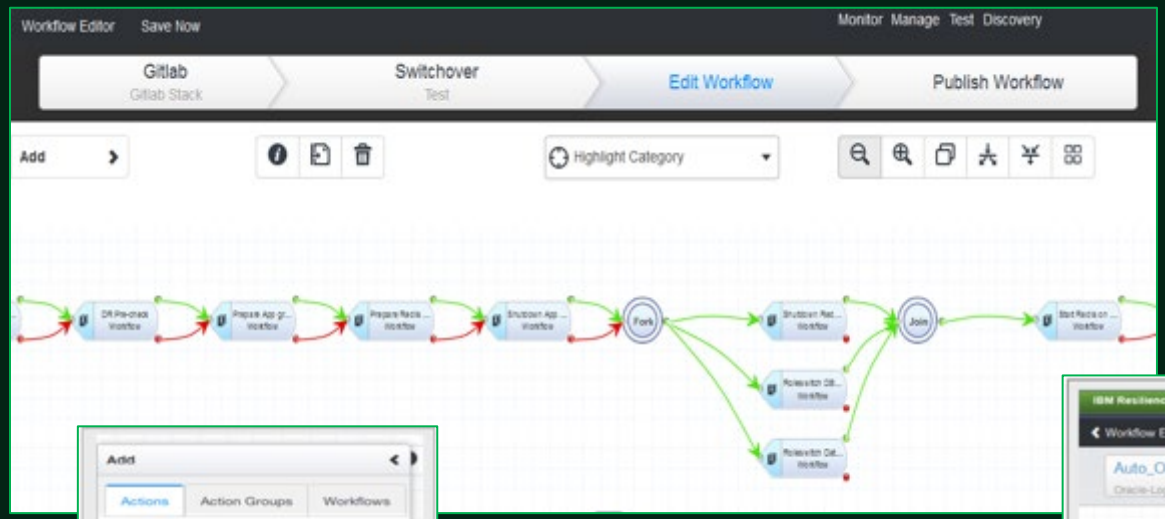


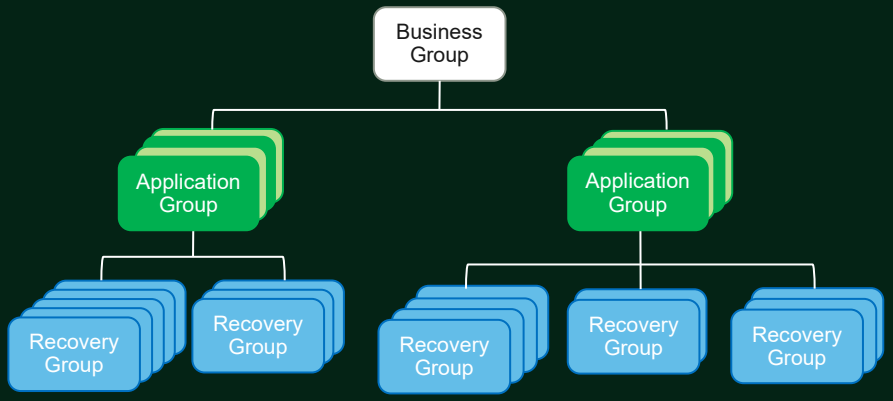
Report Dashboard

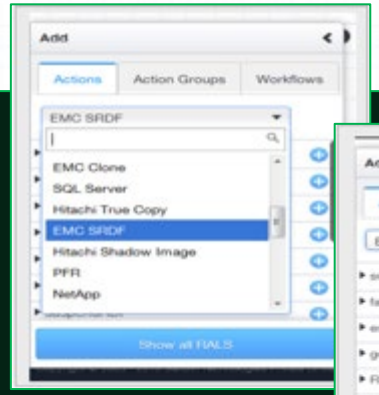
Move clean copy to target location

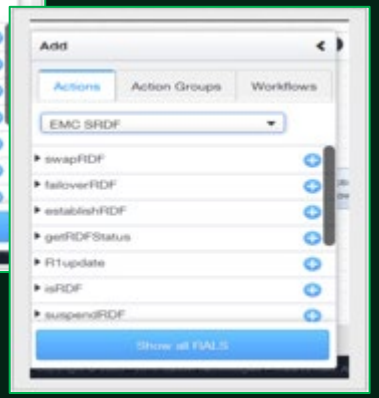
Orchestriertes Testen und Bereitstellen der Recovery Fähigkeiten

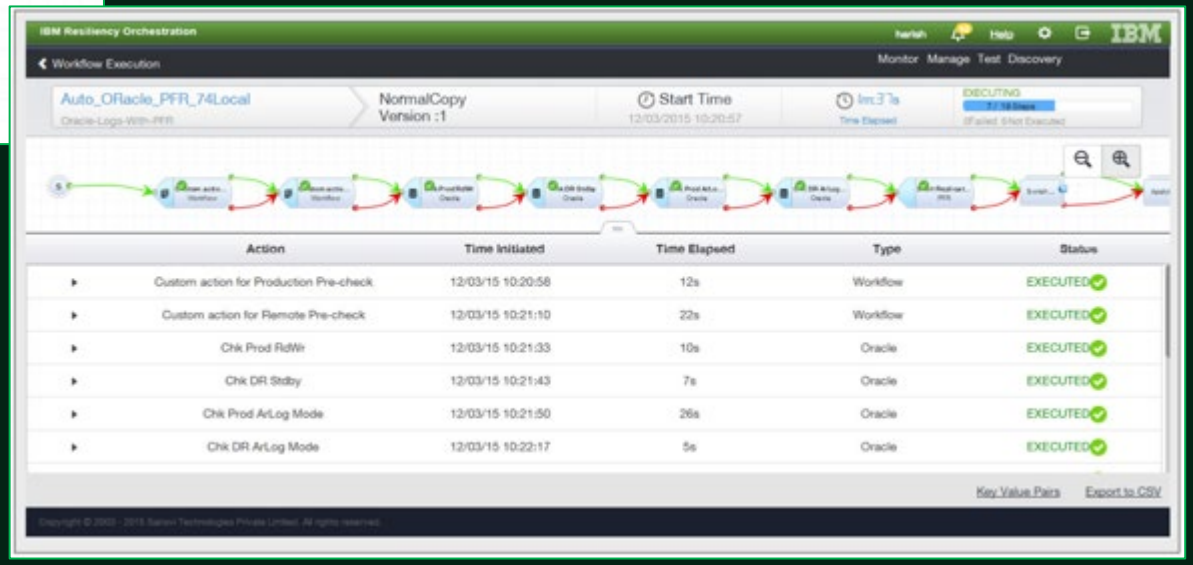
Über heterogene Systems Landschafen für eine zuverlässige, schnelle und fehlerfreie Recovery mit leistungsfähigen Recovery-Workflow Mechanismen und 835+ vor-definierten Pattern



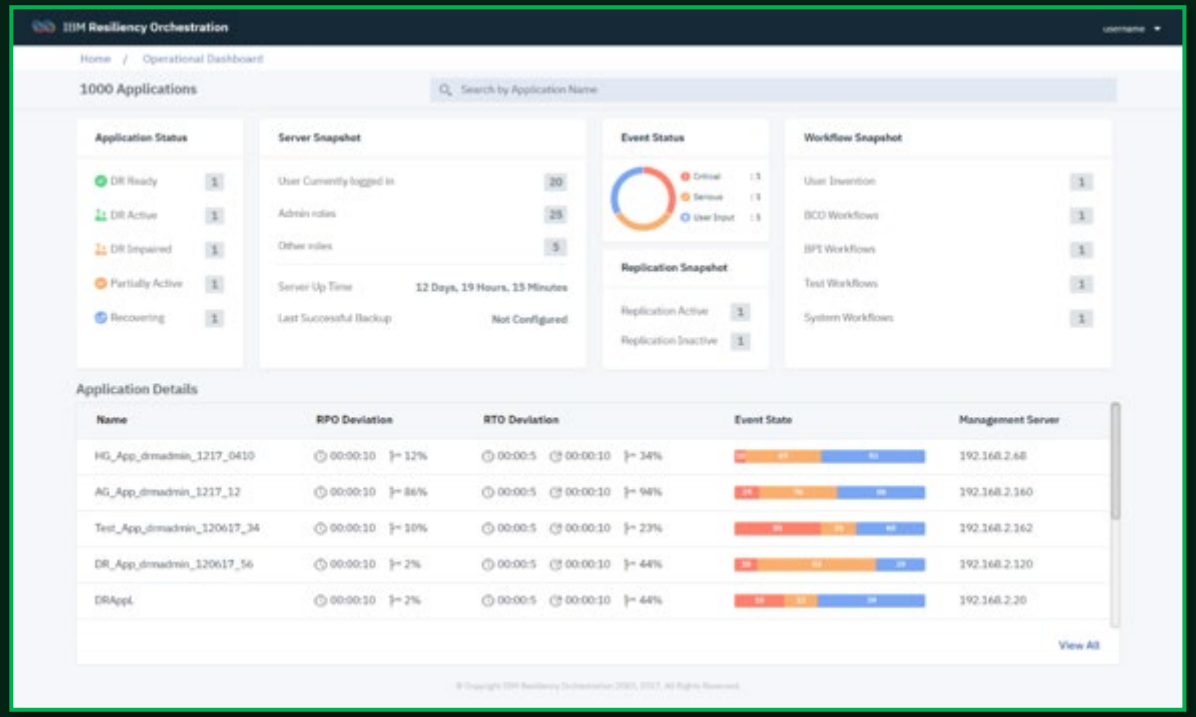




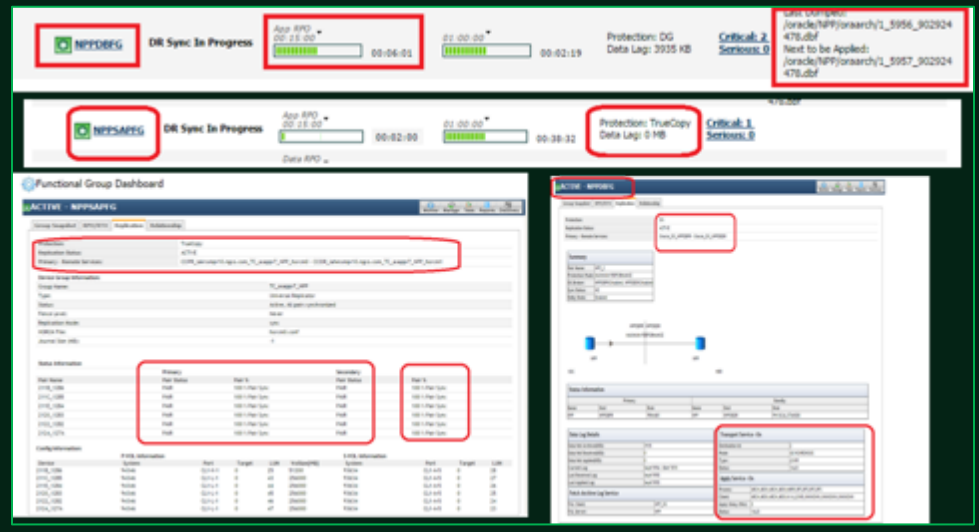




Aussagefähige Desaster Recovery Dashboards und Reports erlauben die DR Fähigkeiten Applikation für Applikation in Echtzeit zu überwachen



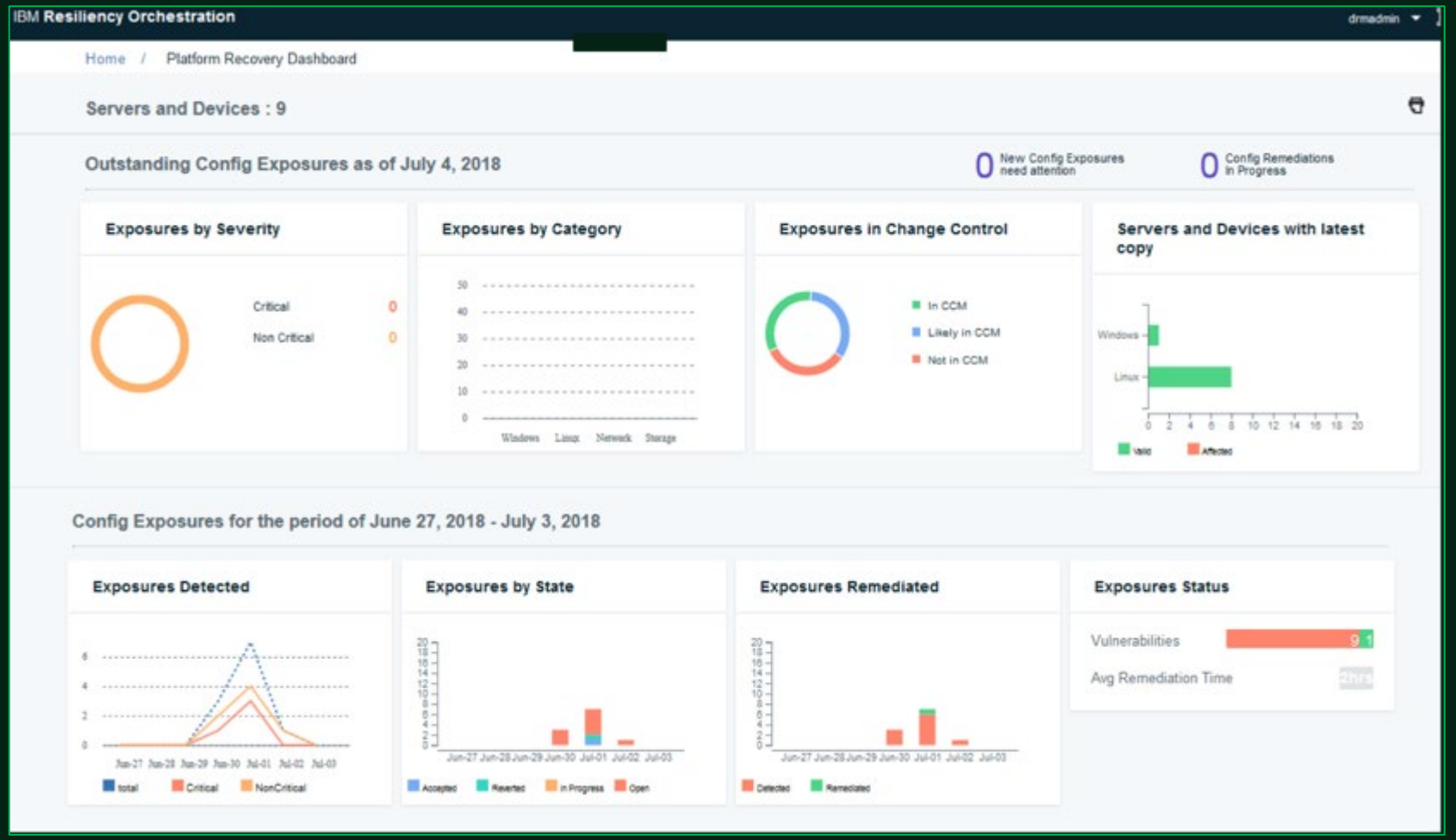
- Applikationsweise Zusammenfassung der Recoveryfähigkeit
- Ereignisse die Eingriffe erfordern
- RPO und Datenrückstand Messung
- Recovery Workflows die momentan benutzt werden

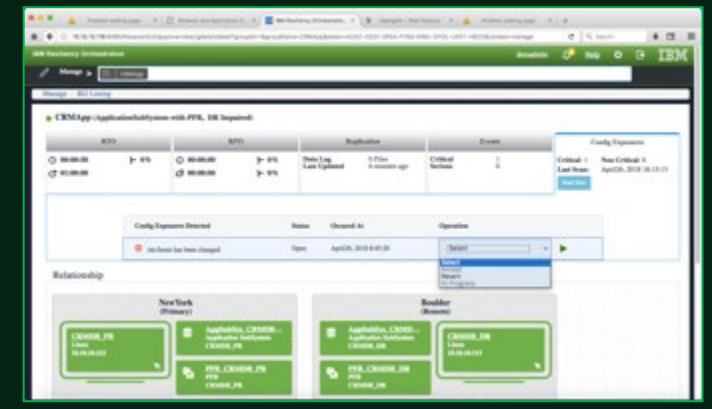


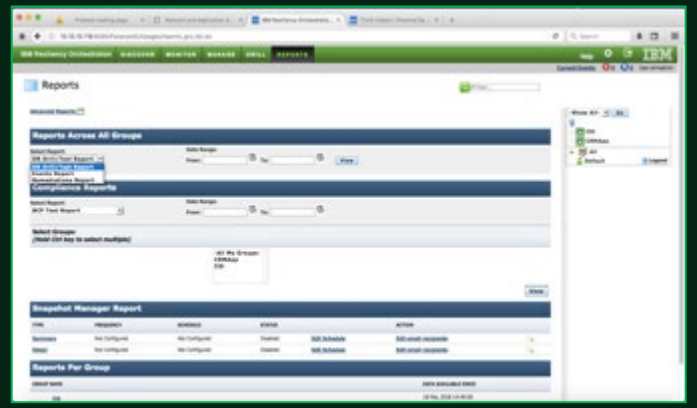
- Database logs Position
- Dashboard mit Überwachung, Alarmen and Reports
- Desaster Recovery Lösungsstatus und Daten RPO and RTO Service Level Agreements (SLAs)
- Out of the box standard und anpassbare compliance Reports

kyndryl

Resiliency Orchestration mit Cyber Incident Recovery bietet ein Dashboard für Transparenz und Steuerung







Agenda

01 Einleitung

02 Disaster Recovery vs. Cyber Incident Recovery

03 Recovery Orchestration

04 Ein möglicher Fahrplan zur Umsetzung

05 Ransomware Angriff

Unser Verständnis der Anforderungen

Status quo

Im Unternehmen fehlt es an:

- Notwendigen Prozessen
- Dokumentationen
- und Maßnahmen

Absicht

Ihr Unternehmen Krisensicher aufzustellen und vorbereitet für den nächsten Angriff zu sein.

Ziel

Einführung einer resilienten Disaster Recovery und Cyber Incident Strategie, um zukünftig sicherzustellen, dass...

- ausreichend Kapazitäten für den DR-Fall vorhanden sind
- im Falle eines Notfalls die MVP Company weiterhin betrieben werden kann

Ein möglicher Fahrplan zur Umsetzung

Erfassung Status Quo

Verständnis der aktuellen Prozesse und Technologien im Bereich Cyber Incident Recovery & Desaster Recovery

Maßnahmenbündel

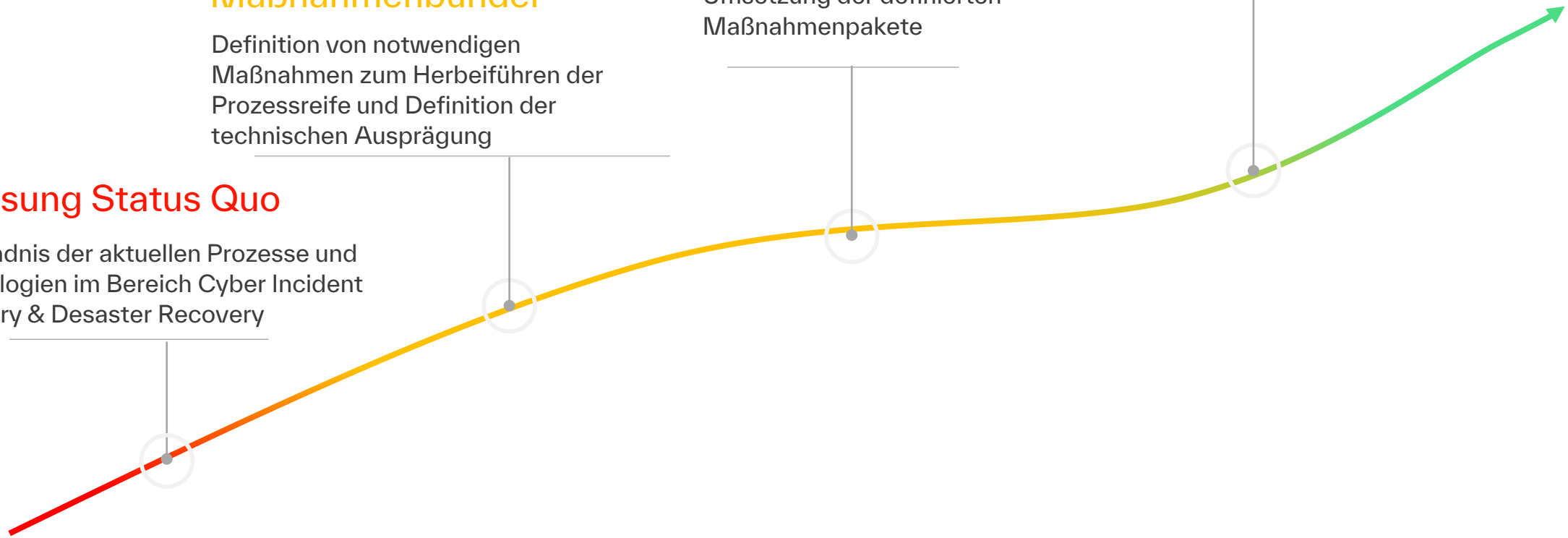
Definition von notwendigen Maßnahmen zum Herbeiführen der Prozessreife und Definition der technischen Ausprägung

Umsetzung

Umsetzung der definierten Maßnahmenpakete

Kontinuierliche Verbesserung

Test & Drill
Change & update
conduct training & awareness programs



kyndryl

Agenda

01 Einleitung

02 Disaster Recovery vs. Cyber Incident Recovery

03 Recovery Orchestration

04 Ein möglicher Fahrplan zur Umsetzung

05 Ransomware Angriff

kyndryl

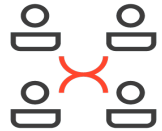
Ransomware Angriff trifft das Unternehmen

Ausgangssituation

Das Unternehmen hat sich Cyber Resilient aufgestellt

Ransomware Angriff

Das Unternehmen entdeckt den Ransomware Angriff und beruft den Krisenstab



Krisenstab kommt zusammen

Der Krisenstab übernimmt die IT-Organisation

Maßnahmen Ransomware

1. Isolieren

Isolieren der betroffenen Systeme, um eine weitere Ausbreitung zu verhindern.

2. Beurteilen

Beurteilen des Schadens, um den Umfang der Wiederherstellung festzulegen.

3. Wiederherstellen

Wiederherstellung der identifizierten Ziele mit Hilfe der Recovery Orchestration in der CI-Umgebung.

4. Überprüfung

Isolierten Bereich überprüfen und Aufbewahrung der Logs für potentielle Strafverfolgungen.

5. Zurückführung in die Produktiv-Umgebung

Die wiederhergestellten Systeme werden zurück in die Produktivumgebung überführt und dort betrieben.

6. Normalbetrieb aufnehmen

Der Normalbetrieb wird wieder aufgenommen.

Zusammenfassend sofern eine entsprechende Strategie mit geeigneten Maßnahmen gegen Ransomware Angriff etabliert ist, lässt sich der Business Impact eines solchen Angriff stark reduzieren.

Vorbereitung und Übung sind die Schlüsselfaktoren für ein Cyber resilientes Unternehmen.

kyndryl

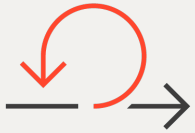
Key Facts to Go

Organisatorische Grundlagen

- Resiliente Geschäftsmodelle
- Unterschied Cyber Incident & Desaster Recovery

Technologische Absicherung

- Lange Backup Aufbewahrungs-Zeiten
- Orchestrierte Recovery



Kontinuierliche Verbesserung & Übung

- Übungen & Tests etablieren
- Stand der Technik

Business Impact des Angriffs stark reduzieren

Kyndryl