

# Cyber-Resilienz in der öffentlichen Verwaltung stärken

---

Die deutsche Komplettlösung für  
Backup und Disaster Recovery



# Herzlich Willkommen!

## Unsere Referenten



**Stefan Utzinger**  
*Geschäftsführer NovaStor*  
[stefan.utzinger@novastor.com](mailto:stefan.utzinger@novastor.com)



**Wolfgang Rudloff**  
*Senior Backup Consultant*  
[wolfgang.rudloff@novastor.com](mailto:wolfgang.rudloff@novastor.com)



- ca. 60 Minuten

- Geschäftsverantwortliche, IT-Entscheider, IT-Admins

- Fragen im Chat

- Folien im Anschluss per E-Mail

# Unsere Agenda



# NovaStor betrachtet Datensicherung ganzheitlich

NovaStor DataCenter – über 500 Installationen im deutschen Mittelstand



**NOVAStOR**

## Ganzheitliche Datensicherung



**Service** – Begleitung vom Erstgespräch über die Implementierung bis in den laufenden Betrieb



**Software** – Hersteller mit eigener Produktentwicklung in Deutschland



**Support** – Erfahrung und Know-how aus zahlreichen Backup-Projekten

- ✓ Deutscher Hersteller und Lösungsanbieter für ganzheitliche Datensicherung
- ✓ R&D & technischer Support in Deutschland
- ✓ Deutsche AGB / EULA
- ✓ Komplettlösung vom Backup-Konzept bis zum Health-Check
- ✓ Transparente Preismodelle mit Flat-Fee Option
- ✓ Übernahme von Verantwortung – vom Monitoring bis zum Managed Backup Service



# Cyber-Resilienz stärken

## Geschäftsrisiken und Kosten minimieren

Ein Überblick

# Cyber-Attacken - weltweit größte Gefahr für Unternehmen

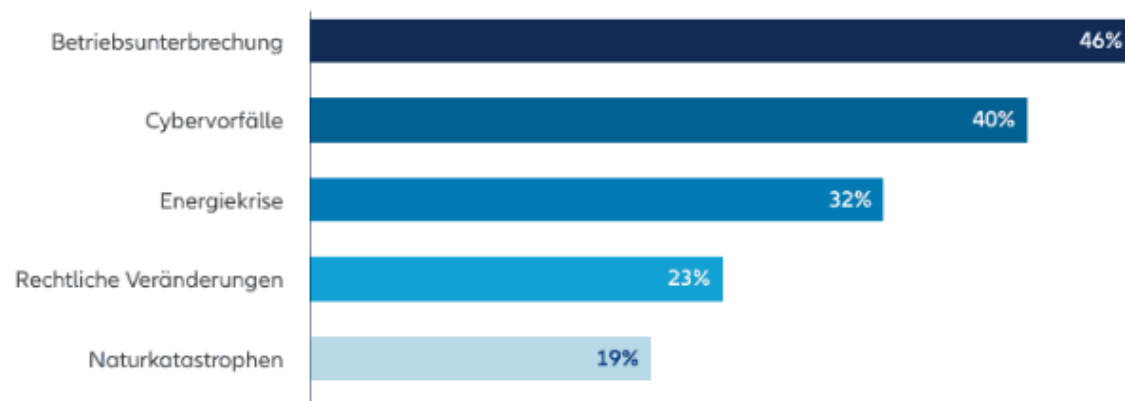
Allianz Risk Barometer 2023



## Top 10 Geschäftsrisiken in Deutschland in 2023

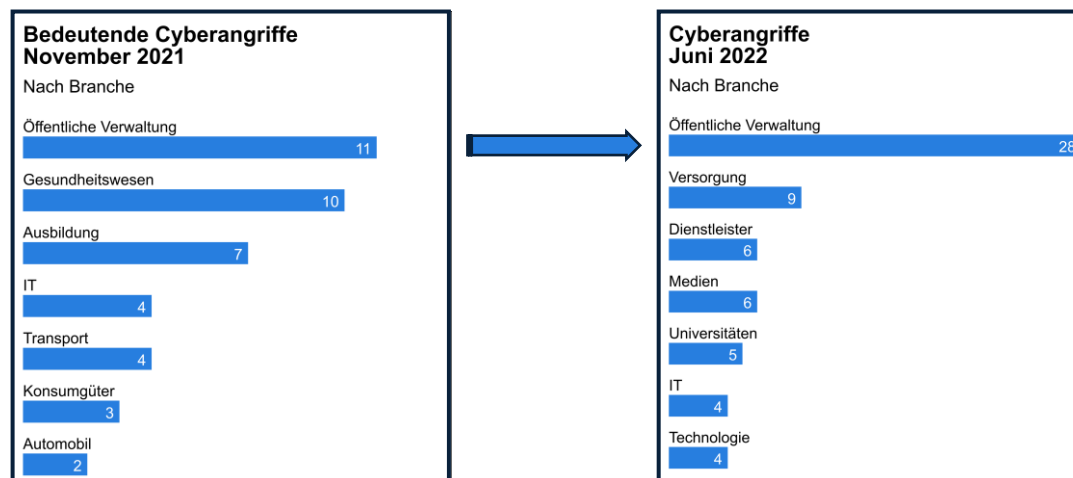
Allianz Risk Barometer 2023

Die Zahlen geben an, wie oft ein Risiko als Prozentsatz aller Antworten für das jeweilige Land ausgewählt wurde: 384. Die Zahlen addieren sich nicht zu 100%, da bis zu drei Risiken ausgewählt werden konnten.



AGCS News & Insights

Quelle: Allianz Global Corporate & Specialty



Quelle: KonBriefing.com

- Betriebsunterbrechung & Cyberfälle sind größte Geschäftsrisiken – hängen meist zusammen!
- Cyber-Angriffe haben sich mehr als verdoppelt!
- Cyber-Versicherungen greifen oft nicht

**Prio A für IT-Verantwortliche: Disaster Resilienz stärken.**

# Cyber-Bedrohungen sind allgegenwärtig

Mehr als 85% aller Unternehmen von einem Cyberangriff betroffen

223 Mrd. Euro Schaden (+358% ggü. 2019)\*



## Cyberattacke: IHK fährt sämtliche IT-Systeme herunter

Stand: 04.08.2022 16:42 Uhr

In ganz Deutschland ging am Donnerstag bei der Industrie- und Handelskammer kaum etwas. Nach einem vermeintlichen Hackerangriff wurden die Computer-Systeme aller IHK-Standorte heruntergefahren - auch in Schleswig-Holstein.



Hacker legen Traktoren-Hersteller Fendt lahm

augsburger-allgemeine.de • Lesedauer: 1 Min.

t3n

## Cyberangriffe auf den Handel nehmen weiter zu – und werden komplexer

Der Handel bietet eine immer größere Angriffsfläche für Hacker:innen. Dabei stehen die eigenen Geschäftsprozesse ebenso im Fokus wie die Lieferkette oder die Anbindung an Zahlungsdienstleister. Eine neue Studie zeigt, worauf Onlienhändler:innen achten sollten.

Datenverfügbarkeit ist für Unternehmen überlebenswichtig



Steigende IT-Abhängigkeit  
Komplexe Bedrohungen  
Hohe Schäden

### Status in vielen Unternehmen:

- Backup-Software
- Aktuelles Backup-Konzept
- Disaster Recovery Planung
- Klare Verantwortlichkeiten
- Wirtschaftliche Transparenz
- Management involviert



\* <https://www.bitkom.org/sites/default/files/2021-08/bitkom-slides-wirtschaftsschutz-cybercrime-05-08-2021.pdf>



# Kundenbeispiele

## Cyber-Angriff

Beispiele, bei denen der NovaStor Support beim Disaster Recovery geholfen hat



### Sanitätshaus- Versorger

**12 Hyper-V Hosts**  
**Umsatz 100 Mio. Euro**

- Zwei Mal betroffen
- Kein Backup-Konzept



### Automobilhändler

**14 Standorte**  
**1.400 Mitarbeiter**

- Backups verschlüsselt
- Kein Backup-Konzept
- Kein Notfallplan



### Anbieter Kraft- & Schmierstoffe

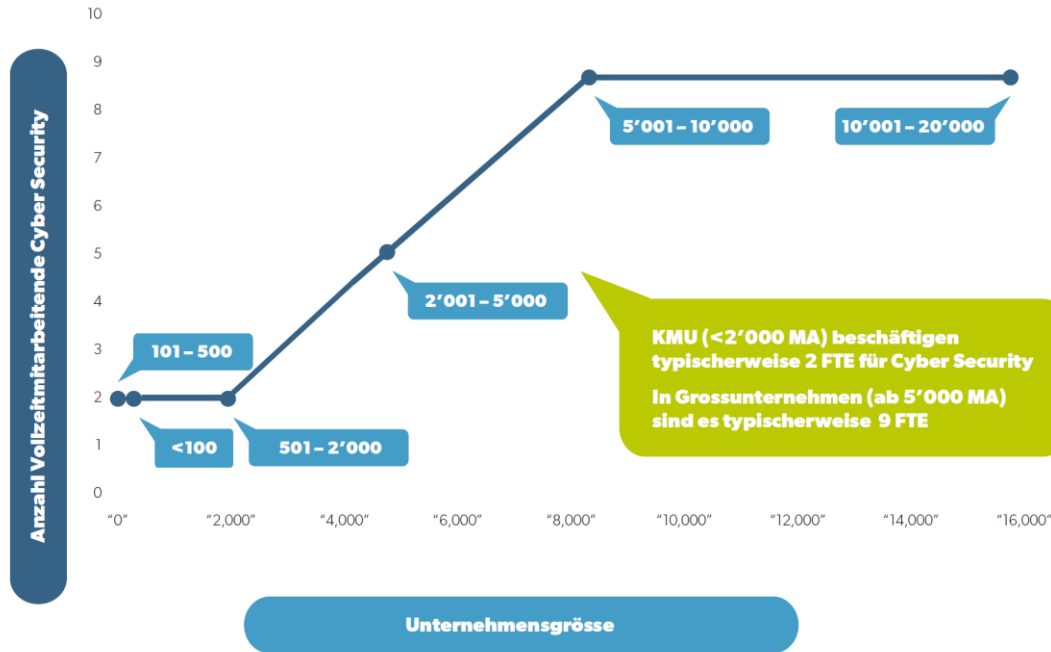
**5 Standorten**  
**200 Mitarbeitern**

- Backups verschlüsselt
- Hohe Service-Kosten
- Kein Backup-Konzepts
- Unzureichende Backups



# Verankerung von Cybersecurity in Unternehmen

Auszug aus der AWK Cyber Resilience Studie 2020



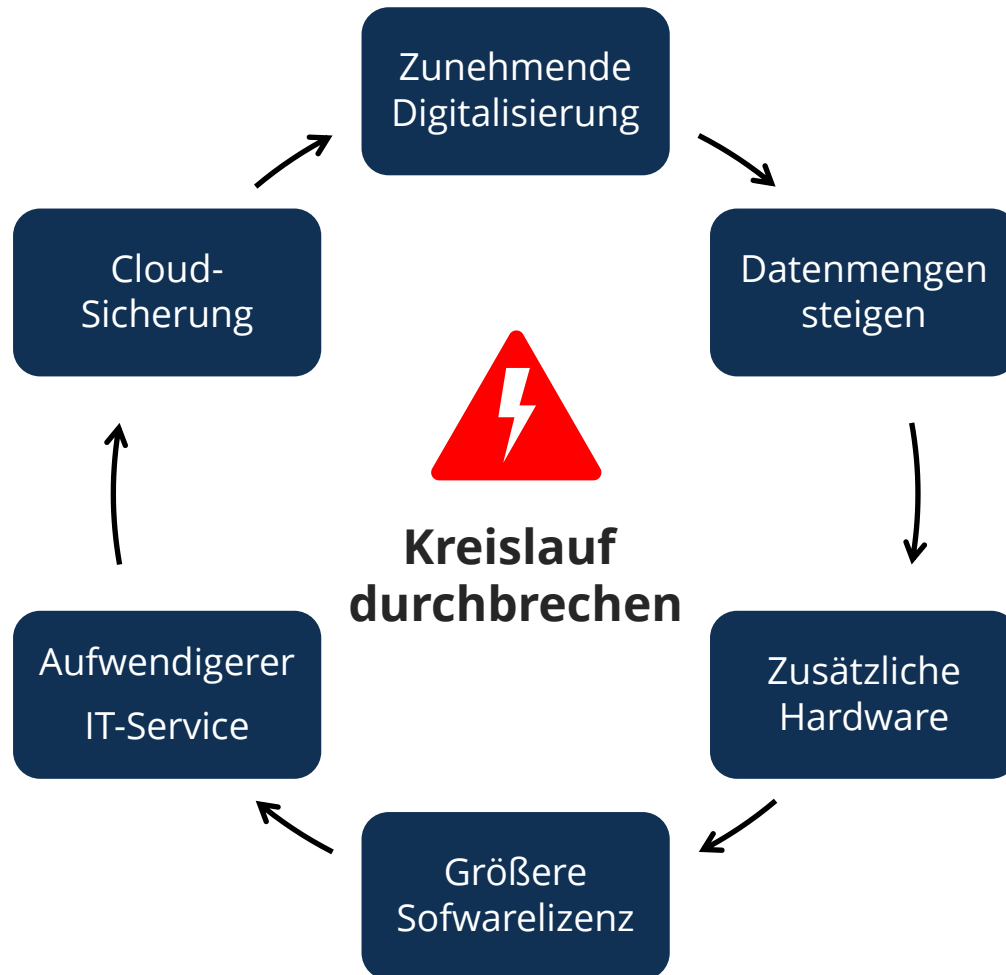
- Aufgrund enormer Geschäftsrisiken sollte **Cyber-Security Aufgabe des Top-Managements** sein
- Top-Management muss **Rahmenbedingungen** schaffen, Cyber-Security in der Organisation verankern und **Ressourcen** freigeben
- Die gesamte **digitale Lieferkette** muss auf **Cyber-Risiken** geprüft werden
- Bei Unternehmen / öffentl. Verwaltungen mit <500 MA gibt es **oft keine dedizierten Cyber-Security Mitarbeiter** – Teilaufgabe der IT-Abteilung



**Insbesondere KMU und öffentlicher Verwaltung fehlen die Ressourcen für Cyber-Resilienz. Daher sollte auf externe Experten zurückgegriffen werden.**

# Treiber der Kostenexplosion

Inflation + Cyber-Attacken + Lieferkettenproblematik = Kostenexplosion



- **Digitalisierung** der Unternehmensprozesse
- **Datenmengen steigen** um 27% pro Jahr an
- Für steigende Datenmenge wird **mehr Hardware** benötigt und verteuert sich überproportional
- Software-Lizenzen sind an Infrastruktur gebunden – **Hersteller erhöhen Preise**
- **Personalmangel**, höhere Löhne und Mehraufwand verteuern IT-Services
- Cloud- / Externe Sicherung wegen Cyber-Attacken immer notwendiger
- **Inflation** treibt die Preisspirale noch schneller
- Auch **Systemhäuser leiden**: Kunden können Preiserhöhungen nicht akzeptieren, Personalkosten steigen – **Erträge sinken**

# Cyber-Resilienz stärken

## Checkliste (Auszug)

- ✓ **Komplexität reduzieren:** Prüfen Sie Ihre Security-Systeme. Ergänzen, überlappen sich die Systeme?
- ✓ **Minimal Viable Company:** Geschäftsfähigkeit und **Priorisierung der Daten** - Kennen Sie die kritischen Applikationen? Welche Geschäftsprozesse müssen unbedingt am Laufen gehalten werden, damit das Unternehmen auch bei einem Cyberangriff agieren kann?
- ✓ **Backup-Konzept** erstellen
- ✓ **Disaster Recovery Plan** erstellen
- ✓ Der **Backup Server** sollte auf einem eigenen physischen Server und **getrennt von der Produktiv-Umgebung** laufen.
- ✓ **3-2-1 Backup Regel** befolgen: lokales Backup und ausgelagertes Backup, „Air Gap“ zwischen Produktiv- und Backup-Daten
- ✓ Regelmäßige **Notfall-Tests** mit allen relevanten Personen
- ✓ **Schulen und sensibilisieren Sie Ihre Mitarbeiter.**

# Komplettlösung für Backup und Disaster Recovery richtig aufsetzen

Betriebswiederherstellung und Arbeitsfähigkeit  
nach Disaster-Fällen sicherstellen

# Ganzheitliche Lösung - essentiell wichtig!



Der Panik Button  
muss einfach  
funktionieren!!



**Im Disaster-Fall: Prozesse müssen geplant, geordnet und zuverlässig ablaufen!**

# Komplettlösung für Backup und Disaster Recovery

Betriebswiederherstellung und Arbeitsfähigkeit nach Disaster-Fällen sicherstellen



Fokus des Webinars:

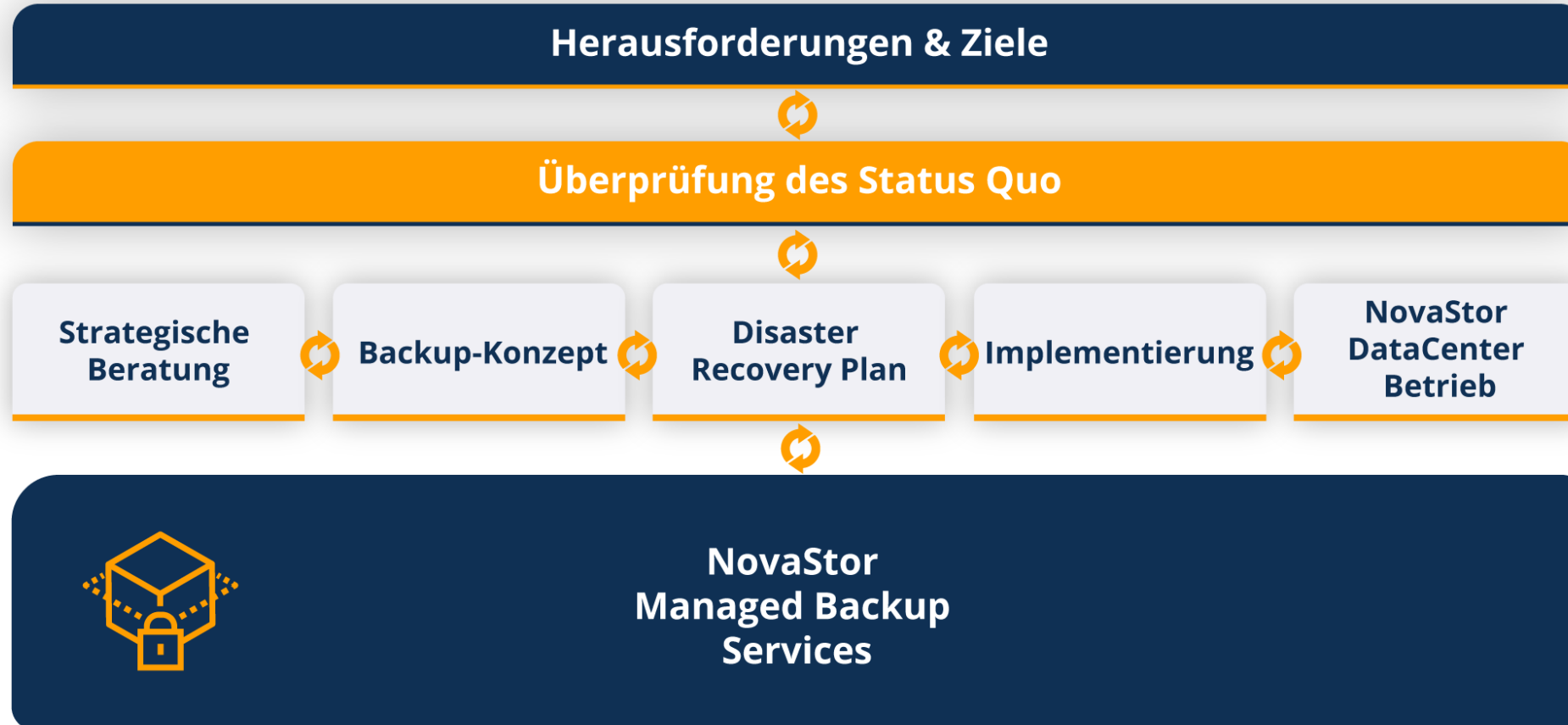
**Cyber-Resilienz  
stärken für eine  
schnelle  
Betriebswieder-  
herstellung**

Eine ganzheitliche Lösung gibt Kunden und Partnern die Sicherheit auch im Disaster-Fall Daten schnell wieder verfügbar zu haben und die Organisation schnell wieder arbeitsfähig zu machen. Dies ist die Basis für eine hohe Cyber-Resilienz.

- X Komplettlösung heißt nicht: Sicherung einzelner Daten**
- ✓ Komplettlösung heißt: Sicherstellen der Datenverfügbarkeit**

# Komplettlösung stärkt die Cyber-Resilienz

am Beispiel von NovaStor DataCenter



# Strategieberatung

Die Strategie bildet die Basis für eine erfolgreiche Disaster Recovery Planung

## Inhalte & Ziele der Strategieberatung

- Strategische Analyse der geschäftskritischen Unternehmensprozesse, Daten und Systeme
- Abschätzung der wirtschaftlichen und gesellschaftlichen Schäden unter verschiedenen Disaster-Szenarien
- Auswirkung gesetzlicher Vorgaben / Compliance Richtlinien auf Datenhaltung / -verwaltung
- Ausarbeitung der Kernprozesse / Verantwortlichkeiten zur Betriebswiederherstellung nach einem Disaster



**Die Strategieberatung bildet die unternehmerische Basis zur Entwicklung eines Backup-Konzeptes und der Disaster Recovery Planung**



# Backup-Konzept

Basis für die Implementierung und Prüfung der Lösung

## Welche Ziele das Backup-Konzept verfolgt

- Geschäftskritische Daten, Prozesse und Systeme dokumentieren
- Berücksichtigung von Compliance / Gesetzlichen Vorgaben
- Verfügbarkeitsanforderungen sicherstellen (RTO, RPO, etc.)
- Aufnahme & Analyse der IT-Infrastruktur & Sicherheitskonzept
- Bedrohungsanalyse, Schwachstellen feststellen & eliminieren
- Backup-Infrastruktur & Backup-Strategie definieren
- Anschaffungen, Einsparpotentiale, Verantwortlichkeiten ermitteln



**Das Backup-Konzept zeigt Verbesserungspotentiale auf und definiert die wichtigen Maßnahmen für das Setup, die Implementierung und Betrieb der Backup Lösung**

# Disaster Recovery Planung

Damit ein Notfall nicht zum Disaster wird!

## Welche Ziele die Disaster Recovery Planung verfolgt

- Ausfallzeiten und finanzielle Schäden verringern
- Business relevante Prioritäten für den Disaster Fall festlegen
- Schnelle Wiederherstellung der Systeme und Daten sicherstellen (Checkliste)
- Klare Verantwortlichkeiten & Prioritäten
- Notfall Zugriff sicherstellen für Kontaktdaten, Checklisten, Handlungsanweisungen, Zugangsberechtigungen etc.



➤ **Die Disaster Recovery Planung stellt sicher, dass alle für den Disasterfall definierten Prozesse zur Wiederherstellung der Betriebsfähigkeit schnell und reibungslos ablaufen**

# Kundenbeispiel

Managed Backup Services bei der Stadt Mannheim

# Stadt Mannheim

Eine Datensicherungslösung für alle Standorte

## Szenario bei der Stadt Mannheim

**Größe:** 7.000 Mitarbeiter an verschiedenen Standorten mit 120 städtischen Betrieben

**Betriebssysteme:** u.a. Windows, RedHAT, SUSE Linux...

**Virtuelle Systeme:** 40 Hyper-V / VMware Hosts mit etwa 350 virtuellen Maschinen

**Anwendungen:** Oracle, SQL, MySQL

**Backup-Volumen:** > 230 TB



# Stadt Mannheim

Eine Datensicherungslösung für alle Standorte

## Gründe für die Komplettlösung NovaStor DataCenter

- ✓ Zentrales Management aller Prozesse für die Umsetzung eines standortübergreifenden Sicherheitskonzeptes
- ✓ Finanzielle Planungssicherheit und Stabilität für das konstante Datenwachstum
- ✓ Backup heterogener Umgebungen, frei Wahl bei Speichermedien und -technologien
- ✓ Datenverfügbarkeit: Geschwindigkeit, mit der ein Restore der gesicherten Daten durchgeführt werden
- ✓ Direkte Ansprechpartner, deutschsprachige Techniker

## NovaStor Managed Backup Services

- Nutzung von NovaStor MBS seit 2020
- NovaStor übernimmt Management der Datensicherung
- Ziel:
  - Experten kümmern sich um die Backup Umgebung
  - Ressourcen der eigenen Mitarbeitern frei schaufeln unter Nutzung geprüfter, externer Dienstleister
- MBS = nächster Schritt in eine digitale und vernetzte Zukunft der Stadt Mannheim

# NovaStor DataCenter

Backup und Cyber Attack Recovery in einem Tool



# Ganzheitliche Backup & Recovery Lösung

NovaStor DataCenter



- ✓ 100% in Deutschland entwickelt & supportet
- ✓ Zentrale Verwaltung über eine intuitive Web-GUI
- ✓ Unterstützung heterogener und verteilter Umgebungen
- ✓ Visuelles Backup-Management
- ✓ Übersichtlich, zuverlässig und hoch performant
- ✓ Mit wenig Aufwand zu managen
- ✓ Support für RMM/Monitoring Systeme
- ✓ Audit-Reports
- ✓ Cloud Storage im CO2 neutralem Rechenzentrum



**Moderne Backup & Recovery Lösung mit voller Funktionsbreite**

# Betriebswiederherstellung muss funktionieren

Regelmäßige Wiederherstellungstests sind Pflicht

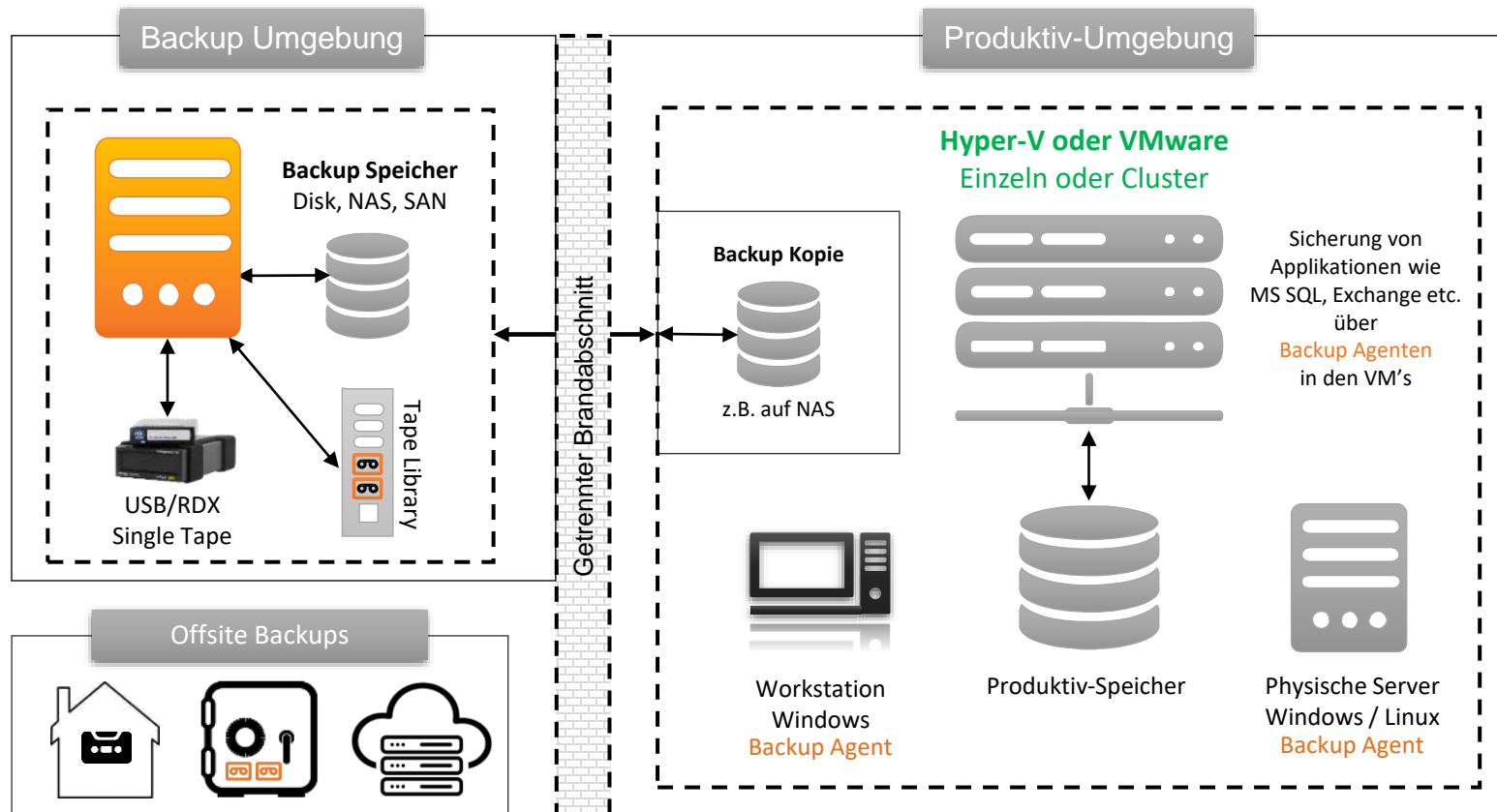
- Regelmäßige Restore Tests sind verpflichtend
- Zeitgesteuerte Restores *ab NovaStor DataCenter 9.3*
  - Granular oder komplett
  - Wahl zwischen Prüfen und echtem Restore
  - Gespeicherte Restore Jobs können jederzeit auch manuell ausgeführt werden.
  - Restore Ergebnisse über Reports
- Gespeicherte Restore Jobs erleichtern den Wiederherstellungsprozess bei einem Disaster



**Backups die sich nicht wiederherstellen lassen können hohe Kosten verursachen, oder sogar die Unternehmensexistenz gefährden**



# Best Practise Beispiel gegen Datenverlust bei Cyber-Attacken



- Vollwertige Agenten
- für physische und virtuelle Maschinen
- Unterstützung von
  - heterogenen Umgebungen
  - mehreren Backup Servern
  - mehreren Standorten
- Volle Backup-Ziel Flexibilität
  - Disk, NAS, SAN, USB/RDX, Tape, Libraries, Cloud, etc.
- Backup Server können physisch oder virtuell sein

 **NovaStor DataCenter - Schützt zuverlässig Daten und Systeme aller Standorte**

# NovaStor DataCenter

## Live Einblick

The screenshot displays the NovaStor DataCenter dashboard with the following components:

- Account:** admin, Lizenz gültig bis 31.12.2023, Unbefristeter NovaCare.
- Navigation:** Dashboard, Serververwaltung, Backup-Schema, Monitoring, Reporting, Wiederherstellung, Zeitplanung, Speicherverwaltung, Benutzerverwaltung, Einstellungen.
- Dashboard Overview:**
  - Auftragsstatus der letzten 24 Stunden:** Donut chart showing 100% success (Erfolg).
  - Verfügbarkeit in den letzten 30 Tagen:** Bar chart showing availability over time with a legend for Abgebrochen, Fehlgeschlagen, Warnung, and Erfolgreich.
  - Medienpool Status:** Table listing media pools with columns for Erreichbar, Backupgröße, Größe des Dateisystems, Freier Speicher, and Belegung.
- Historical Data:**
  - Geschichte / FET Daten in den letzten 30 Tagen:** Bar chart showing historical FET data with a 'Current FET' of 521,329 GB and an 'Aktualisieren' button.
  - Kommende Aufgaben:** List of upcoming tasks including backup jobs and reports.
  - Systembenachrichtigungen:** Log of system notifications such as 'Job Hyper-V succeeded' and 'Backup started: Hyper-V'.

# NovaStor Komplettlösung

Jetzt Kontakt aufnehmen und Vorteile sichern

## Persönliche Beratung



**Jetzt anfragen!**

[www.novastor.de/beratung](http://www.novastor.de/beratung)



**Wolfgang Rudloff**

*Senior Backup Consultant*

[wolfgang.rudloff@novastor.com](mailto:wolfgang.rudloff@novastor.com)



**Besserer Service • Nähe zum Hersteller • Moderne Backup-Lösung mit voller Funktionsbreite  
Höhere Kundenbindung und -zufriedenheit als bei globalen Software-Anbietern**

# Vielen Dank!

## **NovaStor GmbH**

Neumann-Reichardt-Str. 27-33

22041 Hamburg

Germany

Telefon: +49 (40) 63 809 0

Copyright © 2023 NovaStor GmbH. Alle Rechte vorbehalten. NovaStor und das NovaStor Logo sind geschützte Markenzeichen der NovaStor GmbH. Windows ist ein eingetragenes Warenzeichen der Microsoft Corporation. Andere Bezeichnungen können Warenzeichen oder eingetragene Warenzeichen anderer Rechteinhaber sein. Alle Informationen sind freibleibend und unverbindlich. Technische Änderungen, Abweichungen der Abbildungen und Irrtümer vorbehalten.