NOVASTOR

Wie Sie die schnelle Betriebswiederherstellung im Desaster-Fall sicherstellen

Datensicherung als Komplettlösung

Einleitung

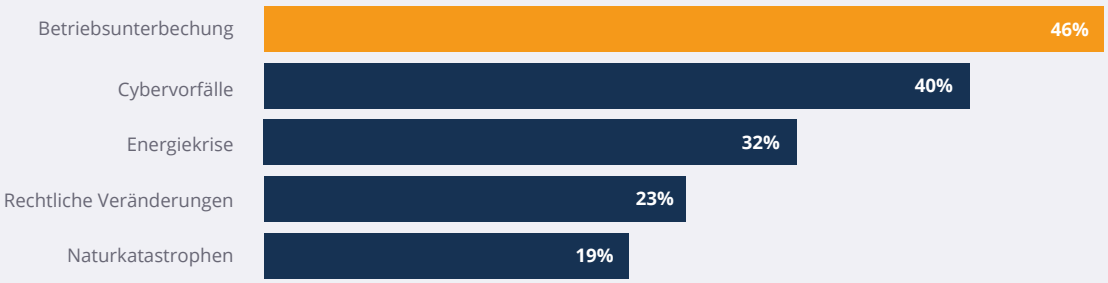
Datenverlust oder Datendiebstahl hat gravierende, nachhaltige Auswirkungen auf den Betrieb einer Organisation, die auch den wirtschaftlichen Untergang bedeuten können.

Betriebsunterbrechungen durch Cyber-Angriffe oder andere Desaster sind in der täglichen Arbeit Realität. Es geht nicht mehr darum, ob ein Cyber-Angriff passiert, sondern wann und wie Sie darauf vorbereitet sind.

Backup und Recovery einzelner Files gehören der Vergangenheit an. Datensicherung wird zum Disaster Recovery Management und funktioniert nur als Komplettlösung. Eine moderne Datensicherungslösung muss im Ernstfall dafür sorgen, dass die Organisation schnellstmöglich wieder arbeitsfähig ist.

Die zentrale Frage, die Sie sich stellen müssen und die in diesem Whitepaper behandelt wird, lautet:

Wie schaffe ich es mithilfe der Datensicherung nach einem Desaster eine schnelle Betriebswiederherstellung zu gewährleisten?



▶ Top 10 Geschäftsrisiken weltweit in 2023, Allianz Risk Barometer 2023

2. Geschäftsrisiken

Die Geschäftsrisiken für Unternehmen sind vielschichtig. Das Allianz Risk Barometer 2023 zeigt, dass Betriebsunterbrechungen zu den größten Geschäftsrisiken zählen, gefolgt von Cybervorfällen. [1]

Datenverlust führt in Organisationen nicht einfach zu Mehrarbeit, sondern kann im schlimmsten Fall den Untergang von Unternehmen bedeuten: vom Stillstand der Produktion, Unterbrechungen der Lieferketten bis zum Verlust von Arbeitsplätzen.

Die Priorität für IT-Verantwortliche liegt darin, die Cyber-Resilienz der Organisation zu stärken, d.h. Maßnahmen zu treffen, die sicherstellen, dass der Ernstfall, z.B. ein Cyber-Angriff, glimpflich und ohne größere Schäden verläuft. Ziel ist es, dass die Organisation den Betrieb schnellstmöglich wiederaufnehmen kann und dass die Datenverfügbarkeit gewährleistet ist. Zwei Beispiele aus der täglichen Arbeit bei NovaStor, dem deutschen Hersteller und Lösungsanbieter für Datensicherung, zeigen, dass die Maßnahmen zur schnellen Betriebswiederherstellung in vielen Unternehmen unzureichend sind.

In den beiden folgenden Fällen war kein Backup-Konzept vorhanden und die Backups wurden verschlüsselt, was die Datenwiederherstellung enorm erschwerte. Das führte wiederum zu einer regelrechten Kostenexplosion – von den Auswirkungen für die Produktion, Lieferung etc. ganz zu schweigen. Die Kosten für die Betriebswiederherstellung überstiegen am Ende deutlich das Investment, was für eine funktionierende Datensicherung inklusive Backup-Konzept und Disaster Recovery Plan notwendig gewesen wäre.

Global agierender Anbieter Kraft- & Schmierstoffe

5 Standorte
200 Mitarbeiter

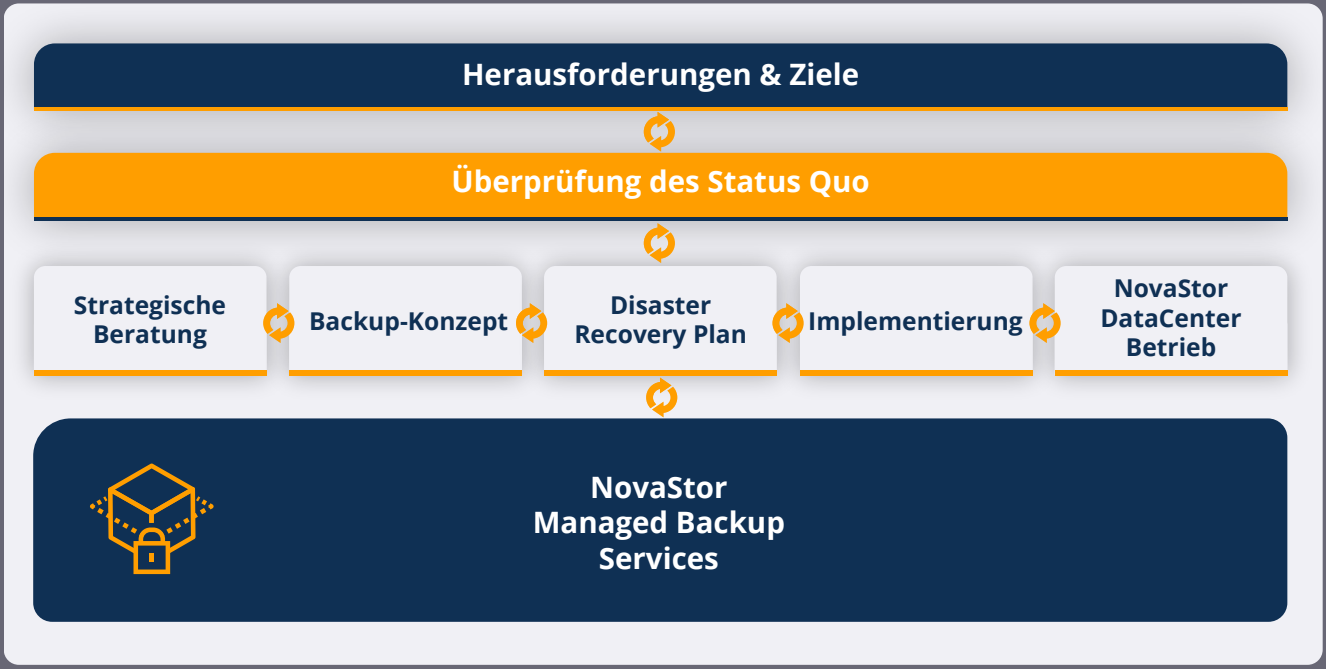
- Backups verschlüsselt
- Hohe Service-Kosten
- Backup-Konzept
- Unzureichende Backups

Automobilhändler

14 Standorte
1.400 Mitarbeiter

- Backups verschlüsselt
- Backup-Konzept
- Disaster Recovery Plan

Die Ursachen für das Versagen der Datensicherung sind vielfältig und keinesfalls mit fehlendem Know-how der Verantwortlichen zu begründen. Fachkräftemangel, zu geringe Budgets, Überlastung, die fortschreitende Digitalisierung und die damit verbundene Komplexität machen es den Verantwortlichen schwer, angemessene Maßnahmen zu ergreifen, die mit den Risiken Schritt halten. Dennoch ist es durchaus machbar, die schnelle Betriebswiederherstellung im Desaster-Fall sicherzustellen. Welche Aspekte und Vorgehensweisen helfen, die Datensicherung erfolgreich aufzusetzen, belastbare Entscheidungen zu treffen und die Cyber-Resilienz Ihrer Organisation zu stärken, behandeln die folgenden Abschnitte.



▶ Schritte zur Komplettlösung für Datensicherung

3. Datensicherung als Komplettlösung

Über die Notwendigkeit von Datensicherungen in Unternehmen gibt es eigentlich nicht viel zu diskutieren, über das Wie, Wann, Womit und Wohin umso mehr. Auch wenn es auf den ersten Blick so scheint, stehen IT-Verantwortliche nicht vor der Aufgabe, sämtliche Daten im Unternehmen einfach zu sichern. Vielmehr stehen sie vor der Herausforderung des Disaster Recovery Managements: die Gegebenheiten des Unternehmens zu analysieren und zu erfassen, was gesichert werden muss, welche Möglichkeiten dafür zur Verfügung stehen und sicherzustellen, dass im Ernstfall die Organisation schnellstmöglich wieder arbeitsfähig ist und die Daten wieder verfügbar sind. Lange Ausfälle sind existenzbedrohend und in jedem Fall zu vermeiden. Die Wiederherstellung der Betriebsfähigkeit nach einem Desaster rückt für IT-Verantwortliche in den Mittelpunkt ihrer Überlegungen. Datensicherheit und Datensicherung wachsen weiter zusammen.

> **Um eine schnelle Betriebswiederherstellung nach einem Desaster-Fall zu erreichen, ist eine ganzheitliche Komplettlösung für Backup und Disaster Recovery erforderlich.**

Weil Komplexität und Gefahren für die IT steigen, muss die Datensicherung stets intelligenter, automatisierter, übersichtlicher werden und mit wenig Aufwand administrierbar sein. Eine Komplettlösung sichert nicht nur einzelne Daten, sondern sie stellt die Verfügbarkeit der Daten sicher. Eine ganzheitliche Lösung gibt Ihnen die Sicherheit auch im Desaster-Fall Daten schnell wieder verfügbar zu haben und die Organisation schnell wieder arbeitsfähig zu machen.

Aus welchen Komponenten besteht eine Komplettlösung?

1 Strategische Beratung und Analyse

In der strategischen Beratung wird der Status Quo aus technischer, wirtschaftlicher und rechtlicher Sicht festgestellt sowie die technischen und unternehmerischen Anforderungen definiert. Entsprechend dieser Prozesse und Prioritäten wird später die Software aufgesetzt. Die Softwarelösung NovaStor DataCenter bildet die Anforderungen ab.

2 Priorisierung der Daten

Hierbei werden die Geschäftsprozesse und die dabei benötigten Daten genau unter die Lupe genommen. Welche Prozesse und Daten sind geschäftskritisch und müssen im Ernstfall zuerst wiederhergestellt werden? Die Einordnung der Daten für die Datensicherung folgt keiner einfachen Ja- / Nein-Struktur, in der Daten entweder gesichert oder nicht gesichert werden. Stattdessen erhalten Daten je nach ihrer Bedeutung für das Unternehmen eine unterschiedliche Einstufung. Je nach Relevanz der Daten folgt deren Sicherung unterschiedlichen Vorgaben. Die Aufbewahrungsdauer ist nicht das einzige Kriterium, das die Bedeutung der Inhalte im Backup-Konzept reflektiert. Von besonders wichtigen Daten sollte zusätzlich zur Sicherung eine Kopie der Sicherung vorgehalten werden. Eine Offline-Backup-Kopie vor Ort zu halten und mindestens eine weitere auszulagern, gilt als Best Practice.

3 Erstellung eines Backup-Konzeptes und Disaster Recovery Plans

Das Backup-Konzept dokumentiert Ihre Datensicherungsstrategie und -maßnahmen. Es umfasst unter anderem eine Übersicht der Daten und IT-Systeme, die für erfolgreiche Restores gesichert werden müssen. Das Backup-Konzept erfordert regelmäßige Kontrollen und gegebenenfalls Aktualisierungen. Der Disaster Recovery Plan legt fest, was zur schnellen Betriebswiederherstellung notwendig ist. Mit einem guten Plan regeln Sie die Verantwortlichkeiten und Zuständigkeiten und stimmen die Business- und Technik-Anforderungen aufeinander ab.

4 Implementierung der Lösung

In der Analyse und dem Backup-Konzept wird definiert, wie bei der Migration der Lösung vorzugehen ist. Im Vordergrund steht bei der Implementierung, dass die im Backup-Konzept definierte Sicherungsstrategie und die im Disaster Recovery Plan definierte Wiederherstellung abgebildet ist. So wird die langfristige Funktionsfähigkeit sichergestellt.

5 Betrieb und regelmäßige Überprüfung der Datensicherung

Die Datensicherung geht in den operativen Betrieb über. Durch die fortschreitende Digitalisierung und stetiges Datenwachstum entwickelt sich in den meisten Firmen die IT-Infrastruktur dynamisch. Neue Server werden aufgesetzt, virtuelle Maschinen und neuer Storage hinzugefügt. Wichtig ist jetzt, dass die Datensicherung nicht auf dem „Status Quo“ stehen bleibt, sondern sich dynamisch und intelligent weiterentwickelt. Hierzu müssen Software-Lösung, Backup-Konzept und Disaster Recovery Plan so ineinander verzahnt sein, dass immer der aktuelle Stand abgebildet wird. Je dynamischer eine IT-Umgebung ist, desto wichtiger ist die ganzheitliche Betrachtung der Datensicherung und die regelmäßige Durchführung von simulierten IT-Notfallszenarien.

- ✓ Durchführung von quartalsweisen Backup Health Checks
- ✓ Mindestens eine jährliche Überprüfung und Aktualisierung von Backup-Konzept und Disaster Recovery Plan
- ✓ Regelmäßige Durchführung von IT-Notfallszenarien
- ✓ Hinzuziehen von Experten zur Vorbereitung und Unterstützung bei Audits

Welche Vorteile bietet eine Komplettlösung für die Datensicherung?

Eine ganzheitliche Datensicherungslösung stärkt die Cyber-Resilienz der Organisation und ermöglicht eine schnelle Wiederaufnahme des Betriebs. Durch das Hinzuziehen von Experten entlasten Sie Ihr Team und profitieren von professioneller Unterstützung und schneller Hilfe von Experten. Systemhäuser können eine ganzheitliche Kundenbetreuung anbieten – von der Analyse bis zur Implementierung bei gleichzeitiger Minimierung des Risikos, weil der Hersteller mit in die Verantwortung geht. Gleichzeitig können die Systemhäuser sich auf Ihr Kerngeschäft konzentrieren.

4. Backup-Konzept

Was vor einigen Jahren noch optional war, ist inzwischen unverzichtbar: Dass Unternehmen für die Datensicherung ein Backup-Konzept und einen Disaster Recovery Plan erarbeiten, muss zum Standard werden. Schließlich geht es darum, Szenarien eines Datenverlustes möglichst vollständig und realistisch vorauszudenken. Vor diesem Hintergrund spielt das Backup-Konzept eine essentielle Rolle, denn es hilft, eine optimale Lösung für die Datensicherung zu konzeptionieren, die alle wesentlichen Anforderungen und Schutzmaßnahmen bei möglichst geringen Kosten erfüllt. Um das Konzept zu erstellen, müssen die IT-Verantwortlichen die Anforderungen der Fachabteilungen kennen. Welche Daten sind geschäftskritisch, welche Daten müssen im Ernstfall zuerst wiederhergestellt werden und was sind im Notfall die ersten Schritte, um die Geschäftstätigkeit wieder aufnehmen zu können? Um diese Fragen zu beantworten, muss die IT-Abteilung verstehen, wie das Unternehmen funktioniert. Nur dann erfüllt die Backup-Lösung Ihren Zweck – nämlich Ausfälle im täglichen Geschäft nach Wichtigkeit abzufangen.

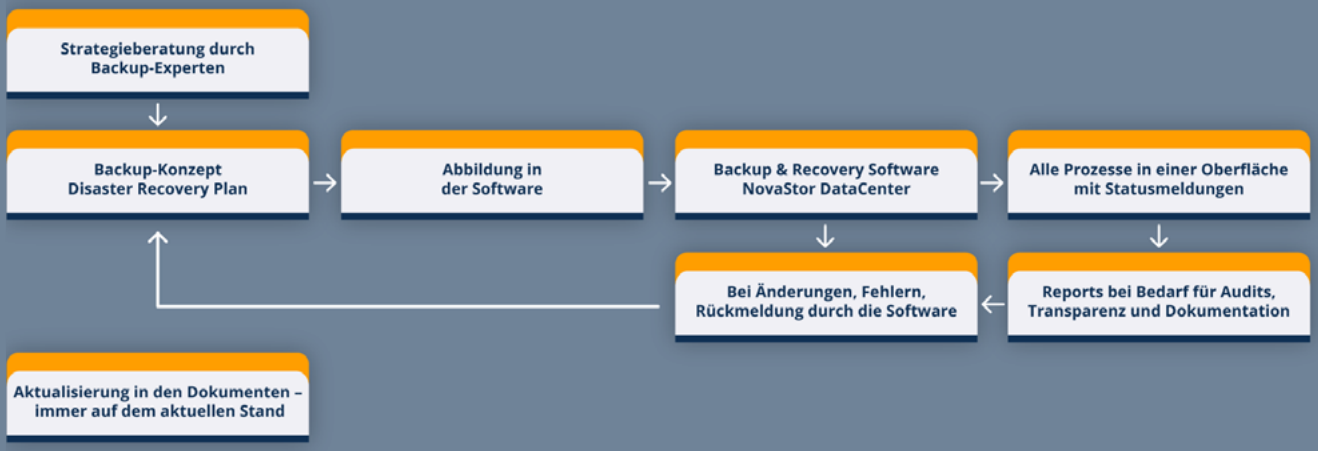
> **Ein Backup-Konzept soll eine möglichst optimale Backup-Lösung konzeptionieren, die alle wesentlichen Anforderungen bei möglichst geringen Kosten erfüllt.**

Welche Ziele verfolgt ein Backup-Konzept?

- ✓ Erfüllung der Business-Anforderungen
- ✓ Erfüllung der gesetzlichen und internen Compliance-Anforderungen
- ✓ Sicherstellen, dass alle Ausfall-Szenarien durch das Backup abgedeckt sind
- ✓ Vermeidung von zu hohen Anschaffungs- und Betriebskosten für die Lösung (TCO)
- ✓ Klare Definition der Verantwortlichkeiten
- ✓ Transparenz auf allen Ebenen

Was beinhaltet ein Backup-Konzept?

- ✓ Strategische Analyse der geschäftskritischen Daten, Prozesse und Systeme
- ✓ Klassifizierung des Unternehmens (KRITIS, ISO o.ä.)
- ✓ Anforderungen für Verfügbarkeit, Compliance, gesetzliche Rahmenbedingungen
- ✓ Aufnahme und Analyse der IT-Infrastruktur und des Sicherheitskonzepts
- ✓ Bedrohungsanalyse für Desaster / Cyberangriffe
- ✓ Schwachstellen feststellen und eliminieren
- ✓ Backup-Infrastruktur und Backup-Strategie definieren
- ✓ Verantwortlichkeiten, regelmäßige Aufgaben



▶ Backup-Konzept und Software sind eng miteinander verzahnt

4.1 Wie Backup-Konzept und Software zusammenspielen

Die Ergebnisse der Strategieberatung und Analyse fließen ins Backup-Konzept und in den Disaster Recovery Plan ein.

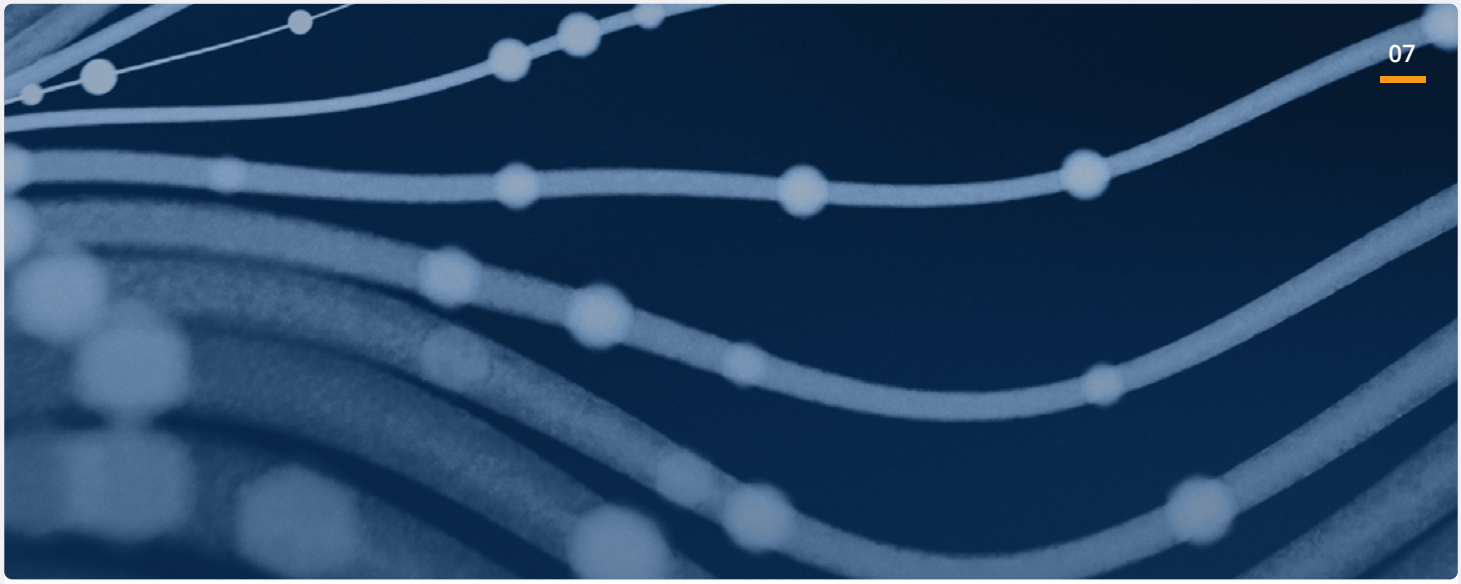
Diese Prozesse und Strukturen, wie Sicherungsintervalle, Backup-Jobs und Sicherungsmedien, werden in der Software abgebildet.

Alle Prozesse lassen sich in einer zentralen Oberfläche überprüfen und managen. Hieraus lassen sich mit wenigen Klicks Reports erstellen, z.B. für Unternehmensprüfungen. Die Reports garantieren eine maximale Transparenz und Sicherheit.

Bei Veränderungen an den Daten oder Systemen oder bei Fehlern gibt die Software eine Rückmeldung, sodass Sie die notwendigen Änderungen direkt vornehmen und ins Backup-Konzept übernehmen können. Das Backup-Konzept bleibt somit auf dem aktuellen Stand und synchron mit der Software.

So wird die Komplettlösung nicht nur der Kern für die unternehmensweite Datensicherung, sondern auch eine zeitsparende Lösung.

> **Das Backup-Konzept und der Disaster Recovery Plan bilden die Basis für die Implementierung und den Betrieb der Datensicherungs-Software.**



5. Disaster Recovery Plan

Der Disaster Recovery Plan beinhaltet alle wichtigen Informationen wie Prozesse, Prioritäten, Verträge oder auch Zuständigkeiten, um im Ernstfall dafür zu sorgen, dass Systeme und Daten schnell und rechtssicher wiederhergestellt werden.

Denn angesichts kleinerer Datenverluste unterschätzt man leicht den Stress und die Zahl der zu koordinierenden Aufgaben, die ein Komplettausfall auslöst. Der Disaster Recovery Plan sollte immer den aktuellen Stand der IT-Infrastruktur abbilden und regelmäßig überprüft werden.

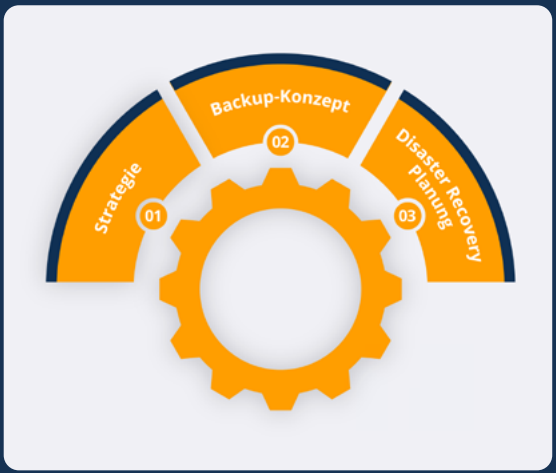
Ist im Notfall der Hersteller Ihrer Datensicherungslösung schnell erreichbar? Ist Hardware für den Disaster Recovery Fall vorhanden? Sind der IT-Abteilung die Business-Prioritäten bekannt? Die Backup-Verantwortlichen kennen in der Regel die Business-Prioritäten nicht, wissen aber welche Kerndienste laufen müssen, bevor eine Anwendung verwendet werden kann. Deshalb gilt:

Regeln Sie die Verantwortlichkeiten und Zuständigkeiten und stimmen Sie die Business- und Technik-Anforderungen aufeinander ab. Und nur, wenn das gelingt, erfüllt die Backup-Software ihr Ziel – und Ihre Datensicherungsstrategie ist erfolgreich umgesetzt.

Welche Ziele verfolgt ein Disaster Recovery Plan?

- ✓ Alle wichtigen Informationen und Prozesse nachvollziehbar schriftlich festgelegen
  - Welcher Notfall erfordert welche Maßnahmen?
  - Wer ist für was verantwortlich?
  - Wer muss verständigt werden?
- ✓ Ausfallzeiten minimieren und finanzielle Schäden verhindern
- ✓ Business relevante Prioritäten festlegen
- ✓ Schnelle Wiederherstellung der Systeme und Daten sicherstellen
- ✓ Checkliste für Wiederherstellungsszenarien
- ✓ Klare Verantwortlichkeiten
- ✓ Notfall-Zugriff für Kontaktdaten, Checklisten, Handlungsanweisungen, Zugangsberechtigungen...
- ✓ Regelmäßige Notfall-Tests und Schulungen

Der Disaster Recovery Plan stellt sicher, dass alle wichtigen Informationen wie Prozesse, Kontakte, Checklisten, Handlungsanweisungen, Zugangsberechtigungen usw. für den Desaster-Fall zur Verfügung stehen.



6. Fazit: Schnelle Betriebswiederherstellung im Desaster-Fall mit einer Komplettlösung

Daten sind die Lebensader moderner Organisationen. Wer die Datensicherung in einem Unternehmen verantwortet, hat eine zentrale Herausforderung zu bewältigen: Nach einem Verlust müssen geschäftskritische Daten wieder zur Verfügung stehen - und zwar innerhalb eines definierten Zeitfensters und bei begrenztem Budget. Um dieses Ziel zu erreichen, muss Datensicherung als ganzheitlicher, dynamischer Prozess verstanden werden, der eine Komplettlösung braucht. Es geht nicht mehr um ein Backup, es geht um eine ganzheitliche Disaster Recovery Lösung.

Nur wenn die Software, die unternehmerischen und technischen Anforderungen (Strategie) und das Backup-Konzept sowie der Disaster Recovery Plan aufeinander abgestimmt sind, ist eine hohe Sicherheit gewährleistet.

Über NovaStor

NovaStor ist der einzige deutsche Lösungsanbieter und Hersteller für Datensicherung, der Backup, Restore und Langzeitaufbewahrung als ganzheitliche Lösung anbietet, um Unternehmen, Behörden und Rechenzentren zu entlasten und einen optimalen Schutz vor Datenverlust zu gewährleisten. NovaStor verbindet Expertise aus hunderten Backup-Projekten mit interner Entwicklungskompetenz, um sowohl Standard- als auch Individualprojekte umzusetzen.

Mit bewährten Datensicherungs- und Archivierungslösungen schützt NovaStor heterogene IT-Infrastrukturen sowie verteilte und wachsende Daten auf sämtlichen Speichertechnologien von Disk über Tape bis Cloud. NovaStor übernimmt Verantwortung für die Datensicherung und -wiederherstellung. Die einzigartige Kombination aus Service-Leistungen, Software und technischem Premium-Support direkt aus Hamburg garantiert die Verfügbarkeit der Daten, auch nach Cyber-Angriffen.

NovaStor ist inhabergeführt und entwickelt seine Lösungen zu 100% in Deutschland.

Quellen:

[1] https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2023-press-de.html

Zum Anfang »