NOVASTOR

Globale IT-Risiken minimieren. In 30 Tagen zu der deutschen Backup-Lösung wechseln!

Das Whitepaper zeigt auf, wie der Wechsel zu einer Backup-Komplettlösung professionell, in fünf Schritten und nur vier Wochen gelingt.

Einleitung

Die zunehmende Digitalisierung und Vernetzung verstärken bei IT-Verantwortlichen vieler Organisationen bereits seit Jahren das IT-Sicherheitsbedürfnis. Durch komplexer werdende Infrastrukturen, steigende Datenmengen und hohe Kosten bei Datenverlust rückt Datensicherung immer mehr in den Fokus.

Der Angriff Russlands auf die Ukraine im Februar 2022 ist eine geopolitische Zäsur in vielen Bereichen, insbesondere die IT-Industrie ist stark betroffen. Zunehmende Cyberattacken und die Warnungen des BSI (Bundesamt für Sicherheit in der Informationstechnik) vor russischen Produkten, insbesondere Kaspersky, zeigen, wie wichtig das Vertrauen in die Hersteller von IT-Produkten geworden ist, neben der reinen Funktionalität und dem Preis der Backup Software.

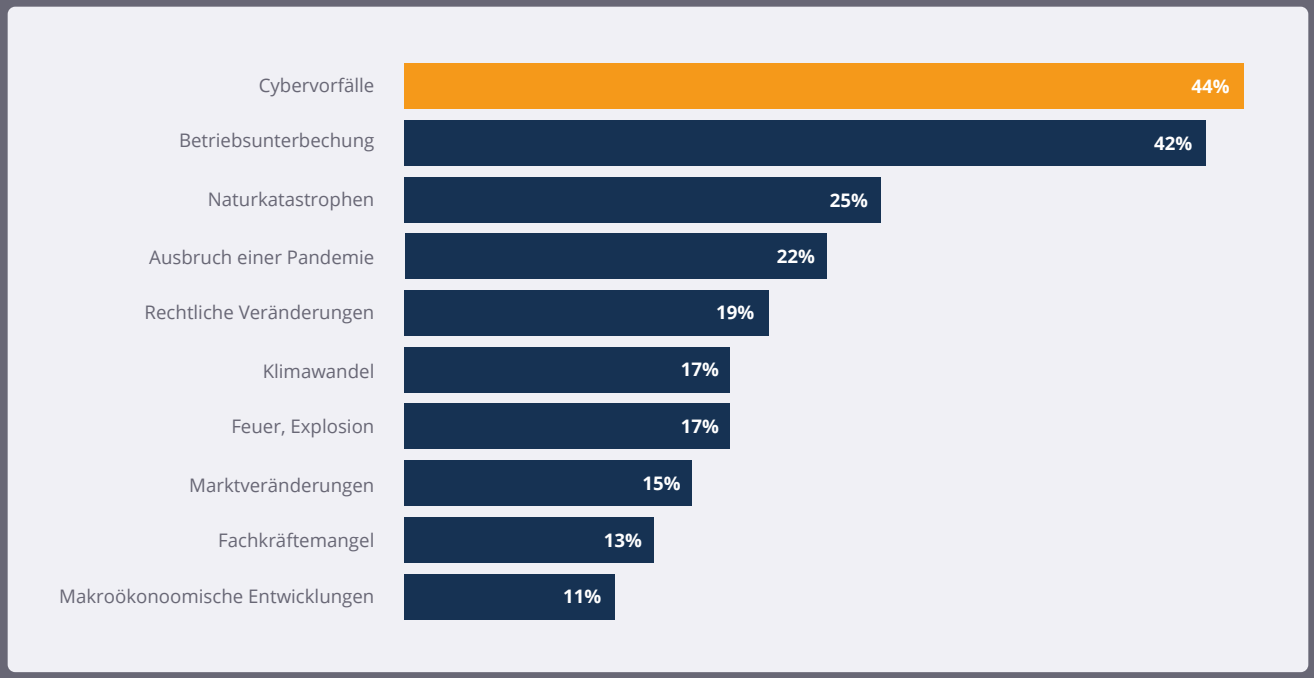
Das Whitepaper zeigt auf, wie die Migration zu einer ganzheitlichen Datensicherungslösung in wenigen Schritten und in einem überschaubaren Zeitraum gelingt. NovaStor empfiehlt für einen schnellen, professionellen Wechsel ein stringentes Vorgehen und das Hinzuziehen von Experten.

Neben technischen Aspekten, werden rechtliche Aspekte und die Wirtschaftlichkeit betrachtet.

Risiko Datenverlust

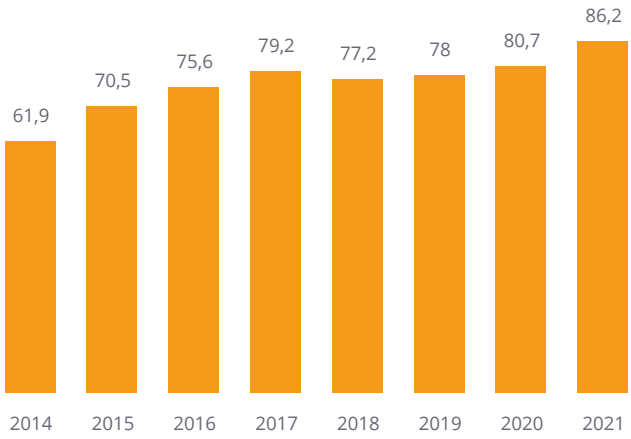
Der Verlust von Daten kann für viele Unternehmen existenzbedrohend sein. Dies liegt nicht nur an der zunehmenden Digitalisierung, sondern auch an der Vernetzung entlang der Lieferkette.

Der Allianz Risk Barometer zeigt deutlich, dass die Unternehmen heute Cybervorfälle (und damit insbesondere Datenverluste oder eingeschränkte Datenverfügbarkeit) als das höchste Geschäftsrisiko einordnen.[1]



▶ Top 10 Geschäftsrisiken weltweit in 2022, Allianz Risk Barometer 2022

Dass das Risiko eines Datenverlustes aufgrund eines Cyberangriffs real ist, zeigt eine Untersuchung der Cyberedge Group 2021. Nach dem Report waren in 2021 alleine bereits mehr als 85% aller Unternehmen von einem Cyberangriff betroffen.[2]



▶ Report der Cyberedge Group

Die meisten dieser erfolgreichen Cyberangriffe hatten nur sehr begrenzte Auswirkungen und haben keinen oder keinen größeren Schaden angerichtet.

Insgesamt ist die deutsche Wirtschaft aber mehr denn je von Cyberangriffen betroffen. Insgesamt 223 Milliarden Euro beträgt der wirtschaftliche Schaden, welcher in 2021 durch Cyberattacken verursacht wurde.[3] Dies geht aus einer Studie des Digitalverbands Bitkom hervor, für die mehr als 1.000 Unternehmen aus unterschiedlichen Branchen befragt wurden.

Zusammenfassend lässt sich sagen, dass ein Cyberangriff kaum zu verhindern ist. Um Datenverluste zu vermeiden, hilft nur die Implementierung einer leistungsfähigen Backup-Lösung, die als letzte Verteidigungslinie die Verfügbarkeit der Daten nach einem Cyberangriff sicherstellt.

Gründe, die existierende Backup-Lösung zu ersetzen

Fast alle Unternehmen und Behörden haben heute bereits eine Datensicherung. Es gibt aber viele Gründe, warum die existierende Datensicherung den erhöhten Anforderungen nicht mehr entspricht:

- Unzuverlässigkeit bei der Datensicherung / Datenwiederherstellung
- Hohe Lizenzkosten und sehr viel Betreuungsaufwand
- Wachsende Datenmengen führen zu unakzeptablen Backup-Zeiten
- Die verfügbaren Zeitfenster reichen für den Restore nicht aus
- Technischer Support durch den Hersteller ist unzureichend
- Interne IT verfügt nicht mehr über ausreichend Ressourcen zum Betrieb der Datensicherung
- Gesetzliche Vorgaben zum Datenschutz werden nicht eingehalten (z.B. DSGVO)
- Backup-Hersteller arbeitet intransparent und ist nicht vertrauenswürdig
- Software-Lösung wird in autokratischen Ländern entwickelt oder der Support erfolgt von dort aus

Sicherlich gibt es noch viele weitere Faktoren, warum die existierende Backup-Lösung ersetzt werden muss. Die meisten Unternehmen wollen im Zuge der Erneuerung der Backup-Lösung zu einer ganzheitlichen Lösung wechseln, damit sie die Verantwortung für die Datensicherung, zumindest teilweise, an den Hersteller oder ein Systemhaus auslagern können. Konkret heißt das: Neben der Backup-Software wünschen sich die Unternehmen Service-Leistungen und Unterstützung von der Implementierung bis in den laufenden Betrieb sowie einen deutschsprachigen, gut erreichbaren technischen Support.

In fünf Schritten zur neuen Backup-Lösung

NovaStor positioniert sich als Hersteller und Lösungsanbieter für Datensicherung. Daher steht bei der Migration immer die Komplettlösung im Mittelpunkt. Die Basis stellt die in Hamburg entwickelte Backup-Software NovaStor DataCenter dar.

Der Wechsel, die Implementierung und der Betrieb einer Komplettlösung besteht im Idealfall aus fünf Schritten: Beginnend bei einer Analyse und Beratung, über die Erstellung eines Backup-Konzeptes, die eigentliche Software-Implementierung bis zur regelmäßigen Überprüfung der Funktionalitäten inkl. ausführlicher Backup- & Restore-Tests. Der deutschsprachige Support durch die Hamburger Backup-Experten stellt die Funktionssicherheit langfristig sicher und hilft bei Fragen oder Problemen.

1. **Beratung**
2. **Erstellung Backup-Konzept**
3. **Software-Implementierung**
4. **Überprüfung der Funktionalitäten**
5. **Deutschsprachiger Support aus Hamburg**

Teile der Komplettlösung können auch von Dritten, z.B. IT-Dienstleistern, erbracht werden und gerade die ersten beiden Schritte (Beratung und Backup-Konzept) sind unabhängig von der eingesetzten Software.

Der gesamte Migrationsprozess für eine mittelgroße Umgebung sollte nicht länger als vier Wochen in Anspruch nehmen und eine deutliche Verbesserung der Backup-Lösung erzielen. In kleineren Umgebungen kann die Beratung sogar schon in der Erstellung eines Backup-Konzeptes münden, womit nochmal Zeit und Kosten eingespart werden.

Schritt 1: Bestandsaufnahme und Beratung

Im ersten Schritt erfolgt eine initiale Beratung durch NovaStors Backup-Spezialisten. Hierbei wird der Status Quo aus technischer, wirtschaftlicher und rechtlicher Sicht festgestellt. Im Rahmen dieser Analyse stellen wir sehr oft fest, dass die mit der Datensicherung betrauten Personen viele der Fragen nicht direkt beantworten können oder auch nicht wissen, wie diese Informationen zu finden sind. NovaStors Experten stehen mit ihrer Erfahrung und wertvollen Analyse-Tools zur Seite.

Folgende Fragen sollten nach der Bestandsaufnahme beantwortet werden können:

- Wie ist das Unternehmen / die Organisation eingeordnet? Gerade bei Unternehmen mit kritischer Infrastruktur muss die Datensicherung, insbesondere die Dokumentation, etwas aufwändiger gestaltet werden, da es spezielle Vorgaben und Richtlinien gibt.
- Existiert ein schriftliches Backup-Konzept und wird es regelmäßig aktualisiert?
- Gibt es einen IT-Notfallplan, der mit dem Backup-Konzept synchronisiert wird?
- Welche gesetzlichen und Compliance Vorgaben existieren und gibt es im Unternehmen Daten, die besonders zu behandeln sind?
- Welche Größe hat die aktuelle Infrastruktur?
- Welche Planung ist für die nächsten drei bis fünf Jahre sinnvoll, basierend auf dem Datenwachstum und strategischen Überlegungen?
- Wo liegen die Stärken und Schwächen der aktuellen Lösung, wo besteht Verbesserungsbedarf? Wichtig ist, ob die Lösung unter Wartung ist und ob es in der Vergangenheit Probleme mit der Datensicherung gegeben hat.
- Hat es schon mal Datenverluste gegeben und was waren die Gründe dafür? Welche Maßnahmen wurden eingeführt, um Datenverlusten künftig vorzubeugen?
- Ist eine Auslagerung der Daten notwendig? Nach dem 3-2-1 Prinzip ist eine Auslagerung generell sinnvoll und notwendig. Wie ist diese Auslagerung gewünscht? Gibt es rechtliche Rahmenbedingungen, warum bestimmte Auslagerungen nicht möglich sind?
- Wie sind die Zuständigkeiten und Verantwortlichkeiten für die Datensicherung im Unternehmen geregelt? Sind diese transparent kommuniziert und schriftlich festgehalten?
- Werden regelmäßige Backup und Restore Checks, sogenannte Health Checks durchgeführt und wie sind die Ergebnisse dokumentiert worden?
- Wie sind die Wartung und technische Betreuung organisiert? Arbeiten Sie mit einem Systemhaus oder dem Hersteller direkt zusammen?
- Soll die Datensicherung zukünftig intern oder extern betrieben werden? Sollen Teile der Verantwortung ausgelagert werden?

Diese und weitere Fragen werden mit der Bestandsaufnahme im Rahmen eines eintägigen Workshops besprochen. Die Ergebnisse fließen in die Dokumentation und Analyse und werden im Rahmen einer Nachbesprechung ausgewertet.

Zusammenfassung:

Auf Basis der Bestandaufnahme und der Ergebnisse können die NovaStor Experten bereits einen Kostenrahmen für die nächsten Schritte, die benötigten Lizenzen sowie den möglichen Betrieb erarbeiten. Somit haben Sie zu jedem Zeitpunkt vollständige Transparenz.

Schritt 2: Prüfung und Erstellung eines Backup-Konzeptes

Bei den meisten Kunden und Systemhäusern liegt bereits „eine Art“ Backup-Konzept vor. Bei genauer Prüfung zeigt sich oft, dass es sich lediglich um eine Auflistung der Systeme oder ein veraltetes Dokument handelt. Als Basis für eine echte Backup-Strategie oder eine Implementierung ist dies leider unzureichend.

Bei der Erstellung des Backup-Konzeptes werden die Informationen aus Schritt 1 verarbeitet und tiefergehende Fragen gestellt. Da NovaStor mit konzeptionellen Vorlagen arbeitet und Erfahrung aus zahlreichen Projekten mitbringt, ist ein effizientes Arbeiten garantiert. Folgende Punkte werden erarbeitet:

- Anlass für die Erstellung des Backup-Konzeptes: Sinnvoll und notwendig ist ein Backup-Konzept in jedem Fall, aber je mehr Informationen vorliegen, desto gezielter lässt sich das Backup-Konzept erstellen. Gab es beispielsweise einen Cyberangriff, Datenverlust, Umstrukturierungen oder einen Mitarbeiterwechsel? Sollen Daten oder Dienstleistungen ausgelagert werden, wird die Infrastruktur erweitert?
- Ziele des neuen Backup-Systems: Gibt es konkrete Vorgaben für RTO (Recovery Time Objective), RPO (Recovery Point Objective), die Infrastruktur? Gegebenenfalls müssten diese sonst ermittelt bzw. festgelegt werden. Hier gilt es, die Klassifizierung des Unternehmens (KRITIS, ISO o.ä.) und gesetzliche Rahmenbedingungen, Compliance-Vorgaben und die Datenschutzgrundverordnung (DSGVO) zu berücksichtigen.
- Aufnahme der aktuellen Infrastruktur und Backup-Strategie sowie Definition der Ziel-Infrastruktur und der langfristigen Backup-Strategie
- Festlegung der organisatorischen Implementierung und der Verantwortlichkeiten
- Schwachstellen und Maßnahmen zu deren Eliminierung: Wenn die Schwachstellen in der Wertschöpfungskette und damit nicht zu 100% im Einflussbereich des Auftraggebers liegen, sind entsprechende Vorschläge zu erarbeiten.
- Im Ergebnis entsteht ein konkreter und umsetzbarer Vorschlag für die Backup-Strategie, Implementierung und benötigte Hardware, der als Vorlage für die Unternehmensleitung ausgearbeitet werden kann.
- Zum Schluss wird das Backup-Konzept als pflegbare Dokumentation übergeben
- NovaStor kann die Wartung des Backup-Konzeptes im Rahmen von regelmäßigen Health Checks oder als Teil der Betreuungsleistungen übernehmen.

Zusammenfassung:

NovaStors Experten nehmen die benötigten Informationen schnell auf, mit dem Ziel das Backup-Konzept zügig zu erstellen. Je nach Umfang der Umgebung dauert das etwa zwischen einer und vier Wochen. Das Ergebnis ist ein einfach zu wartendes Dokument, welches auch im Rahmen von Audits verwendet werden kann.

Schritt 3: Implementierung der Lösung

Im nächsten Schritt erfolgt die Implementierung der neuen Lösung auf Basis von NovaStor DataCenter. In der Analyse in Schritt 1 und dem Backup-Konzept in Schritt 2 wurde auch definiert, wie bei der Migration der Lösung vorzugehen ist.

Meist empfehlen wir das „RIP and replace“ Szenario, welches sich für alle Umgebungen mit Retention Zeiten von bis zu 90 Tagen eignet. In dem Fall deinstallieren NovaStors Experten die existierende Lösung und installieren die Backup Software NovaStor DataCenter auf der vorhandenen bzw. der Zielinfrastruktur.

In einigen Fällen oder bei Langzeitaufbewahrungen ist es angebracht, die existierende Lösung auf einer kleineren Infrastruktur ausschließlich für Restores weiter zu betreiben. Da NovaStor DataCenter auch über eine Langzeitarchivierungsfunktion verfügt, können sukzessiv auch die länger zu behaltenden Datenbestände übertragen werden. Dies wird im Rahmen des Backup-Konzeptes detailliert festgelegt.

Im Vordergrund steht bei der Implementierung, dass die langfristige Funktionsfähigkeit sichergestellt wird.

- Die Implementierung erfolgt gemäß dem erarbeiteten und verabschiedeten Backup-Konzept. Diese Vorgehensweise ist die sicherste. Alternativ lässt sich eine Best Practice-Implementierung durchführen.

- Im 1. Schritt werden die Backup-Infrastruktur vorbereitet und die Systeme aufgesetzt.
- Danach werden die entsprechenden Backup Jobs, Speicher, Aufbewahrungsfristen usw. angelegt. Hierbei bindet NovaStor den IT-verantwortlichen aktiv in Form eines „Training on the Job“ ein, sodass eine hohe Qualität des regelmäßigen Betriebs sichergestellt wird.
- Im Rahmen der Implementierung werden Backup und Restore Tests durchgeführt, damit sichergestellt ist, dass alle Jobs korrekt laufen.
- Abschließend erfolgt eine Zertifizierung der Umgebung inklusive der Dokumentation von Maßnahmen, die noch erfolgen sollen (z.B. Anschaffung einer Tape Library oder der Auslagerung in die Cloud)
- Da in vielen Fällen der Betrieb durch das Unternehmen selbst oder einen beauftragten Dienstleister erfolgt, erarbeitet NovaStor auch einen Vorschlag für eine regelmäßige Überprüfung, die dann auch von einem Dienstleister erbracht werden kann.

Zusammenfassung:
Das Ziel der Implementierung ist eine ganzheitliche Betrachtungsweise der Datensicherung und die Sicherstellung, dass eine schnelle Verfügbarkeit der Daten jederzeit gegeben ist. Wenn die benötigte Hardware funktionsfähig verfügbar ist, wird für die Implementierung einer mittelgroßen Umgebung ca. eine Woche benötigt.

Schritt 4: Regelmäßige Überprüfung der Datensicherung

Die Implementierung ist abgeschlossen und 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 weiterentwickelt. Je dynamischer eine IT-Umgebung ist, desto wichtiger ist die ganzheitliche Betrachtung der Datensicherung und die regelmäßige Durchführung von simulierten IT-Notfallszenarien.

NovaStor schlägt folgende Maßnahmen vor:

- Durchführung von quartalsweisen oder jährlichen Backup Health Checks, bei denen die Datensicherung auf „Herz und Nieren“ überprüft wird
- Mindestens eine jährliche Überprüfung und Aktualisierung von Backup-Konzept und IT-Notfallplänen
- Regelmäßige Durchführung von IT-Notfallszenarien: Bei größeren Umgebungen ist es von Vorteil nicht alle Szenarien auf einmal durchzuführen, sondern jeweils kleinere Teil-Szenarien.
- Hinzuziehen von Experten zur Vorbereitung und Unterstützung bei Audits (Intern, KRITIS, ISO usw.), wenigstens bei den ersten Audits ist dies empfehlenswert
- Durchführung regelmäßiger Besprechungen zu folgenden Punkten:
  - Feststellung technischer oder organisatorischen Änderungen
  - Infrastruktur-Empfehlungen auf Basis aktualisierter Planungen
  - Definition und Ergreifung von Maßnahmen (Infrastrukturerweiterungen)
  - Review der Datensicherung

Zusammenfassung:
Die fehlende regelmäßige Überprüfung führt schnell dazu, dass die Datensicherung im Notfall nicht mehr die gewünschten Ergebnisse erbringt. Wenn man mit einem Backup-Konzept, IT-Notfallplan und einer

professionellen Implementierung eine gute Grundlage gelegt hat, dann ist die regelmäßige Überprüfung mit geringem Aufwand durchzuführen.

Schritt 5: Technische Betreuung

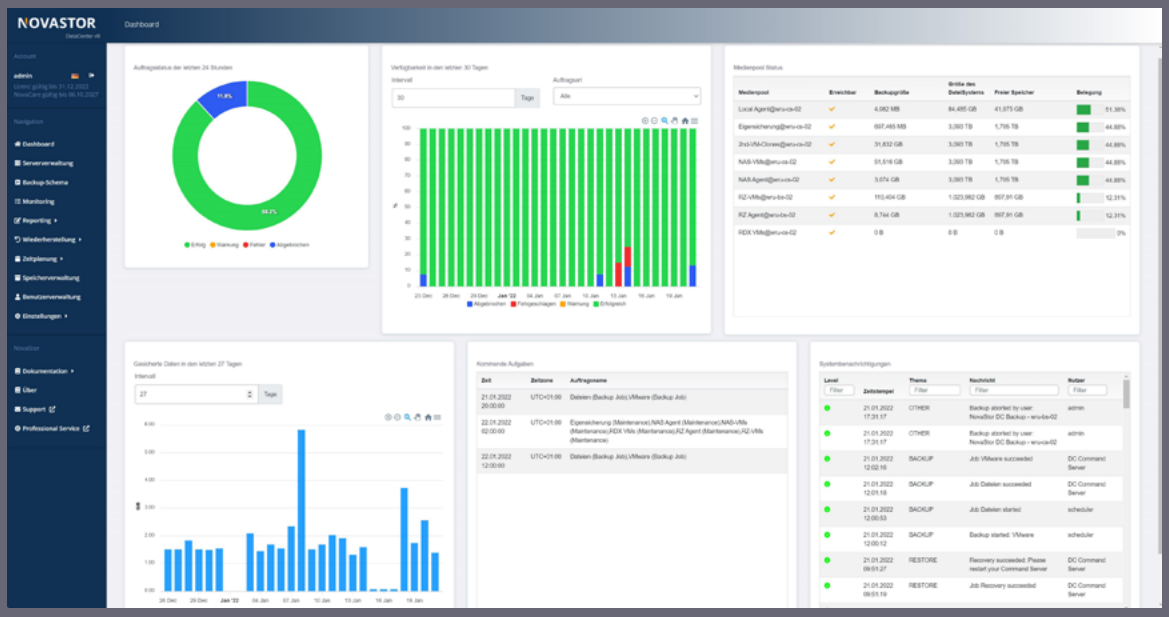
Zu jeder guten Lösung gehören professionelle Ansprechpartner im technischen Support, an die Sie sich wenden können.

NovaStor sieht die technische, deutschsprachige Betreuung durch lokale Backup-Experten als wichtig an und erbringt im Rahmen der Service-Verträge u.a. folgende Leistungen:

- Der technische Support im Rahmen von NovaCare umfasst Updates, Upgrades und Hilfe bei technischen Problemen.
- Jedem Kunden ist ein fester, technischer Ansprechpartner zugeordnet.
- Die Kunden werden proaktiv bei wichtigen Updates informiert.
- Auf Wunsch übernehmen NovaStors Techniker eine Einführung in neue Funktionen von NovaStor DataCenter, die Neuorganisation der Backup Jobs oder geben Hilfe bei komplexen Restores.
- Weitere Leistungen, wie z.B. die Anbindung an eine Tape Library oder die Integration neuer Abteilungen und Standorte erbringen die Techniker im Rahmen von Zusatzleistungen (Professional Services).
- NovaStor bietet regelmäßig Schulungen und Zertifizierungen rund um NovaStor DataCenter sowie das Thema Datensicherung an.
- Managed Backup Services (MBS) by NovaStor gehört zu NovaStors Standard-Leistungen, d.h. NovaStor übernimmt temporär das Management der Backups.

In eigener Sache:

Eine professionelle und zuverlässige Datensicherung ist heute ein unverzichtbarer Bestandteil jeder IT-Infrastruktur. NovaStor schreibt die technische Betreuung von Anfang an groß. Erfahrene Backup-Experten betreuen und beraten die Kunden vom Standort Hamburg aus in allen Belangen rund um die Datensicherung.



Komplettlösung für Backup, Restore und Archivierung

Das Ergebnis einer professionell aufgesetzten Datensicherung auf Basis von NovaStor DataCenter ist eine zuverlässige Lösung, die beständig weiterentwickelt wird. Daher kann NovaStor als deutscher Hersteller und Lösungsanbieter auch Verantwortung für Ihre Datensicherung übernehmen – von der Installation bis in den Betrieb!

Ihre Vorteile:

- Entwicklung und Support in Deutschland
- Zentrale Verwaltung über ein intuitives Web Interface
- Automatisiertes, visuelles Backup Management
- Transparent, zuverlässig und hoch performant
- Mit wenig Aufwand zu managen
- Support für RMM/Monitoring Systeme
- Audit-Reports auf Knopfdruck
- Zusammenarbeit mit Systemhäusern
- Services direkt vom Backup Experten

→ Unternehmen und Systemhäuser können sich jederzeit auf NovaStor verlassen.

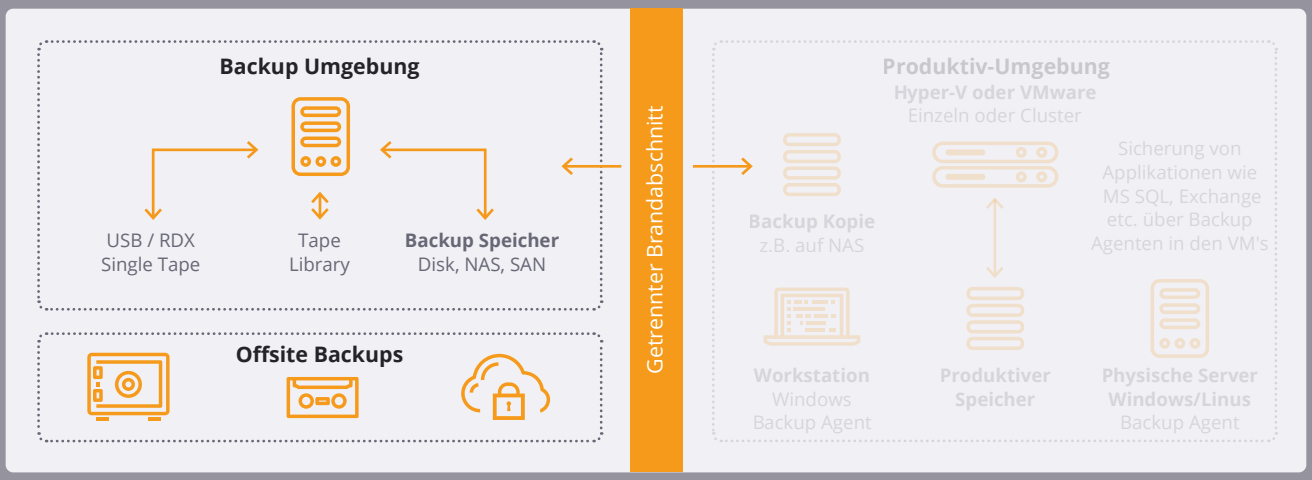
Best Practice Setup gegen Datenverlust bei Cyber-Attacken

Ransomware-Angriffe gelten als eine der größten Bedrohungen für die Datensicherheit und die Business Continuity. Seit 2019 ist die Ransomware-Bedrohung weltweit um 232% gewachsen. Deutschland verzeichnete in 2021 mit einem enormen Anstieg um 3256% sogar die meisten Ransomware-Angriffe in EMEA.[4]

Daher gilt: Wenn Ransomware trotz aller Schutz- und Vorsichtsmaßnahmen in die produktive IT-Umgebung vorgedrungen ist, muss die Backup-Umgebung die letzte Verteidigungslinie bilden, um betroffene Daten und Systeme zeitnah und zuverlässig wiederherzustellen.

Da eine funktionierende Backup-Umgebung jederzeit Ransomware verschlüsselte Daten und Systeme wiederherstellen kann und damit die Lösegeldzahlung hinfällig wird, sind die Backup-Umgebung und die Backups eines der primären Angriffsziele.

Um sowohl die Backup-Umgebung als auch die gesicherten Daten wirksam vor Angriffen und sonstigen Desastern zu schützen, ergreifen Sie folgende Maßnahmen:



1. Backup Umgebung abgeschirmt und getrennt von der Produktiv-Umgebung betreiben

- Der Backup-Server sollte eigenständig und unabhängig von der produktiven Umgebung laufen - für optimale Sicherheit und Verfügbarkeit der Backup-Umgebung.
- Der Backup-Server und die Backup-Speicher sollten nicht Mitglied der Domäne sein.
- Die Backup-Speicher sollten ausschließlich nur dem Backup-Server zugänglich sein, entweder über eigenen HBA angeschlossen, oder zumindest über VLAN getrennt.
- Die Backup-Server Firewall sollte nur zwingend benötigte Ports offen haben.

2. 3-2-1-Backup-Strategie

Die 3-2-1-Backup-Strategie empfiehlt mindestens 3 Kopien der Daten auf 2 unterschiedlichen Speichermedien wovon 1 Backup Kopie an einen externen Standort (Offsite Backup) auslagert wird.[5]

Die 3-2-1-Backup-Strategie ist eine wirksame Ergänzung zu den Schutzmaßnahmen der Backup-Umgebung. Selbst wenn nach einem Desaster lokale Daten und Backups nicht mehr zur Verfügung stehen, sind immer noch die extern gelagerten Backup-Kopien für eine Wiederherstellung verfügbar.

Es gibt verschiedene Möglichkeiten Backup-Kopien auszulagern. Meistens werden die Backup-Kopien auf transportable Medien wie RDX-, USB-, oder Bandmedien geschrieben und anhand einer Strategie zur Medienrotation ausgelagert. Diese Strategie erfordert manuelle Prozesse, die naturgemäß fehleranfällig sind.

Bei einem wichtigen Thema wie Datenverfügbarkeit und Business Continuity sollte die Fehleranfälligkeit so gering wie möglich gehalten werden. Um das 3-2-1 Backup komplett zu automatisieren, empfiehlt es sich, die Backup-Kopien mittels eines regelmäßigen Zeitplans über die Cloud zu einem externen Standort wie einem sicheren Rechenzentrum der Wahl oder einer Colocation zu übertragen.

3. Windcloud: CO_2 neutrales Cloud Backup

NovaStor setzt bei der Wahl des Cloud Backups 100% auf den Standort Deutschland und hat eine Kooperation mit der Windcloud 4.0 GmbH in

Enge-Sande, Schleswig-Holstein. Windcloud bietet Cloud Storage in Deutschland an und stellt zu 100% sicher, dass die Daten DSGVO-konform gespeichert werden. Weiterhin gewährleistet Windcloud, dass die Rechenzentrumsleistungen zu 100% aus erneuerbaren Energien betrieben werden. Darüber hinaus wird die Abwärme der Server direkt vor Ort in einer Algenfarm veredelt.[6] Selbstverständlich können Sie mit NovaStor DataCenter auch andere Cloud-Anbieter anbinden und die Daten dort speichern.

Ergebnis: Sicherstellung einer funktionierenden Datensicherung

Das Ergebnis einer Zusammenarbeit mit NovaStor ist in jedem Fall eine funktionierende Datensicherung, die nicht nur die technischen, sondern auch die organisatorischen Anforderungen erfüllt.

Schriftliche Festlegung im Backup-Konzept

Definition der geschäftskritischen Daten und Systeme, Verfügbarkeiten, Maßnahmen

Compliance & gesetzliche Anforderungen

Backup Strategie, Sicherheitsmaßnahmen, Verantwortlichkeiten

Prüfung der Backup Umgebung

Reports – läuft alles ordnungsgemäß

Health-Check – Prüfung der Backup Umgebung und Prozesse

Restore-Tests – können die Daten/Systeme im gewünschten Umfang wiederhergestellt werden?

Räumlich getrennte Verwahrung der Kopien

3-2-1 Backup Regel beachten

Systeme müssen nach einem Desaster zeitnah wiederhergestellt werden können

Redundanzen erhöhen die Verfügbarkeit und Datensicherheit

IT-Notfall Handbuch

Schneller und geregelter Restore im Notfall

Kontaktliste und Handlungsanweisungen zu Sofortmaßnahmen

Wiederanlaufpläne mit Checklisten

Auf einen Blick: NovaStors Leistungen für Sie

Unsere ganzheitliche Datensicherungslösung visualisiert komplexe Backup-Prozesse übersichtlich, entlastet Backup-Verantwortliche und sorgt dafür, dass Sie das Schlimmste verhindern können, wenn Ihre Organisation von Ransomware angegriffen wird.

NovaStors Komplettlösung umfasst unter anderem eine performante Software, ein Backup-Konzept und regelmäßige Backup Health Checks.

1. Experten entwickeln für Sie ein Backup-Konzept und halten es schriftlich fest.
2. Im nächsten Schritt stellen sie sicher, dass die Sicherung wie gewünscht erfolgen.
3. Und sie testen bereits vorhandene Sicherungen daraufhin, ob die Medien lesbar sind und sich die fraglichen Systeme im gewünschten Umfang wiederherstellen lassen.

Über NovaStor

Als deutscher Hersteller und Lösungsanbieter entwickelt NovaStor Software für Backup, Restore und Archivierung und entlastet IT-Abteilungen mit Dienstleistungen von der initialen Konzeption bis in den laufenden Betrieb. 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 verbindet Expertise aus hunderten Backup-Projekten mit interner Entwicklungskompetenz, um sowohl Standard- als auch Individualprojekte umzusetzen. Unternehmen, Behörden und Rechenzentren erhalten von NovaStor zukunftssichere Lösungen für Datensicherung und Archivierung.

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-2022-press-de.html

[2] https://www.isc2.org/-/media/ISC2/Research/Cyberthreat-Defense-Report/2021/CyberEdge-2021-CDR-Report-v10--ISC2-Edition.ashx

[3] https://www.bitkom.org/sites/default/files/2021-08/bitkom-slides-wirtschaftsschutz-cybercrime-05-08-2021.pdf

[4] https://www.all-about-security.de/threats-und-co/alarmierender-anstieg-bei-ransomware-und-boesartigen-cyberangriffen-sowie-eine-verdopplung-der-bedrohungen-in-2021)

[5] https://www.storage-insider.de/was-ist-die-3-2-1-backup-regel-a-782641/

[6] https://windcloud.de/unternehmen/ueber-uns

Zum Anfang »