NOVASTOR

Backup & Restore Strategien für Unternehmen

Was bedeuten die Entscheidungen, die Sie beim Sichern Ihrer Daten treffen, für die Wiederherstellung? Verschaffen Sie sich einen Überblick, mit welchen Strategien Sie Ihre angestrebten Ziele erreichen.

Backup & Storage-Konzepte – Eine Hilfestellung

Über die Notwendigkeit von Datensicherungen in Unternehmen gibt es nichts zu diskutieren; über das Wie, Wann, Womit und Wohin umso mehr. Auch wenn es auf den ersten Blick so scheint, stehen Backup-Verantwortliche nicht vor der Aufgabe, sämtliche Daten im Unternehmen einfach zu sichern.

Vielmehr stehen sie vor der Herausforderung, die Gegebenheiten des Unternehmens zu analysieren und zu erfassen, was gesichert werden muss, und welche Möglichkeiten dafür zur Verfügung stehen. Schließlich gilt es, aus den Hunderten möglichen Backup-Lösungen diejenige zu identifizieren, die am besten zum Unternehmen passt.

Welche Aspekte und Vorgehensweisen helfen, einen Anfang zu finden und belastbare Entscheidungen zu treffen, behandelt das folgende Dokument.

Daten qualifizieren – Backup auf der Ort- / Zeit-Achse

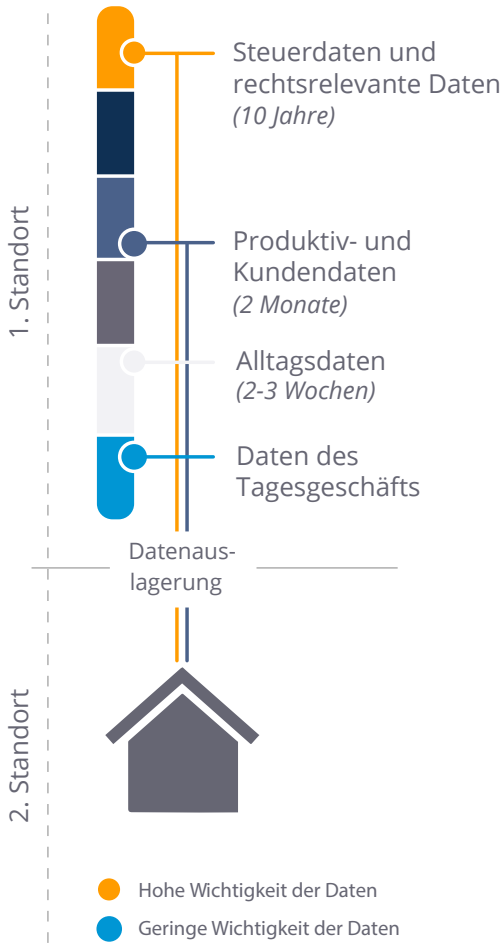
Begrenzte Budgets und begrenzte Speicherkapazitäten erfordern einen möglichst effektiven Umgang mit den zur Verfügung stehenden Möglichkeiten. Darum beginnt Backup bei den Produktivsystemen - mit der Qualifikation der zu sichernden Daten, Systeme und Anwendungen. Die Einordnung der Daten für die Datensicherung 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 Siche-

rung unterschiedlichen Vorgaben. Beispielsweise müssen steuerlich relevante Buchhaltungsdaten deutlich länger verfügbar bleiben als die tägliche E-Mail-Korrespondenz. Doch 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. Allerdings kann eine Kopie Unternehmen nur zuverlässig vor einem Datenverlust durch den Ausfall der ursprünglichen Sicherung schützen, wenn die Kopie sich an einem anderen Standort befindet als das Original. Im Backup-Konzept spiegelt diese Anforderung sich im Schritt der Datenauslagerung an einen zweiten Standort wider.

Exemplarische Unterteilung von Daten nach Aufbewahrungsdauer und -ort



Wichtige Fragen zur Evaluierung einer passenden Backup-Lösung

- Wie erfolgt die Datensicherung?
- Wer ist verantwortlich?
- Welche Daten sichern Sie?
- Wann führen Sie die Datensicherung durch?
- Welches Speichermedium wollen Sie nutzen?
- Wo bewahren Sie die Datensicherung auf?
- Wie schützen Sie die Datensicherung, z.B. vor Zerstörung durch Dritte?
- Wie lange wollen/müssen Sie die Datensicherung aufbewahren?

D2D/T – Die Basis der Backup-Architektur

Die Datensicherung erfasst alle geschäftskritischen Daten mindestens einmal: Von den Servern im Netzwerk überträgt die Backup Software die Daten auf ein Sicherungsmedium. Für die Ausgestaltung dieser Sicherung haben Verantwortliche zahlreiche Möglichkeiten, die Datensicherheit und –verfügbarkeit auf unterschiedliche Art zu beeinflussen.

Das Speichermedium: Disk, Tape oder Cloud?

Die Frage, ob die Sicherung des Unternehmensservers auf Disk, Tape oder Cloud erfolgen soll, stellt sich den meisten kleinen und mittelständischen Unternehmen nicht. Der hohe Nutzerkomfort von Festplattensystemen – ob eine einzelne USB-Platte oder RDX - sticht etwaige Preisvorteile

von Magnetbändern aus. Nur, wer eine grundsätzliche Affinität zu Tape verspürt oder seine einzige Sicherung abends aus dem Unternehmen transportieren möchte, wird das Magnetband der gegenüber Stößen empfindlicheren Festplatte vorziehen.

Auf Basis der anfänglichen Einteilung von Daten empfiehlt es sich, unterschiedliche Partitionen des Speichers für unterschiedliche Datentypen zu reservieren. Backup Jobs für Daten von niedrigerer oder höherer Wertigkeit stehen damit auf demselben Medium voneinander unabhängige Partitionen zur Verfügung.

Aufgrund von Bandbreitenbeschränkungen und Vorbehalten gegenüber der Einhaltung von Datenschutzrichtlinien durch den Anbieter spielt die Cloud in einstufigen Backup-Konzepten von kleinen und mittelständischen Unternehmen bisher kaum eine Rolle.

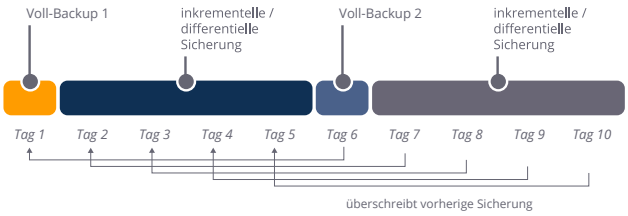
Aufbewahrungsdauer

Ob Disk oder Tape – um Speichermedien effizient zu nutzen, werden Datensicherungen regelmäßig überschrieben. Hierfür definieren Backup-Verantwortliche in ihren Backup-Aufträgen den Zeitraum, nach dem die Backup Software die erste erstellte Sicherung überschreibt.

In einem klassischen „First in, first out"-Konzept[1] kann beispielsweise an Tag eins eine Vollsicherung einer Anwendung laufen, während an den folgenden vier Tagen inkrementelle oder differentielle Sicherungen stattfinden. Am sechsten Tag erfolgt eine neue Vollsicherung, welche die erste Vollsicherung überschreibt. In der Folge werden alle inkrementellen und differentiellen Sicherungen, die sich auf die erste Vollsicherung beziehen mit Sicherungen überschrieben, die sich auf die neue Vollsicherung beziehen.

Steht ausreichend Speicherplatz zur Verfügung können Unternehmen mehrere Vollsicherungen mit zugehörigen inkrementellen / differentiellen Sicherungen erstellen, bevor sie die erste Vollsicherung überschreiben.

Beispiel: First in, First out-Rotationssicherung im 5-Tages-Rhytmus



Daten, die an Tag 1 im Produktivsystem vorhanden waren, aber am fünften Tag aus dem produktiven System gelöscht wurden, können in dem oben skizzierten Beispiel ab dem sechsten Tag nicht mehr aus den Sicherungen rekonstruiert werden. Aus diesem Grund sollte die Aufbewahrungsfrist nicht zu kurz gewählt oder als Stellschraube bei knapp werdendem Speicherplatz genutzt werden.

[1] Typische Alternativen zu „First in, first out" sind Strategien wie „Grandfather-Father-Son" oder „Tower of Hanoi".

Standards für schnelles und sparsames Backup & Restore

Um ohne Geschwindigkeitsverluste Speicherplatz zu sparen, können Anwender nach einer initialen Vollsicherung inkrementelle oder differentielle Sicherungen einsetzen. Maßgeblich für die Entscheidung für inkrementelle oder differentielle Sicherungen ist die Frage, welcher Vorteil für den Anwender im Vordergrund steht: Eine möglichst effiziente Speichernutzung oder möglichst kurze Restore-Fenster?

Setzt man auf eine sparsame Speichernutzung und kurze Backup-Fenster auf Kosten längerer Restore-Fenster empfiehlt sich die Kombination von Vollsicherung und inkrementeller Sicherung. Die inkrementelle Sicherung erfasst nur die Daten, die sich seit dem letzten Backup verändert haben. Die Wiederherstellung erfordert die Vollsicherung und sämtliche inkrementelle Sicherungen, die bis zum Restore-Zeitpunkt entstanden sind. Die differentielle Sicherung dagegen erfasst bei jedem Backup sämtliche Änderungen an den Daten seit der letzten Vollsicherung und ermöglicht so einen schnelleren Restore.

Nutzt man differentielle Sicherungen reichen für den Restore des aktuellen Datenbestands die Vollsicherung und die jüngste differentielle Sicherung.

Unabhängig von Speicherplatz sowie Backup- und Restore-Fenstern bietet die Kombination aus Vollsicherung und differentiellen Sicherungen einen weiteren Vorteil. Da für den Restore grundsätzlich nur zwei Sicherungen genutzt werden – die Vollsicherung und eine differentielle Sicherung – , erzielt der Einsatz differentieller Sicherungen eine deutlich geringe Komplexität und Fehleranfälligkeit als inkrementelle Sicherungen und Incremental Forever.

Incremental Forever

Die Strategie, nach einer ersten Vollsicherung ausschließlich inkrementelle Sicherungen durchzuführen, nennt sich Incremental Forever. Damit das Konzept beim Restore aufgeht, muss die eingesetzte Backup Software synthetische Backups unterstützen. Diese lösen den Konflikt zwischen differentiellen und inkrementellen Sicherungen per Software-Funktion: Synthetische Sicherungen stellen die gesicherten Daten aus einer vollen und beliebig vielen inkrementellen Sicherungen in einem Schritt wieder her.

Auf Basis von Informationen, die in den Metadaten hinterlegt sind, setzt die Backup Software die inkrementellen Sicherungen so zusammen, dass sie einer Vollsicherung des aktuellen Datenbestands entsprechen. Damit soll der Restore aus einem synthetischen Backup dem Restore aus differentiellen Sicherungen in nichts mehr nachstehen.

> **Tipp:**
>
> Incremental Forever erfordert die Verfügbarkeit der Metadaten. Achten Sie daher auf den Einsatz einer Software, die Metadaten verteilt hält. Befinden die Metadaten sich ausschließlich in einer zentralen Datenbank kann bei einem Ausfall der Datenbank kein Restore mehr stattfinden.

Vorteile mehrstufiger Backup-Architekturen

Unabhängig davon, welches Speichermedium und welche Sicherungsstrategien ein Unternehmen wählt, einstufige Backup-Architekturen haben eine große Schwäche: Im Verlustfall hängt der Erfolg des Restores an der Lesbarkeit eines einzigen Backup-Mediums. Darum setzen Unternehmen für Daten, die als besonders wichtig eingestuft werden, auf mehrere nachgeschaltete Backup-Speicher. Ob D2D2D oder D2D2T – mehrstufige Backup-Architekturen erweitern den Handlungsspielraum der Backup-Verantwortlichen deutlich.

Zu den Möglichkeiten mehrstufiger Backup-Architekturen zählen:

- Schutz vor Datenverlust durch Sicherungsverlust
- Paralleler Einsatz unterschiedlicher Medientypen
- Schutz vor lokalen Bedrohungen der Daten
- Unbegrenzte Aufbewahrungsfristen

Erweitert man das grundlegende Backup-to-Disk um eine Stufe, kann man alternative Medien mit spezifischen Vorteilen nutzen und einen weiteren Standort einführen. Zusammen ergibt sich eine Backup-Strategie, die Unternehmen vor jedem denkbaren Datenverlust schützt und eine Vielzahl von Aufbewahrungsfristen zulässt.

Disk-to-Disk-to-? – Was kommt nach der ersten Sicherung?

Sind die Daten einmal gesichert, kann ein Defekt des Backup-Mediums auftreten und die Sicherungsmaßnahme unterlaufen. Beispielsweise kann die Ursache für den Verlust der Produktivdaten zugleich die Datensicherung zerstören – wie im Fall von Überschwemmungen, Diebstahl oder Vandalismus.

Es stellt sich die Frage, welches Medium die Schwachstelle des D2D-Konzeptes optimal behebt. Betreibt ein Unternehmen ein Rechenzentrum befindet sich das Backup üblicherweise in einem anderen Brandabschnitt als die Produktivdaten. In kleinen oder IT-fremden Umgebungen besteht diese Möglichkeit in den seltensten Fällen. Die zweite Sicherungsstufe bietet sich daher als transportable Ebene an. Wird das Disk-Backup auf ein lokal angeschlossenes Magnetband oder eine USB-Platte kopiert, kann diese zweite Sicherung aus dem Unternehmen entfernt werden.

Für die Aufbewahrung außerhalb des Unternehmens eignen sich Schließfächer oder andere Unternehmensstandorte. In jedem Fall sollte vor dem Transport und der Auslagerung eine Verschlüsselung der Datensicherung erfolgen.

Bitte beachten:

Die Lagertemperatur von Magnetbändern wird leicht unter- oder überschritten. Die Herstellerangaben sind zu berücksichtigen. Bereits in einem Servergehäuse verbaute Festplatten erleiden leicht Transportschäden. Ein Transport sollte nur in einer für diesen Zweck produzierten Box erfolgen.

Eine dritte Möglichkeit für die Auslagerung von Daten bieten Cloud-Backup-Dienste. Auch wenn diese sich in den meisten Unternehmen bisher nicht als valide Alternative zu selbst verwalteten Speichern durchgesetzt haben, bieten professionelle Backup Software Produkte bereits heute die Möglichkeit, Cloud-Destinationen ebenso komfortabel auszuwählen und zu nutzen wie Festplatten. Wer in die Cloud sichert, erspart sich den manuellen Transport der Medien und gibt die Verantwortung für die sichere Aufbewahrung der Sicherungen an professionelle Dienstleister ab.

Restore-Geschwindigkeit: Disk, Tape oder Cloud?

Während Festplatten per Plug-and-Play zur Verfügung stehen, erfordern Magnetbänder einen Ladevorgang, der den Beginn des Restores verzögert. Dennoch erzielen Restores von Disk nicht grundsätzlich die kürzeren Restore-Fenster.

Auf Magnetbändern werden Daten sequentiell gespeichert; auf Disk werden Daten in kleinen Einheiten auf unterschiedlichen Sektoren abgelegt. Daraus ergeben sich für die Wiederherstellung einzelner Dateien kürzere Restore-Zeiten von Disk als von Tape. Komplette Systeme wiederum können von Magnetbändern schneller als von Disks wiederhergestellt werden.

Die Verfügbarkeit der Daten aus der Cloud kann bei großen Datenmengen kaum mit anderen Medien mithalten. Aufgrund von Bandbreitenbeschränkungen eignet sich der Restore aus der Cloud vor allem für einzelne Dateien. Für große Datenmengen werden die meisten Unternehmen im Restore-Fall auf ein Offline-Medium zurückgreifen, das vom Cloud-Storage-Anbieter zum Kunden transportiert werden muss. Das resultierende Restore-Fenster liegt dadurch deutlich höher als bei lokal verfügbaren Sicherungen. Aufgrund dieser Schwäche bei der Wiederherstellung großer Datenmengen und kompletter Systeme kommt das Cloud Backup nur unter besonderen Bedingungen – beispielsweise, wenn der Cloud-Anbieter in der Nähe des Unternehmens ansässig ist – für unternehmenskritische Systeme in Frage[2].

[2] Auch die Einhaltung europäischer Datenschutzrichtlinien spricht für die Wahl eines lokal ansässigen Anbieters von Cloud-Storage

Mehrere Standorte fürs Backup nutzen

Haben Unternehmen mehrere Standorte empfiehlt es sich, diese für die Backup-Strategie zu nutzen. Soweit es die Entfernung zwischen den Standorten zulässt, können Sicherheitskopien des Backup an den jeweils anderen Standort transportiert und dort gelagert werden. Allerdings sollten Verantwortliche vorab prüfen, ob sie die ausgelagerten Medien über die Backup Software am ur-

sprünglichen Standort per Fernzugriff für einen Restore nutzen können. Der Rücktransport würde im Restore-Fall eine unnötige – und definitiv unerwünschte – Verzögerung bedeuten.

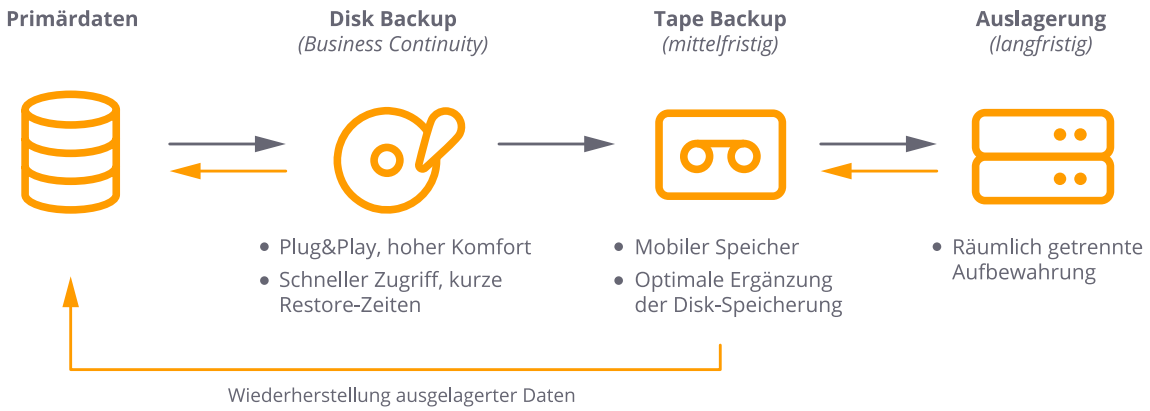
Die eleganteste und beste Art, weitere Unternehmensstandorte für das Backup-Konzept zu nutzen, erfordert den Einsatz einer zentralen Datensicherungssoftware. Geeignete Backup-Produkte erlauben IT-Administratoren, Disk Pools an anderen Standorten direkt als Backup-Ziel – und Restore-Quelle – auszuwählen. Die Lösung bietet vollen Schutz vor Datenverlust durch Schäden am lokalen Backup-Medium, ohne einen Transport und eine externe Lagerung des Mediums zu erfordern.

eigenen Backup Job auf das Auslagerungsmedium kopiert wird.

Die Rolle der Software in Backup-Konzepten

Die Backup Software spielt bei der Umsetzung des Backup-Konzeptes eine zentrale Rolle. Einerseits lassen sich nur Prozesse implementieren, die im Funktionsumfang der Backup Software vorgesehen sind. Zum Beispiel lassen sich in der Backup-Architektur nur Medien nutzen, welche die Backup Software unterstützt. Andererseits eignet sich die Backup Software als Stellschraube für Kostenfaktoren, beispielsweise über die freie Wahl

Backup to Disk to Tape - Das Beste aus 2 Welten



Flexible Aufbewahrungsfristen

Die zweite Sicherungsebene kann neben der Auslagerung zum Zwecke der Absicherung des Backups der besonderen Behandlung wichtiger Daten dienen. Beispielsweise müssen steuerlich relevante Daten über Jahre aufbewahrt und kurzfristig abrufbar sein. Gleiches gilt für andere rechtlich bedeutsame Daten. In der Backup Software lässt sich die Auslagerung wichtiger Daten einfach automatisieren: Zum Zweck der langfristigen Datenaufbewahrung definiert man aus den Backup-Daten ein Subset, das gemäß der Vorgaben in einem

des Storage-Herstellers und damit der Preisklasse.

Über den finanziellen Aspekt hinaus können IT-Verantwortliche mit der eingesetzten Backup Software die Backup-Geschwindigkeit beeinflussen. Über Multistreaming und Multiplexer kann die Backup Software Datensicherungen beschleunigen, indem sie die Backup-Daten eines Auftrags in mehrere parallele Datenströme aufteilt. Je mehr Datenströme, desto kürzer die Sicherung. Diese Funktion können Anwender gleichermaßen für die Wiederherstellung der Daten nutzen, um das Restore-Fenster zu verkürzen.

Fazit: Ein Unternehmen – Eine Backup-Lösung

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.

Den Weg zum Backup-Ziel definieren IT-Verantwortliche in ihrem Backup-Konzept. Dieses liefert Antworten auf zahlreiche Fragen: Wann sollen die Sicherungen stattfinden? Wo stehen die Speichermedien? Wie lange sollen die Backups vorgehalten werden? Welche Daten sollen länger zur Verfügung stehen? Vor welchen Gefährdungen wollen wir uns schützen?

Als Stellschrauben für Zeit- und Kosten-Faktoren dienen die zwei Kernbestandteile jeder Backup-Architektur: Die eingesetzte Backup Software mit ihrem Funktionsumfang und die Speichermedien.

Am Ende steht statt Hunderter möglicher Lösung eine Backup-Lösung, die sich täglich bewähren muss. Backup-Verantwortliche tun gut daran, das Unternehmen im Blick zu halten, dem Aufkommen etwaiger Insellösungen in einzelnen Abteilungen entgegenzuwirken – und die etablierte Backup-Lösung gelegentlich auf den Prüfstand zu stellen.

Über NovaStor

Als deutscher Hersteller und Lösungsanbieter entwickelt NovaStor Backup und Restore Software 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 an drei Standorten vertreten: in Deutschland (Hamburg), den USA (Agoura Hills) und der Schweiz (Rotkreuz).

Zum Anfang »

NovaStor GmbH
www.novastor.de

Neumann-Reichardt-Straße 27-33
22041 Hamburg

kontakt@novastor.de
Telefon: +49 40 638 09 0