WHITEPAPER

NovaBACKUP

LEITFADEN FÜR EINE

EFFIZIENTE BACKUP STRATEGIE

Wie Sie mit einer gut durchdachten Backup-Strategie Datenverluste reduzieren und Betriebsausfälle vermeiden.

INHALT

REDUNDANZ

Redundanz in der Datensicherung einbauen

Da die Verwaltung Ihrer Daten für den Erfolg Ihres Unternehmens immer wichtiger wird, wird auch der Schutz dieser Informationen immer wichtiger. Ihr Tagesgeschäft hängt von diesen Daten ab, und deren Verlust kann katastrophale Folgen haben.

> Nach einem größeren Datenverlust geben fast 70% aller Kleinunternehmen innerhalb eines Jahres auf. [i]

Sie müssen sich von drei Seiten gegen Datenverlust schützen:

1. **Externe Bedrohungen:** Ransomware und andere Schadprogramme werden immer raffinierter. Aber nicht nur Cyber-Angriffe nehmen zu. Auch andere Bedrohungen wie Naturkatastrophen und extreme Wetterbedingungen gehören dazu.

2. **Interne Bedrohungen:** Software- und Hardwarefehler können zu Datenverlusten führen. Und durch menschliches Versagen können Daten versehentlich gelöscht werden.

3. **Remote-Systeme:** Die Zunahme von Remote-Arbeit bedeutet, dass Sie möglicherweise mehr Geräte in verschiedenen Standorten überwachen müssen. Dadurch haben Angreifer mehr Möglichkeiten, in Ihr System einzudringen, und es wird für Sie schwieriger, den Überblick zu behalten.

Vorbeugende Maßnahmen wie die Aktualisierung der Antiviren-Software und die Sensibilisierung des gesamten Teams sind ein absolutes Muss, da 68% der Datenschutzverletzungen auf den Faktor Mensch zurückzuführen sind (z. B. menschliches Versagen, Missbrauch, Phishing und gestohlene Anmeldedaten). [ii]

Leider kommt es selbst bei sorgfältigstem Schutz immer wieder zu Datenverlusten. Beispielsweise gaben 73% der Gesundheitsorganisationen an, dass in 2023 ihre Daten von Cyberkriminellen verschlüsselt wurden. [iii]

Wenn Ihre Daten durch menschliches Versagen oder böswillige Angriffe verloren gehen, wird Ihr Geschäftsbetrieb gestört und Ihr Umsatz gerät unter Druck. Sie können, wenn überhaupt, erst wieder voll arbeiten, sobald Ihre Daten wiederhergestellt sind. Eine gute Datensicherung ist daher von unschätzbarem Wert.

> „31% der befragten Unternehmen benötigten zwischen einem und sechs Monaten, um sich von einem Ransomware-Angriff zu erholen, nachdem sie das Lösegeld bezahlt hatten. Im Gegensatz dazu erholten sich 45% der Unternehmen, die Backups verwendeten, innerhalb einer Woche."
>
> Sophos [iv]

Dieses Dokument zeigt Ihnen, wie Sie die richtige Backup-Strategie für Ihr Unternehmen entwickeln und was Sie dabei beachten müssen.

BEWÄHRTE PRAKTIKEN

Backup-Richtlinien und bewährte Praktiken

Bei der Datensicherung geht es nicht nur darum, eine Kopie wichtiger Dateien zu erstellen oder die Daten auf dem firmeneigenen OneDrive zu speichern. Diese Maßnahmen sind wichtig, aber der Schutz durch eine umfassende Backup-Strategie geht weit darüber hinaus.

Ein Backup ist viel mehr als nur eine Kopie einer Datei. Es ist ein Sicherheitsnetz für Ihre geschäftskritischen Daten. Es werden nicht nur Kopien Ihrer Dateien erstellt, sondern auch mehrere Versionen an verschiedenen Orten über einen längeren Zeitraum aufbewahrt. Das bedeutet, dass Sie zu einem beliebigen früheren Zeitpunkt zurückkehren können, wenn etwas schief geht.

Datensicherung nach der 3-2-1-Regel

Eine der einfachsten und effektivsten Best Practices für die Datensicherung ist die 3-2-1-Regel:

Wenn Sie über mehrere Kopien Ihrer Daten auf verschiedenen Speichermedien verfügen, können Sie auf eine redundante Kopie zurückgreifen, selbst wenn eines dieser Medien beschädigt wird. Wenn Sie zusätzlich eine Kopie Ihrer Datensicherung extern oder in der Cloud aufbewahren, haben Sie im Falle eines Datenverlustes, z.B. durch einen Brand im Büro, eine unbeschädigte Sicherungskopie.

Zu beachtende Richtlinien...

Da Unternehmen immer mehr Daten produzieren, werden Vorschriften zum Schutz sensibler Informationen immer wichtiger. Regierungen auf der ganzen Welt schaffen ständig neue Gesetze und aktualisieren bestehende, die sicherstellen sollen, dass Unternehmen alles in ihrer Macht Stehende tun, um private Daten zu schützen.

Unternehmen jeder Größe müssen die Gesetze zum Datenschutz einhalten. Nur so können sie die Sicherheit ihrer eigenen Daten und die ihrer Kunden gewährleisten, ihren Ruf schützen und hohe Bußgelder vermeiden, die bei Nichteinhaltung der Vorschriften verhängt werden können. Die Einhaltung der Gesetze kann jedoch eine Herausforderung darstellen, wenn die IT-Ressourcen ohnehin knapp sind und oft nur ein begrenztes Budget zur Verfügung steht.

74% der Kunden von Managed Service Providern haben Probleme mit der Einhaltung von Vorschriften wie HIPAA, GDPR und PCI-DSS.[v]

Backup-Strategien und -Lösungen können sowohl an Ihre Bedürfnisse als auch an standort- und branchenspezifische Standards angepasst werden.

...standortbezogen

Anforderungen entwickeln sich aufgrund des ständigen technologischen Wandels ständig weiter. Nachfolgend sind einige wichtige Vorschriften aufgeführt, die in Europa und Nordamerika zu beachten sind.

Europa

General Data Protection Regulation (GDPR): GDPR ist eine EU-Verordnung, die den Schutz personenbezogener Daten von EU-Bürgern regelt. Sie verpflichtet Unternehmen dazu, angemessene Maßnahmen zum Schutz personenbezogener Daten zu ergreifen, einschließlich des Einsatzes sicherer Methoden zur Datensicherung. Außerdem müssen die Behörden im Falle eines Datenverlusts oder -diebstahls benachrichtigt werden.

Da es sich bei GDPR um ein umfassendes Gesetz handelt, das die Nutzung und Speicherung von Informationen für ganz Europa regelt, haben viele Länder eigene Regelungen hinzugefügt, um den länderspezifischen Anforderungen gerecht zu werden.

Bundesdatenschutzgesetz (BDSG): Das BDSG ergänzt GDPR in Deutschland und enthält zusätzliche Regelungen zur Datenverarbeitung und Datensicherheit. Insbesondere Sicherheitsbehörden müssen die Regelungen des BDSG beachten, da die GDPR-Vorschriften für sie nicht gelten.

Das deutsche Bundesministerium für Wirtschaft und Klimaschutz hat weitere Hinweise speziell zur Datensicherung veröffentlicht. So wird beispielsweise darauf hingewiesen, dass das Sicherungsmedium für die regelmäßige Datensicherung getrennt von der Produktionsumgebung aufbewahrt werden sollte.

Nord Amerika

California Privacy Rights Act (CPRA): Die Änderung des kalifornischen Gesetzes zum Schutz der Privatsphäre von Verbrauchern (California Consumer Privacy Protection Act, CCPA), die am 1. Januar 2023 in Kraft getreten ist, soll Verbrauchern mehr Mitspracherecht bei der Verwendung ihrer persönlichen Daten durch Unternehmen geben, die diese Daten erheben.

Kalifornien war nur der erste Bundesstaat, der ein Datenschutzgesetz verabschiedete, und inzwischen gibt es ähnliche Gesetze in Virginia, Connecticut, Colorado, Utah, Michigan, Ohio, New Jersey und Pennsylvania, die regeln, wie Daten gesammelt und geschützt werden müssen. Obwohl die Gesetze ähnlich sind, gibt es einige Besonderheiten, die Unternehmen, die in diesen Staaten mit personenbezogenen Daten arbeiten, beachten sollten.

Quebec's Law 25: Alle Unternehmen, die personenbezogene Daten erheben und in Québec tätig sind, müssen vor der Verwendung, Übermittlung oder Offenlegung von Daten die Einwilligung der betroffenen Person einholen. Das Gesetz wurde im Laufe der Jahre mehrfach geändert, wobei die wichtigsten Änderungen am 22. September 2023 in Kraft getreten sind.

...branchenspezifisch

Wenn Sie in einer Branche tätig sind, die mit sensiblen Daten zu tun hat, müssen Sie wahrscheinlich mit zusätzlichen regulatorischen Anforderungen rechnen.

Gesundheitswesen

Einrichtungen des Gesundheitswesens, insbesondere Arztpraxen, sind ein häufiges Ziel von Cyberkriminellen. Hinzu kommt, dass im Gesundheitswesen die sensibelsten Daten in Patientenakten gespeichert werden. Daher ist es von entscheidender Bedeutung, mit den Compliance-Vorschriften und den neuesten technologischen Entwicklungen Schritt zu halten.

Mehr als 60% der Cybersicherheitsvorfälle haben negative Auswirkungen auf die Patientenversorgung.[vi]

§75B des Sozialgesetzbuches V (SGB 5): Ähnlich wie GDPR umreißt §75B des Sozialgesetzbuches V (SGB 5), das in Zusammenarbeit mit der Kassenärztlichen Bundesvereinigung (KBV) verfasst wurde, die Anforderungen an die IT-Sicherheit, insbesondere für Arztpraxen.

Dieses Gesetz umfasst u.a. Aspekte wie Backup-Planung, Datensicherungs-häufigkeit und Wiederherstellungstests. Weitere Informationen zu den IT-Sicherheitsvorschriften nach §75 SGB 5 finden Sie unter: https://hub.kbv.de/pages/viewpage.action?pageId=63537333

Handel

Zahlungen und Überweisungen sind natürlich ebenfalls ein Ziel für böswillige Akteure. Die Gewährleistung einer robusten Datensicherheit ist daher für jedes Unternehmen, das beispielsweise Kreditkarteninformationen speichert, von entscheidender Bedeutung. Jedes System, das mit Kreditkartendaten in Berührung kommt, einschließlich Managed Service Provider (MSP), die die Daten nicht selbst verarbeiten, muss die Sicherheitsanforderungen erfüllen.

Payment Card Industry Data Security Standard (PCI-DSS): Unternehmen, die Kreditkartendaten verarbeiten, müssen die sichere Speicherung und Übertragung dieser Informationen gewährleisten. Unternehmen müssen alle Web-Assets identifizieren und dokumentieren und sicherstellen, dass Anwendungen und Systemkomponenten sicher konfiguriert sind und Schwachstellen identifiziert werden können.

WIEDERHERSTELLUNG

Verstehen Sie Ihre Daten und Wiederherstellungsziele

Die Einhaltung der Vorschriften ist nur die halbe Miete, wenn es um Ihre Backup-Strategie geht. Genauso wichtig sind Ihre individuellen Ziele. Dazu gehört, dass Sie Ihre Daten und geschäftskritischen Informationen kennen und entscheiden, welche Wiederherstellungszeiten für Sie akzeptabel sind.

- Führen Sie eine **Bestandsaufnahme** der vorhandenen IT-Systeme, Anwendungen und Daten sowie der Remote- und Home-Office-Standorte durch, um die wichtigsten Systeme und Daten sowie den potenziellen künftigen Bedarf zu ermitteln.

- Ermitteln Sie Ihre **Datenabhängigkeiten** und die Informationen, auf die Ihr Unternehmen angewiesen ist. Berücksichtigen Sie, wie Finanz- und Kundendaten interagieren und sich auf die Entscheidungsfindung auswirken, sowie alle vertraglichen Verpflichtungen, die Sie einhalten müssen.

- Überlegen Sie, wie **häufig sich Ihre Daten ändern**. Einige Ihrer Daten ändern sich täglich. Für diese Daten ist eine häufigere Sicherung sinnvoller als für Daten, die sich im Laufe der Zeit nur geringfügig ändern.

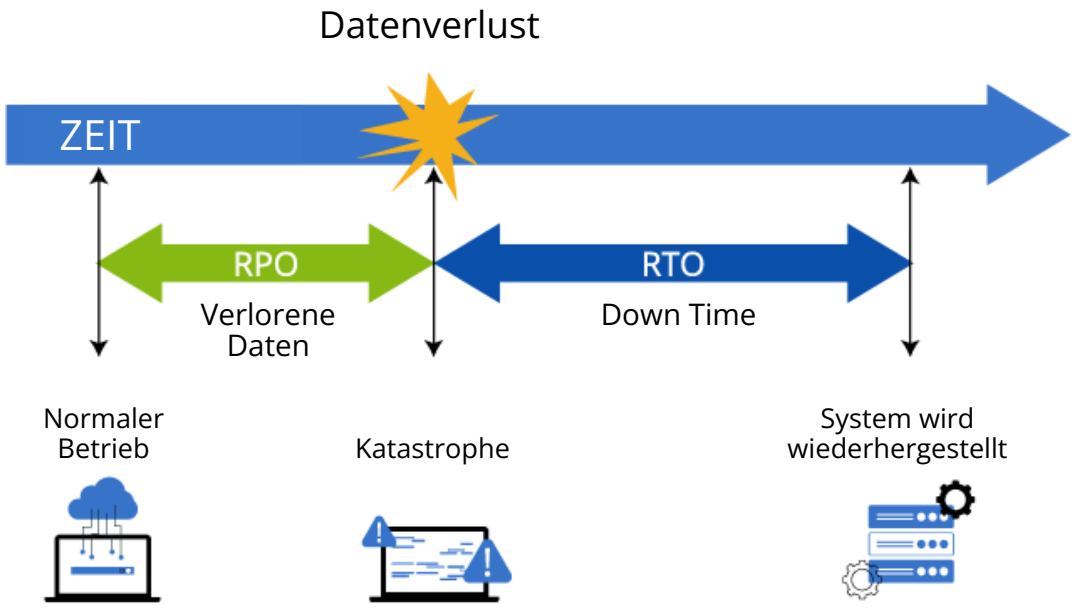
Jedes Unternehmen ist verpflichtet, Geschäftsunterlagen für einen bestimmten Zeitraum aufzubewahren - oft zwischen sechs und zehn Jahren, je nach Standort und Branche. Die Einteilung Ihrer Daten in kritische, betriebliche, geschäftliche und persönliche Kategorien hilft Ihnen bei der Festlegung der Aufbewahrungsfrist. Die Festlegung von Aufbewahrungsrichtlinien hilft Ihnen auch, Ihre Speichermedien effizienter zu nutzen, indem Sie veraltete oder unnötige Backups löschen.

Wenn Sie die Abhängigkeiten Ihrer Daten kennen, können Sie besser einschätzen, wie lange Sie Ihr Geschäft im Falle eines Datenverlustes aufrechterhalten können und wie viele Daten im schlimmsten Fall verloren gehen könnten. Mit diesem Wissen können Sie die Ziele festlegen, die eine Backup-Strategie erfüllen muss.

Die Wiederherstellungsziele sind ein wesentlicher Bestandteil jeder Sicherungsstrategie und lassen sich in zwei Komponenten unterteilen:

1. **Recovery Time Objective (RTO):** RTO ist die maximal tolerierbare Zeitspanne, während der ein Computer, ein IT-System, ein Netzwerk oder eine Anwendung nicht verfügbar sein darf.

2. **Recovery Point Objective (RPO):** RPO beschreibt die maximale Menge an verlorenen Daten, die ein Unternehmen im Falle eines Datenverlustes unter Aufrechterhaltung des normalen Geschäftsbetriebes tolerieren kann.



Die Bestimmung von RTO und RPO ist hilfreich für das Verständnis der Anforderungen Ihres Unternehmens in Bezug auf die Ausführung notwendiger Geschäftsfunktionen und für die Festlegung einer geeigneten Backup-Strategie.

RTO hilft dabei, Ihre Backup-Strategie zu priorisieren und zu definieren. Beispielsweise müssen Sie Ihre Bandbreitenbeschränkungen kennen, da diese einen direkten Einfluss auf Ihre Backup- (oder besser: Wiederherstellungs-) Strategie haben können. Sie sollten auch darüber nachdenken, wo Sie Ihre Backups aufbewahren. Beispielsweise können Sie Ihre ausgelagerte Kopie schneller wiederherstellen, wenn sie sich in der Cloud befindet und Sie nicht an einen anderen Ort reisen müssen.

Ihr RPO hilft Ihnen bei der Festlegung der Backup-Intervalle. Normalerweise werden geschäftskritische Daten einmal täglich (oder häufiger) gesichert und zu einer bestimmten Zeit ausgeführt, damit die lokale Infrastruktur nicht beeinträchtigt wird. Für die meisten Unternehmen sind daher die Abendstunden die beste Zeit für Backups.

BACKUP-STRATEGIE

Entwicklung einer Backup-Strategie: Welche Möglichkeiten gibt es?

Bei der Festlegung Ihrer Backup-Strategie ist es wichtig, die verschiedenen verfügbaren Optionen zu evaluieren. Denn die Implementierung der für Sie am besten geeigneten Lösung ist entscheidend, um sicherzustellen, dass geschäftskritische Daten nach jedem Datenverlustszenario verfügbar sind.

Sicherung von Dateien und Anwendungen und Desaster Recovery

Datei-Backup: Der Zweck eines Datei-Backups ist es, einzelne Dateien und Ordner schnell und einfach wiederherstellen zu können. Unabhängig davon, ob eine einzelne Datei verloren gegangen ist oder die interne Festplatte nicht mehr funktioniert, ist ein Datei-Backup die effizienteste Methode, um geschäftskritische (oder weniger kritische) Informationen wiederherzustellen.

Anwendungs-Backup: Ein Anwendungs-Backup stellt sicher, dass alle mit der Anwendung verbundenen Daten, einschließlich ihrer Konfiguration und Abhängigkeiten, erhalten bleiben. Es erweitert das Konzept der Dateisicherung auf komplexere Daten wie Datenbanken, ganze Anwendungen oder sogar Snapshots virtueller Maschinen.

Disaster recovery: Desaster Recovery ermöglicht die Wiederherstellung des gesamten Betriebssystems und seiner Daten. Das bedeutet, dass Sie im Katastrophenfall Ihr gesamtes System auf vorhandener oder neuer Hardware oder als virtuelle Maschine in einem Schritt wiederherstellen können.

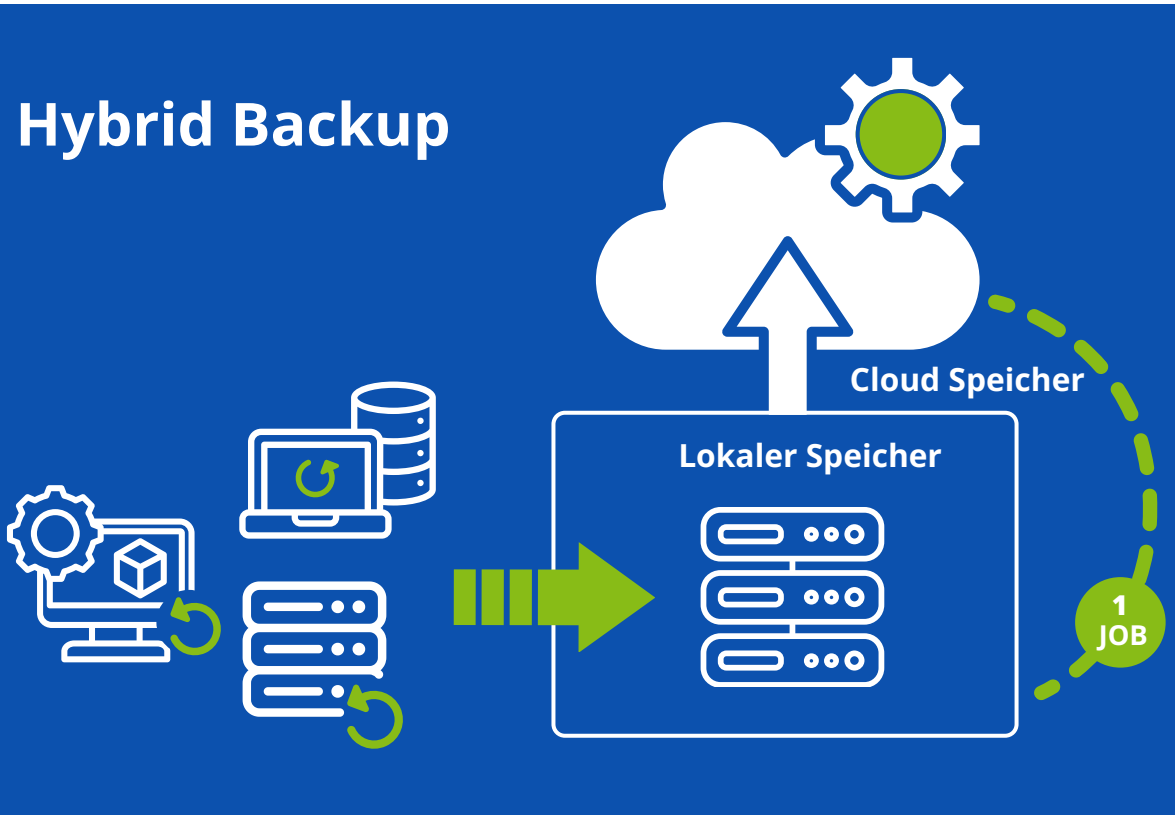
Backups von Dateien und Anwendungen sowie Desaster Recovery sind wichtige Bestandteile einer umfassenden Backup-Strategie und können in unterschiedlichen Intervallen durchgeführt werden. Beispielsweise können geschäftskritische Dateien häufiger gesichert werden als Anwendungen.

Lokal, Offsite und Hybrid Backup

Nach der 3-2-1-Regel sollten Sie sowohl interne als auch externe Backups aufbewahren. Das bedeutet, dass Sie folgende Backups benötigen:

Lokales Backup: Ein Backup, das auf einem Gerät gespeichert wird, das sich im selben Büro befindet. Da es direkt verbunden ist, bietet es die schnellste Wiederherstellung von Dateien und Systemen.

Offsite-Backup: Ein Offsite-Backup ist die einzige Möglichkeit, Daten wiederherzustellen, wenn das lokale Backup beschädigt oder anderweitig nicht verfügbar ist. Heutzutage ist es für Unternehmen üblich, Cloud-Speicher zu verwenden.



Den Überblick über zwei oder mehr Sicherungsorte zu behalten, muss aber nicht kompliziert sein. Mit einer **Hybrid Backup-Lösung** können Sie lokales und Cloud-Backup in einem einzigen Backup-Job kombinieren, wobei alle Daten zunächst auf das ausgewählte lokale Speichergerät und von dort aus in die Cloud gesendet werden.

Backup Methoden

Grundlegend gibt es drei wesentliche Sicherungsmethoden - jede mit ihren eigenen Vor- und Nachteilen. Darüber hinaus gibt es eine neue Sicherungsmethode, die das Beste aus allen Welten vereint: Incremental Forever Backup.

Traditionelle Backupmethoden

- **Vollbackups** enthalten alle ausgewählten Daten, was die Wiederherstellung erleichtert. Sie sind jedoch speicher- und zeitaufwändig und daher für den regelmäßigen Einsatz nicht geeignet, insbesondere für kleine und mittlere Unternehmen mit wachsenden Datenbeständen oder MSPs, die mehrere Kunden betreuen müssen.

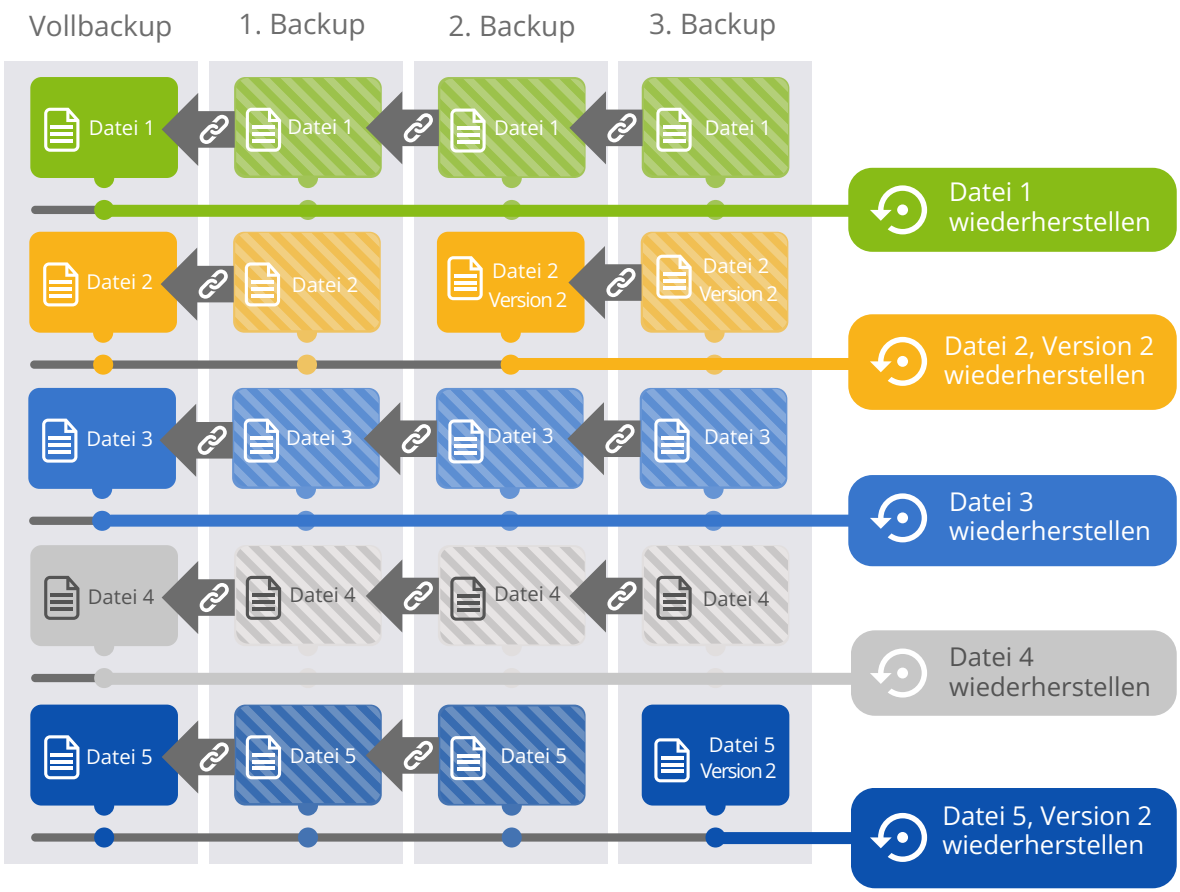
- **Inkrementelle Backups** erfassen nur die Änderungen seit der letzten Sicherung und sind daher wesentlich schneller und speichereffizienter. Wiederherstellungen können jedoch mühsam sein, da das erste Backup und jedes einzelne inkrementelle Backup benötigt werden, um alle Daten wiederherzustellen.

- **Differenzielle Backups** enthalten alle Änderungen, die seit dem letzten vollständigen Backup an Ihren Daten vorgenommen wurden. Dies vereinfacht die Wiederherstellung, da Sie nur Ihr vollständiges Backup und das letzte differenzielle Backup benötigen, um alles abzudecken. Es entstehen jedoch viele redundante Sicherungen, die den Speicherbedarf erhöhen.

Incremental Forever Backup

Incremental Forever Backup greift Ideen der traditionellen inkrementellen und differentiellen Backups auf, beseitigt aber deren Schwächen. Es funktioniert wie folgt:

- **Erste Vollsicherung:** Der Prozess beginnt mit einer einzigen Vollsicherung aller ausgewählten Dateien.
- **Nur inkrementelle Sicherungen:** Nachfolgende Sicherungen erfassen nur die Änderungen seit der letzten Sicherung.
- **Effiziente Datenverknüpfung:** Jedes Inkrement enthält Verknüpfungen zu allen früheren Versionen einer Datei oder eines Ordners, auch wenn diese nicht geändert wurden. Ähnlich wie bei der differenziellen Sicherung bleiben alle Informationen in jedem Inkrement erhalten, jedoch ohne Datenredundanz zwischen den Sicherungsdateien.



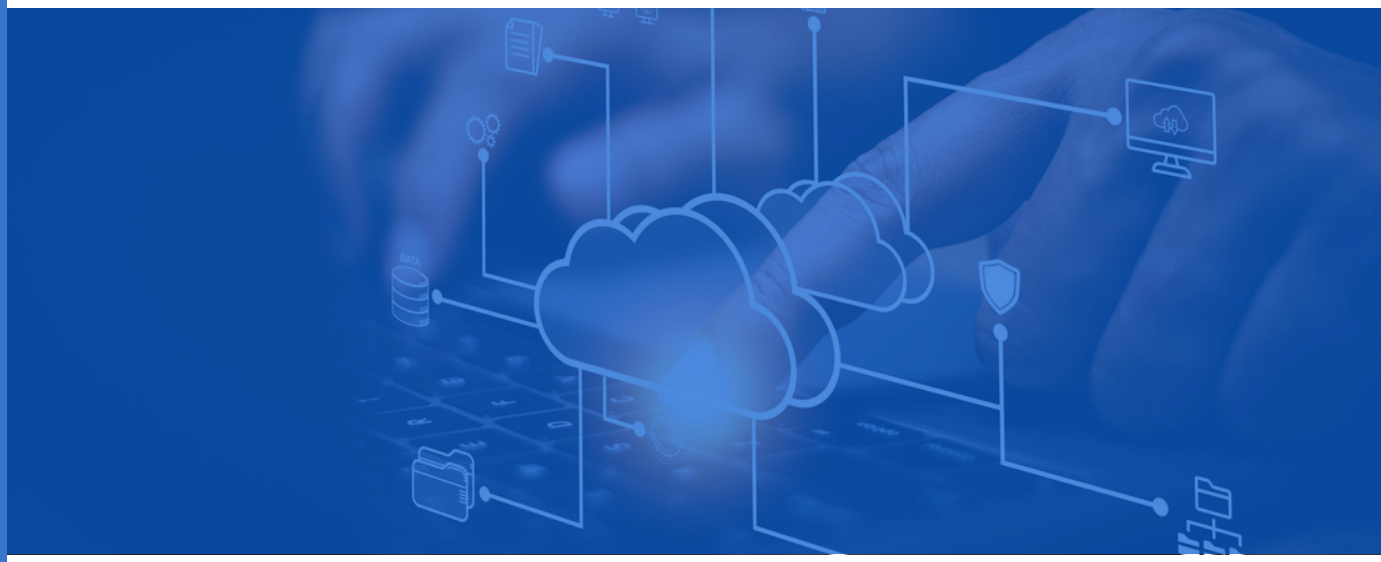
Die Hauptvorteile von Incremental Forever-Backups liegen in der erheblichen Verkürzung der Backup-Zeiten nach dem ersten vollständigen Backup und in der Reduzierung der Speicherkosten durch den Wegfall der Datenredundanz. Sie profitieren auch von vereinfachten Wiederherstellungen mit automatischen Verknüpfungen zwischen inkrementellen Backups und einer flexiblen Aufbewahrung, die sicherstellt, dass wichtige Daten immer verfügbar sind, wenn ältere Dateien gelöscht werden.

Sonstige zu berücksichtigende Funktionen

Speichermedien

Wenn Sie mehrere Kopien Ihrer Backups an verschiedenen Orten aufbewahren, benötigen Sie verschiedene Speichermedien. Wählen Sie diejenigen aus, die für Ihre Umgebung am besten geeignet sind. Dies könnte eine Mischung aus den folgenden Medien sein:

- **Externe Festplatten (HDD),** Solid State Drives (SSD), USB-Laufwerke: Sind einfach zu bedienen, haben eine hohe Speicherkapazität, sind relativ preiswert und übertragen Daten schnell. Sie sind jedoch anfällig für Beschädigungen und Diebstahl.
- **Network Attached Storage (NAS):** Hierbei handelt es sich um einen zentralisierten Datenspeicher, oft mit eingebauter Redundanz. Die Anschaffungskosten können jedoch hoch sein, und die Einrichtung und Verwaltung erfordern technische Kenntnisse.
- **Cloudspeicher:** Bietet einfachen Zugriff von überall aus, sofortige Skalierbarkeit und vom Anbieter verwaltete Sicherheit. Für die Sicherung und Wiederherstellung der Daten ist jedoch eine Internetverbindung erforderlich.



Komprimierung

Durch die Komprimierung Ihrer Daten auf dem Backup-Medium können Sie viel Speicherplatz und Zeit sparen.

Verschlüsselung

Verschlüsselung stellt sicher, dass Ihre Daten für Unbefugte unlesbar sind und nur von vertrauenswürdigen Parteien eingesehen werden können. Dies ist besonders wichtig für Daten, die außerhalb des Unternehmens gespeichert werden. Es gibt zwei Hauptarten der Datenverschlüsselung:

- **Verschlüsselung am Speicherort:** Stellt sicher, dass niemand ohne den richtigen Verschlüsselungscode auf Ihre Daten auf dem Speichermedium, z.B. in der Cloud, zugreifen kann.
- **Verschlüsselung bei der Übertragung:** Dieser zusätzliche Verschlüsselungsmechanismus schützt Ihre Daten auf dem Weg zum Speichermedium vor unbefugtem Zugriff.

Automatische Backups

Eine gute Backup-Lösung sollte Backups automatisch durchführen, ohne dass ein ständiges manuelles Eingreifen erforderlich ist. Sie können einen Zeitplan für Backups festlegen und die Software damit beauftragen, diese zuverlässig für Sie durchzuführen. Noch besser ist es, wenn Sie einen Urlaubsplan erstellen, um die Backups zu pausieren, wenn Ihre Kunden oder Kollegen in den wohlverdienten Urlaub fahren.

Meldungen, Berichte und Warnungen

Regelmäßige Berichte über den Status Ihrer Backups und eventuell aufgetretene Probleme sind unerlässlich, damit Sie immer wissen, ob Ihre Daten vollständig gesichert sind und Sie diese im Notfall schnell wiederherstellen können.

Versionierung

Eine gute Backup-Lösung sollte es Ihnen ermöglichen, mehrere Versionen Ihrer Dateien und Systeme zu speichern, für den Fall, dass Sie auf frühere Versionen zurückgreifen müssen.

PLANEN

Backup-Strategie planen

Soweit haben Sie:

- die Regularien und Best Practices kennengelernt
- Ihre unternehmenskritischen Daten identifiziert
- Ihre Wiederherstellungsziele definiert
- die richtigen Backup-Optionen für Ihr Unternehmen in Betracht gezogen

Jetzt ist es an der Zeit, Ihren Backup-Plan zu erstellen.

Beispiel für einen Backup-Plan

Schützen Sie geschäftskritische Daten, die schnell wiederhergestellt werden müssen:

- Führen Sie monatlich ein Desaster Recovery Backup Ihres Systems durch.
- Plus täglich Backups von Daten und Anwendungen, die 30 Tage lokal und 90 Tage in der Cloud gespeichert werden.
-

Schützen Sie Daten, die sich selten ändern:

- Führen Sie monatlich ein Desaster Recovery Backup Ihres Systems durch.
- Plus wöchentliche Backups von Daten und Anwendungen mit einer Aufbewahrungszeit von 30 Tagen lokal und in der Cloud.

Für eine umfassende Strategie empfehlen wir eine Kombination von Sicherungsarten, bei der Ihre Daten an mehreren Orten gespeichert werden. Sichern Sie Ihre geschäftskritischen Dateien so oft wie möglich, insbesondere wenn sie sich häufig ändern. Gleichzeitig sollten Sie regelmäßige Backups für Desaster Recovery und Anwendungen durchführen. Mit der richtigen Backup-Lösung können Sie Backups so planen, dass sie automatisch ausgeführt werden, und angemessene Aufbewahrungsfristen für Ihre Daten festlegen.

Hersteller guter Datensicherungslösungen bieten umfassende Unterstützung an. Wenn Sie sich also nicht sicher sind, welche Strategie für Ihr Unternehmen die richtige ist, können Sie sich an den Experten wenden, um die für Sie beste Lösung zu finden.

Dokumentieren Sie Ihren Backup-Plan

Sobald Sie Ihre Backup-Strategie festgelegt haben, dokumentieren Sie diese. Eine klar definierte und schriftlich festgehaltene Strategie hilft Ihnen, den Überblick über Ihre Backups zu behalten und stellt sicher, dass Sie Ihre Daten jederzeit wiederherstellen können.

Dokumentieren Sie:

- Was wird wann und wo gespeichert?
- Regeln für die Aufbewahrung
- Wer ist wofür verantwortlich?
- Wer überprüft die Backups regelmäßig?
- Wie oft werden die Sicherungen überprüft?
- Wie oft werden neue Daten, Anwendungen und Systeme in den Backup-Plan aufgenommen?

Wenn Sie mit einem Managed Service Provider zusammenarbeiten, besprechen Sie mit ihm die Anforderungen an die Dokumentation des Backup-Plans. So können Sie sicher sein, dass er alles in seiner Macht Stehende tut, um Ihre Daten zu schützen.

Backup zur Sicherstellung der Datenwiederherstellung testen

Der vielleicht wichtigste Aspekt Ihrer Backup-Lösung ist die Fähigkeit, Ihre Daten wiederherzustellen. Es ist von entscheidender Bedeutung, dass die Backup-Software auch im schlimmsten Fall funktioniert.

Neben einer gut geplanten Backup-Strategie und regelmäßigen Backups ist es daher wichtig, diese Backups regelmäßig zu testen.

- Testen Sie Ihre Backups und stellen Sie sicher, dass Sie Ihre Daten und Systeme wiederherstellen können.
- Überprüfen Sie, ob das Backup funktioniert und Ihre Daten zum NAS oder in die Cloud gesendet werden.
- Stellen Sie sicher, dass die Speichermedien funktionieren und keine defekten Blöcke aufweisen.
- Vergewissern Sie sich, dass Sie alle Passwörter und Verschlüsselungscodes zur Hand haben, um Ihre Backups schnell entschlüsseln zu können.

Backup-Spezialisten können bei der Datensicherung helfen

Wir von NovaBACKUP helfen Ihnen, die richtige Lösung für Ihr Unternehmen zu finden. Jede IT-Umgebung ist anders und hat einzigartige Anforderungen. Unser Ziel ist es, Ihre Backup- und Recovery-Anforderungen zu erfüllen und Ihr IT-Team langfristig zu ergänzen.

Vereinbaren Sie einen Beratungstermin mit einem unserer Backup-Experten, um Ihre Anforderungen und Ziele zu besprechen, und wir helfen Ihnen, die perfekte Lösung zu finden.

ÜBER NOVABACKUP

Die NovaBACKUP Europe GmbH ist spezialisiert auf Backup und Disaster Recovery für Reseller und Managed Service Provider mit Fokus auf die Betreuung stark regulierter, professioneller Branchen. Mit über einer Million geschützten Maschinen und über zwanzig Jahren auf dem Markt, ist es das Ziel von NovaBACKUP, weltweit leistungsstarken, zuverlässigen und erschwinglichen Datenschutz zu bieten.

Weitere Informationen zu NovaBACKUP und unseren Produkten finden Sie unter www.novabackup.de

Sprechen Sie noch heute mit einem unserer Backup-Experten für eine kostenlose Beratung zu Ihrer Backup-Umgebung.

Sources:

i Consoltech
ii 2024 Data Breach Investigations Report – Verizon
iii The State of Ransomware in Healthcare 2023 – Sophos (Aug 2023)
iv The State of Ransomware 2023 – Sophos (May 2023)
v Kaseya's 2022 Global Benchmark Survey Report
vi The Global Healthcare Cybersecurity Study – Claroty (2023)

NovaBACKUP Europe GmbH
Marienstrasse 89
30171 Hannover

Tel.: +49 (40) 80811371

Email: kontakt@novabackup.de
www.novabackup.de