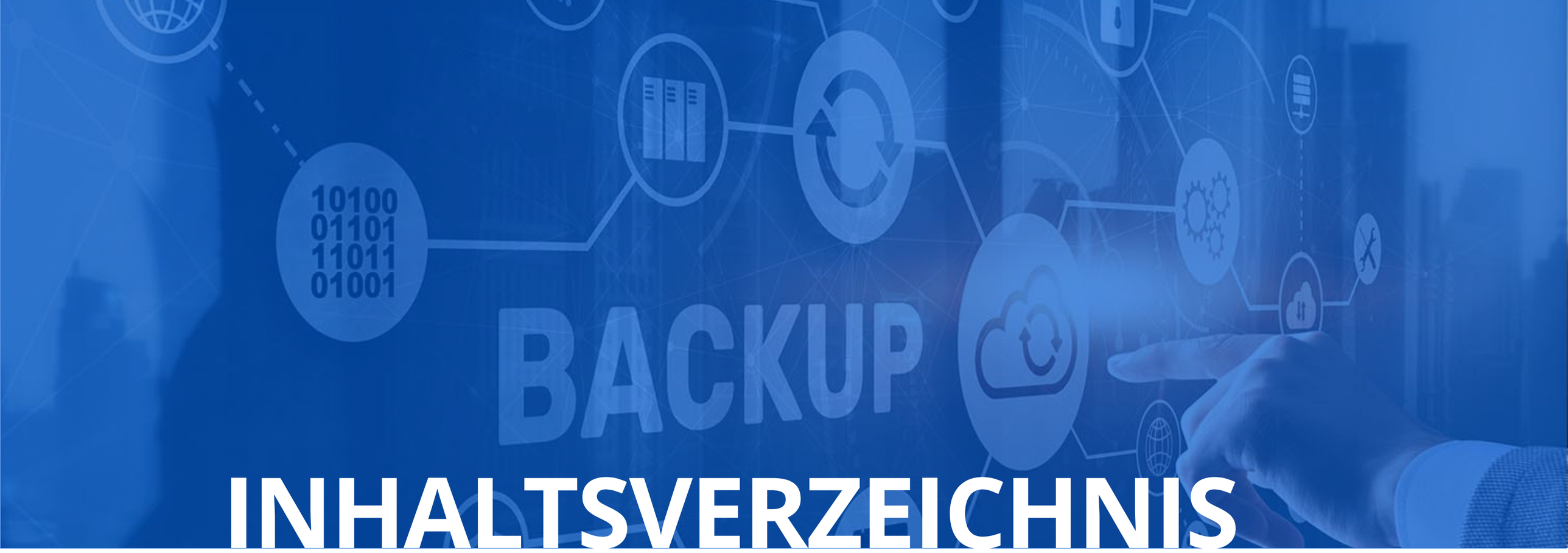
LEITFADEN

NovaBACKUP

LEITFADEN FÜR EINE EFFIZIENTE
BACKUP STRATEGIE

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



INHALTSVERZEICHNIS

EINLEITUNG

Geschäftskritische Daten werden heute überwiegend in digitaler Form und oft an verschiedenen Orten gespeichert. Damit steigt das Risiko, dass einzelne Informationen oder ganze Datenbestände verloren gehen, was schwerwiegende Folgen für die Produktivität und manchmal sogar für das Überleben eines Unternehmens haben kann.

Die Gründe für die Beschädigung oder Beeinträchtigung der Daten eines Unternehmens sind vielfältig:

Externe Bedrohungen: Die Häufigkeit von Angriffen wie Ransomware und anderer Schadsoftware, die Ihre Daten verschlüsselt, hat weltweit für Aufsehen gesorgt. Wir sollten jedoch nicht vergessen, dass es auch unvorhergesehene Ursachen wie Naturkatastrophen gibt, die ebenso verheerend sein können.

Interne Bedrohungen: Obwohl Cyberkriminalität die Schlagzeilen beherrscht, gibt es auch alltäglichere Ursachen für Datenverluste, von gewöhnlichen Fehlern durch menschliches Versagen bis hin zu Softwarefehlern und Hardwareausfällen.

Remote-Systeme: Die moderne Unternehmenslandschaft besteht zunehmend aus Mitarbeitern, die von zu Hause oder anderen Standorten aus arbeiten. Dies stellt Systemadministratoren vor größere Sicherheitsherausforderungen, da diese eine größere Angriffsfläche und eine größere Anzahl verteilter Geräte schützen müssen.

Unabhängig von der Ursache, der Verlust von Daten ist ein potenziell unternehmensschädigendes Ereignis.

Was kann man dagegen tun?

Vorbeugende Maßnahmen wie Viren- und Vulnerability-Scanner, Passwortmanagementsysteme und sogar Sicherheitsschulungen verbessern die Fähigkeit, Probleme frühzeitig zu erkennen und sind ein absolutes Muss. Wenn diese Methoden jedoch versagen, ermöglicht nur ein aktuelles und wiederherstellbares Backup aller kritischen Daten und/oder Systeme eine rechtzeitige Rückkehr zum normalen Geschäftsbetrieb.

> 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 – The State of Ransomware 2023

Die gute Nachricht ist, dass eine umfassende Datenschutzstrategie und eine verständliche Dokumentation der Verfahren nicht nur sicherstellen, dass Ihre Daten im Katastrophenfall wiederhergestellt werden können, sondern auch einen großen Teil Ihrer rechtlichen Anforderungen erfüllen, wenn die Compliance-Prüfer vor der Tür stehen. Dieses Whitepaper führt Sie durch die wichtigsten Schritte zur Entwicklung einer umfassenden Backup- und Wiederherstellungsstrategie, die auf die Bedürfnisse Ihres Unternehmens zugeschnitten ist.

BESTANDTEILE EINER EFFIZIENTEN BACKUP-STRATEGIE

Die folgenden vier Schritte helfen Ihnen, die wichtigen Informationen zu konsolidieren und so eine Backup-Strategie zu entwickeln, die auf Ihre Bedürfnisse zugeschnittene ist, die Vertrauen schafft, die vorhandenen Ressourcen optimal nutzt und einen effizienten Betrieb ohne Unterbrechungen ermöglicht.

Kenntnis Ihrer Daten und Systeme

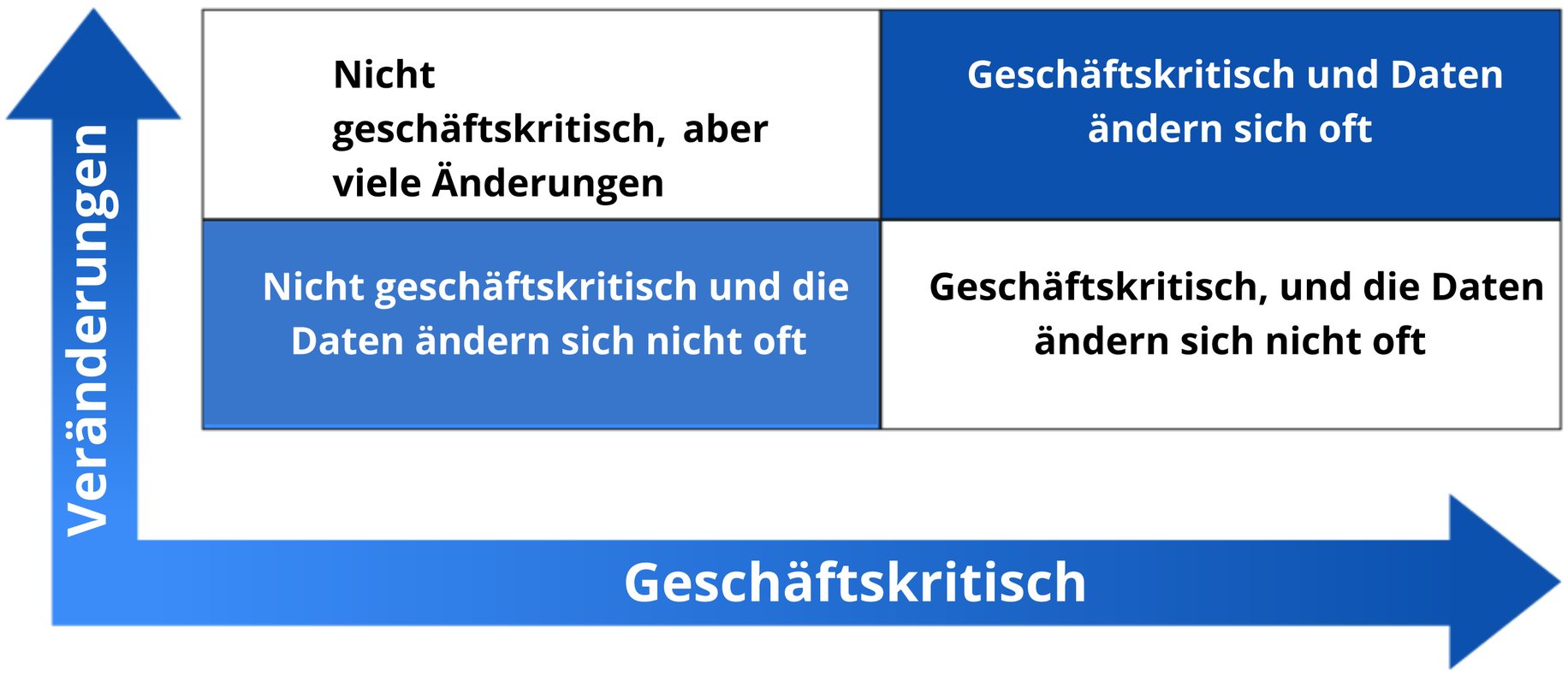
Ermitteln von Recovery-Anforderungen

Backup-Bausteine

Dokumentation

1 Kenntnis Ihrer Daten und Systeme

Beginnen Sie mit einer Bestandsaufnahme der vorhandenen IT sowie der Remote-Standorte und -Mitarbeiter. Auf diese Weise können Sie die wichtigsten Systeme, Daten und zukünftigen Anforderungen ermitteln. Die folgende Struktur ermöglicht es Ihnen, Ihre Geschäftsdaten zu kategorisieren, damit Sie einen besseren Überblick über die verschiedenen Datentypen und deren Priorität erhalten.



Um zu analysieren, in welche Kategorie Ihre Daten und Systeme fallen könnten, sollten Sie die folgenden Punkte berücksichtigen:

Einfluss der Daten auf das Unternehmen: Daten, ohne die das Unternehmen nicht funktionieren kann, sind wichtiger und sollten mehr Aufmerksamkeit erhalten als Daten, die für das Tagesgeschäft nicht von Bedeutung sind. Geschäftskritische Daten sind z.B. Finanzdaten, Kundendaten, vertragliche Verpflichtungen und generell Informationen mit Einfluss auf den Umsatz.

Gesetzliche Anforderungen: Gesetzliche Verordnungen wie die General Data Protection Regulation (GDPR) oder der California Consumer Privacy Act (CCPA) beschreiben wie Organisationen, die personenbezogene Daten verarbeiten, diese handhaben müssen. Andere Standards wie die Datenschutz-Grundverordnung (DSGVO) oder der Payment Card Industry Data Security Standard (PCI DSS) schreiben vor, dass ALLE Unternehmen, die personenbezogene Daten empfangen, verarbeiten, speichern oder übertragen, eine sichere IT-Umgebung bereitstellen müssen.

Daten, die unter solche Regelungen fallen, müssen beim Backup gesondert behandelt werden.

Nicht nur die aktuelle Situation, sondern auch die kurz- und mittelfristige Planung sollte in eine zukunftssichere Backup-Strategie einfließen. Dadurch vermeiden Sie unnötige Folgekosten.

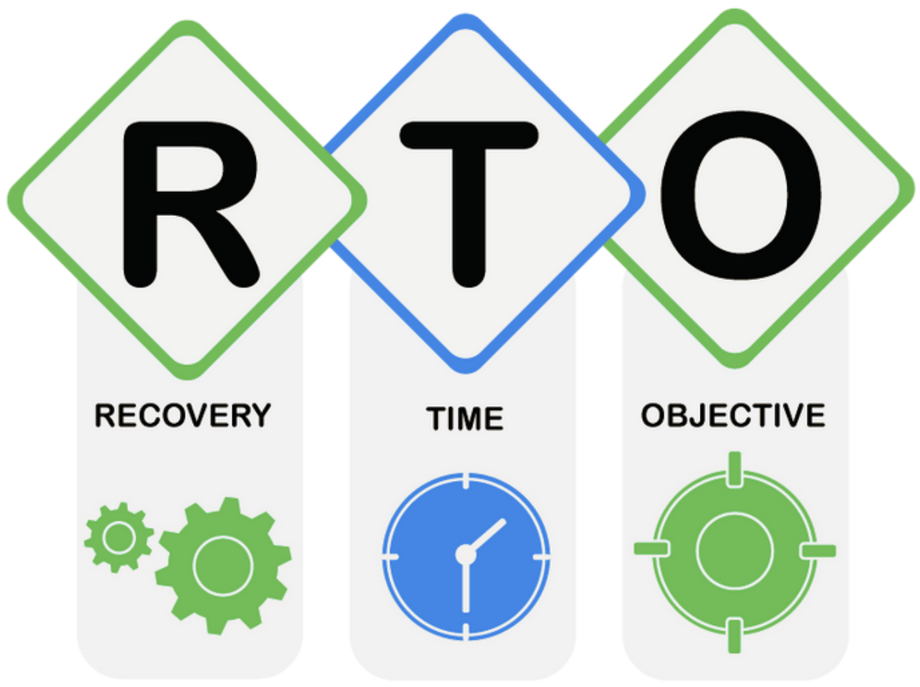
Aufbewahrungsfristen: Jedes Unternehmen ist verpflichtet, Geschäftsunterlagen je nach Standort und Branche für einen bestimmten Zeitraum aufzubewahren. Dieser Zeitraum liegt häufig zwischen sechs und zehn Jahren. Die Einteilung Ihrer Daten in kritische, betriebliche, geschäftliche und persönliche Kategorien hilft Ihnen später bei der Festlegung der Aufbewahrungsfristen, die bestimmen, wie lange Sicherungsdaten aufbewahrt werden, bevor nicht mehr benötigte Daten gelöscht werden können. Wenn Sie planen, große Datenmengen langfristig aufzubewahren, können zusätzliche Archivierungstechnologien erforderlich sein.

2 Ermitteln von Recovery-Anforderungen

Da Sie nun wissen, welche Daten für Ihr Unternehmen wichtig und welche weniger wichtig sind, können Sie abschätzen, wie lange Sie Ihr Unternehmen im Falle eines Datenverlusts aufrechterhalten können bzw. wie viele Daten im schlimmsten Fall verloren gehen könnten. Dies wird auch durch zwei Kennzahlen definiert: Recovery Time Objective (RTO) und Recovery Point Objective (RPO).

Wann sollte Ihr letztes erfolgreiches Backup abgeschlossen sein?

Wie schnell müssen Sie den Betrieb wiederherstellen und wieder aufnehmen?



RTO (Recovery Time Objective)

“RTO ist die maximal tolerierbare Zeitspanne, während der ein Computer, ein IT-System, ein Netzwerk oder eine Anwendung außer Betrieb sein darf.“

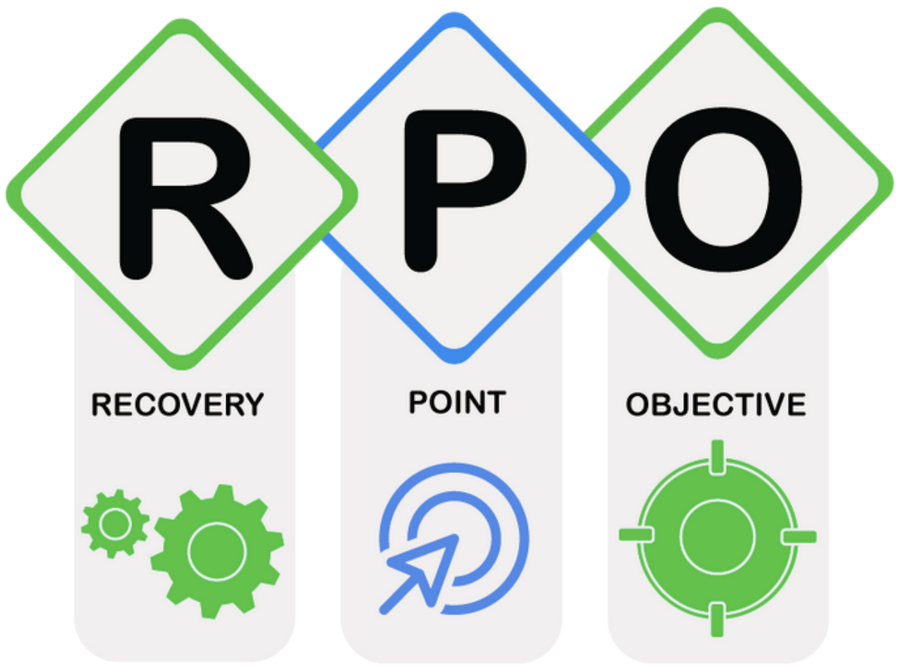
Wie viel Ausfallzeit kann Ihr Unternehmen maximal tolerieren, bevor die Unterbrechung ernsthafte Auswirkungen auf den Betrieb und die Einnahmen hat? Wie lange darf die Wiederherstellung Ihres Backups maximal dauern? Unterschiedliche Datentypen haben natürlich unterschiedliche Anforderungen an die Verfügbarkeit. Höhere Verfügbarkeitsanforderungen wirken sich beispielsweise auf die Anzahl der Backups aus und können kürzere (oder sogar kontinuierliche) Backup-Intervalle erforderlich machen. Wenn Sie Ihre RTO kennen, können Sie die relevanten Daten für Ihre Backup-Strategie entsprechend priorisieren.

Stellen Sie sich die Frage, ob eine Datensicherung vor Ort oder außerhalb Ihres Standorts sinnvoll ist:

Für die meisten, wenn nicht sogar für alle Branchen ist die Sicherung geschäftskritischer Daten außerhalb der lokalen Geschäftsräume und damit getrennt von der Produktionsumgebung ein Muss. Experten empfehlen, zumindest die 3-2-1-Backup-Regel zu befolgen (Backup an mindestens 3 Orten, auf mindestens 2 verschiedenen Speichermedien, davon 1 extern).

Um Ihr RTO im Auge zu behalten, müssen Sie jedoch Ihre Bandbreitenbeschränkungen kennen, da sich diese direkt auf Ihre Backup-Strategie auswirken können. Bandbreitenbeschränkungen zwischen den Systemen können nicht nur die Netzwerkleistung beeinträchtigen, wenn große Backups während der Produktionszeit durchgeführt werden, sondern auch unnötige Ausfallzeiten verursachen, während das Unternehmen auf den Abschluss einer Wiederherstellung wartet.

Tipp: Wenn Sie die maximale Bandbreite von Wechsellaufwerken, Netzwerkverbindungen und Cloud-Verbindungen ermitteln, können Sie die Wiederherstellungszeiten besser einschätzen.



RPO (Recovery Point Objective)

"RPO beschreibt die maximale Menge an verlorenen Daten, die ein Unternehmen im Falle eines Datenverlustes tolerieren kann, bei gleichzeitiger Aufrechterhaltung des normalen Geschäftsbetriebes."

Wir sprechen hier von dem Zeitpunkt, bis zu dem Ihre Backup-Lösung in der Lage sein muss, Daten wiederherzustellen. Wenn Ihr RPO beispielsweise zwei Stunden beträgt, müssen Sie in der Lage sein, Daten wiederherzustellen, die nicht länger als zwei Stunden vor dem Datenverlust erstellt oder verändert wurden. Mit dem Verinnerlichen dieser Kennzahl, haben Sie einen guten Anhaltspunkt, um zu definieren, wie oft Ihre unterschiedlichen Daten und Systeme gesichert werden sollten.

Beachten Sie Ihr Zeitfenster für die Datensicherung:

Backups sollten so geplant werden, dass die Übertragung der Daten vom System auf das Speichermedium die Leistung Ihrer Infrastruktur nicht beeinträchtigt. Für die meisten Unternehmen sind die Abendstunden am besten geeignet. Unternehmen, die rund um die Uhr arbeiten, müssen möglicherweise ihre Produktionsprozesse an das Backup-Fenster anpassen, um die Belastung der Produktionssysteme so gering wie möglich zu halten.

Damit Ihr RPO kurz bleibt, sollten diese Backup-Fenster nicht zu weit auseinander liegen. Ihr RPO hilft Ihnen, die Abstände zwischen den Backups zu bestimmen. Normalerweise werden geschäftskritische Daten einmal täglich oder häufiger gesichert. Es kann ratsam sein, das Backup-Intervall zu erhöhen, um z.B. SQL-Datenbanken, die sich ständig ändern, aus dem letzten Backup rekonstruieren zu können.

Die Bestimmung Ihrer Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) dient dazu, Ihre Geschäftsanforderungen für die Ausführung der erforderlichen Funktionen zu verstehen. Es hilft Ihnen, Ihre kritischen Systeme und Anwendungen zu identifizieren und zu definieren (in Minuten oder Stunden), wie viel Ausfallzeit für jede Komponente akzeptabel ist.

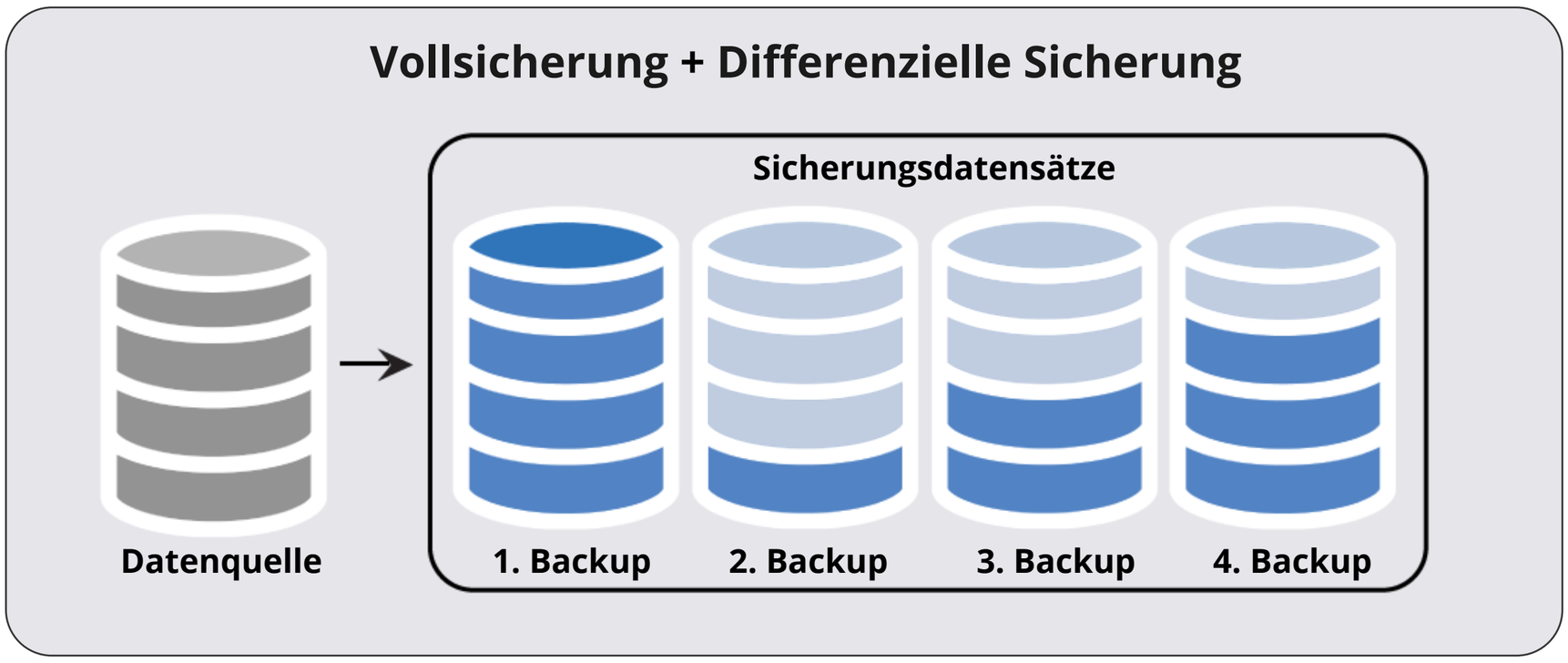
3 Backup-Bausteine

Für die Sicherung Ihrer Daten bietet jede Backup-Lösung unterschiedliche Möglichkeiten. Im Laufe der Jahre wurden diese Lösungen um neue und spektakuläre Funktionen erweitert, die versprechen, Ihre Daten noch mehr zu schützen. Aber für wahrscheinlich mehr als 90% der Unternehmen sind die bekannten und bewährten Backup-Methoden ausreichend, um eine schnelle Wiederherstellung zu gewährleisten.

Grundlagen der Datensicherung

Vollsicherung: Hier werden alle ausgewählten Daten komplett gesichert. Dieser Backup-Typ ist die Grundlage für alle Datei-, Anwendungs- und System-Backups.

Differenzielle Sicherung: Es werden nur die Daten gesichert, die sich seit der letzten Vollsicherung geändert haben oder neu hinzugekommen sind. Für eine Wiederherstellung werden sowohl die Vollsicherung als auch die letzte differenzielle Sicherung des gewählten Wiederherstellungspunktes benötigt.



Inkrementelle Sicherung: Es werden nur die Daten gesichert, die sich seit der letzten inkrementellen Sicherung geändert haben oder neu hinzugekommen sind. Diese Sicherungen sind oft kleiner als differentielle Sicherungen. Eine Wiederherstellung erfordert die Vollsicherung und alle inkrementellen Sicherungen bis zum gewählten Wiederherstellungspunkt.

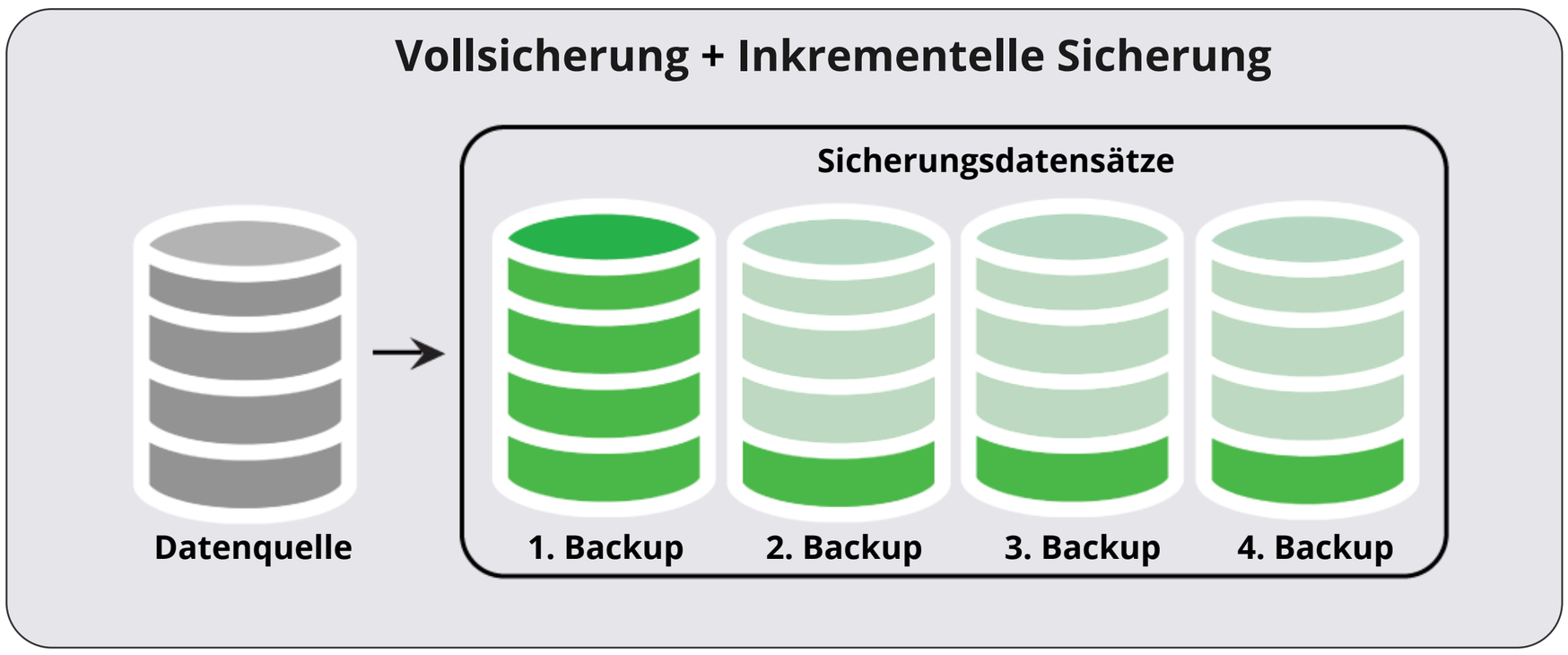


Image Backup

System Image oder Disaster Recovery Backup: Alle Systemdaten einschließlich Dateisystem, Anwendungen und Betriebssystem werden in einem einzigen Image gesichert und ermöglichen die schnelle Wiederherstellung eines kompletten Rechners einschließlich aller Programme und Einstellungen. Ein Image ist ein spezielles Format, das auch systemspezifische Konfigurationsdaten enthalten kann. Diese Images können virtuelle Festplatten (VHD/VHDx) sein, die als virtuelle Maschinen gemountet werden können. Diese Sicherungen werden häufig in regelmäßigen Abständen zusätzlich zu den regulären Dateisicherungen durchgeführt.

Andere Optionen

Kontinuierliches Backup: Einige Software- oder Cloud-Dienste bieten optional ein kontinuierliches Backup an, bei dem alle neuen oder geänderten Daten sofort gesichert werden. Viele SaaS-Backup-Lösungen, die in der Cloud sichern, z. B. für Dienste wie Microsoft 365, bieten diese Funktion.

Weitere zu berücksichtigende Funktionen:

Verschlüsselungsverfahren: Ein Algorithmus oder eine Technologie (z. B. AES 256), mit der Sie Ihre Daten verschlüsseln können. Dies ist besonders wichtig für Backups, die außerhalb des Unternehmens gespeichert werden.

Komprimierung: Die auf dem Sicherungsmedium gespeicherten Daten werden komprimiert und können damit Speicherplatz und Zeit sparen (da weniger Daten geschrieben werden müssen). Besonders hilfreich sind Lösungen, die die zu sichernden Daten bereits auf dem System komprimieren und so die Bandbreite weniger belasten.

Sicherung geöffneter Dateien: Auf geöffnete Dateien und Anwendungen kann über einen Volume Snapshot Service (VSS) Dienst zugegriffen werden, so dass einzelne Änderungen häufiger gesichert werden können.

Scripting: Die Möglichkeit, Skripte vor und nach der Datensicherung auszuführen, bietet Systemadministratoren ein hohes Maß an Flexibilität und Anpassungsfähigkeit bei der Durchführung von Wartungsaufgaben.

BACKUP PLAN

Für einen umfassenden Backup-Plan kombinieren Sie nun Ihre Anforderungen mit den typischen Funktionen einer Backup-Lösung. Es ist wichtig, dass Sie nicht nur einen Backup-Job für Ihre gesamte Umgebung erstellen, sondern diesen auch an die Kategorien anpassen, die im Kapitel Kennen Sie Ihre Daten und System definiert wurden.

Die genaue Anzahl der Backup-Aufträge in Ihrem Backup-Plan hängt von der Art der Daten, aber auch von der Branche ab, in der Sie tätig sind. In einer stark regulierten Branche wie dem Gesundheitswesen sollten Sie die Anzahl der täglichen und wöchentlichen Aufträge erhöhen (sofern Ihre Bandbreite dies zulässt), um Ihr RPO zu reduzieren. Wenn Sie jedoch z. B. ein kleines Geschäft betreiben, müssen Sie Ihre Daten möglicherweise nicht so häufig sichern. Die folgenden Beispiele zeigen Ihnen einige Varianten, wie Sie Ihren Backup-Plan angehen können.

Geschäftskritische Daten, die sich häufig ändern

Für Daten, die für Ihr Unternehmen wichtig sind, wäre es ratsam, sie folgendermaßen zu sichern:

Führen Sie einmal pro Woche, idealerweise am Wochenende, ein vollständiges Backup durch und bewahren Sie diese vollständigen Backups einen Monat lang auf.

Zusätzlich fünf differentielle Backups pro Woche, da diese Ihre RTO verkürzen und eine schnelle Wiederherstellung im Falle eines Datenverlustes ermöglichen. Diese Backups werden normalerweise von Montag bis Freitag durchgeführt. Bewahren Sie differenzielle Backups zwei Wochen auf.

Ein wöchentliches Image-Backup für die Wiederherstellbarkeit des gesamten Systems sollte mit monatlicher Aufbewahrung aufgesetzt werden.

Vollständige und differenzielle Backups sollten auf einem lokalen Speicher, z. B. einem NAS, gespeichert werden, um eine schnelle Wiederherstellung einzelner Dateien (RTO) zu ermöglichen. Das Hinzufügen eines Cloud-Speichers für Offsite-Backups ermöglicht die Wiederherstellung von jedem beliebigen Ort aus. Dies ist besonders wichtig für Unternehmen, deren Mitarbeiter an verschiedenen Standorten und/oder von zu Hause aus arbeiten.

Durch die Verwendung eines inkrementellen Verfahrens für Backups in der Cloud sparen Sie Zeit bei der Sicherung und ermöglichen es Mitarbeitern, die nur über einen langsamen DSL-Anschluss verfügen, ihre Daten problemlos zu sichern. Außerdem empfiehlt es sich, das Image-Backup auf einem lokalen Gerät für den schnellen Zugriff und auf einem zusätzlichen Wechseldatenträger an einem sicheren Ort außerhalb des Büros zu speichern.

Unkritische Daten, die sich selten ändern

Für die Daten, die weiterhin benötigt werden, deren Verlust aber nicht das Geschäft ruinieren würde, können Sie die Sicherungsaufträge wie folgt einrichten:

1

Einmal im Monat eine vollständige Sicherung mit einer Aufbewahrungsfrist von 4 bis 6 Monaten.

1

Wöchentliche differentielle Backups.

1

Ein Image-Backup alle 6 Monate mit einer Aufbewahrungsfrist von einem Jahr.

Wenn Ihre Bandbreite es zulässt, können Sie alle Dateien und Anwendungen für die langfristige Aufbewahrung in einer Cloud speichern. Da wahrscheinlich kein schnelles Rollback erforderlich ist und nicht viele Änderungen vorgenommen werden, ist es für das Unternehmen akzeptabel, wenn die Wiederherstellung einige Tage dauert.

BEISPIELSPEICHERPLATZ

Anmerkung zur Größe des Backup-Speichers

Bevor Sie sich für eine Methode entscheiden, sollten Sie die Menge der zu sichernden Daten berücksichtigen und damit die Größe Ihres Backup-Speichers bestimmen. Dies gilt nicht nur für das erste Backup, sondern für alle Backups, die Sie im Rahmen Ihres Datenaufbewahrungszyklus regelmäßig durchführen.

Nachfolgend ein Beispiel für einen Fileserver mit einem aktuellen Datenbestand von 500 GB, für den eine wöchentliche Vollsicherung und eine tägliche differentielle Sicherung geplant ist. Um abzuschätzen, wie viele Daten in einem bestimmten Zeitraum zusätzlich anfallen, kann es hilfreich sein, ein Tool wie z.B.

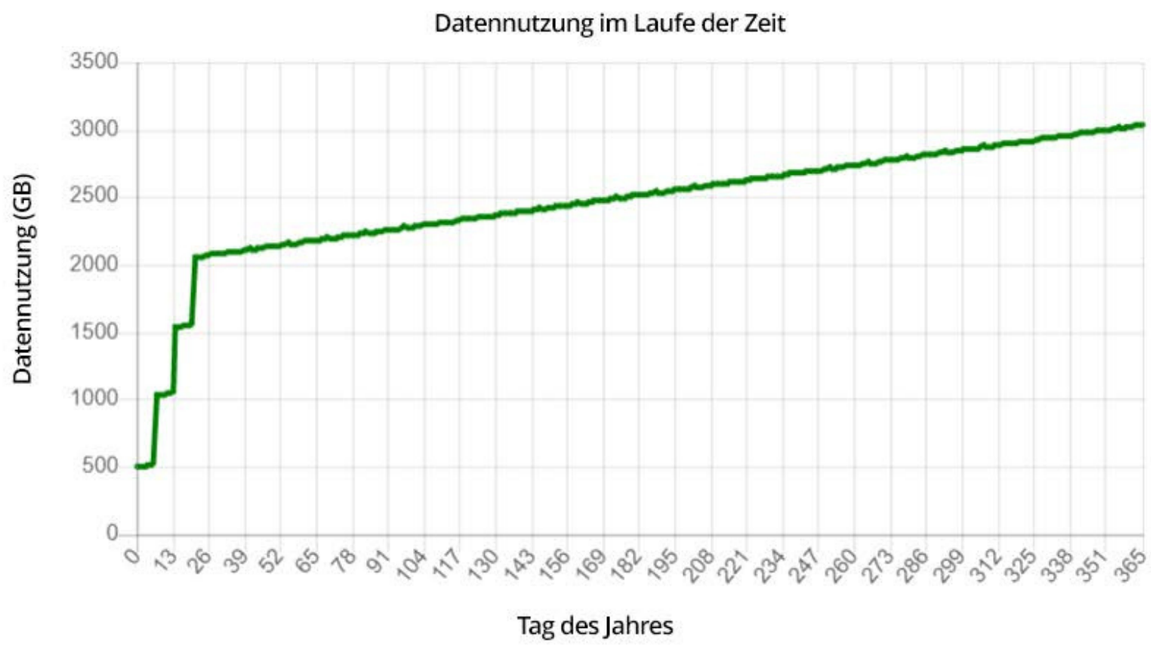
www.BackupCalculator.com

Speicherplatzbedarf:

Gesamte aktuelle Daten: **500 GB**

Gesamtdatengröße nach 1 Jahr: **760.71 GB**

Anforderungen an den Backup-Speicherplatz im Jahr 1: **3035 GB**



Server: 1

Daten pro Server: 500GB

Wöchentliche Änderungen der vorhandenen Daten: 5GB Neue Daten pro Woche: 5GB

Verwendung von Backup-Komprimierung: No

4 Dokumentation

Die Fähigkeit, Dateien und Systeme im Falle eines Datenverlusts schnell wiederherzustellen, hängt nicht nur von einem gut funktionierenden Backup ab, sondern auch von gut dokumentierten Prozessen, damit jeder weiß, was zu tun ist, wo alles zu finden ist, in welcher Reihenfolge wiederhergestellt werden muss usw. Es ist auch wichtig, die Prozesse klar zu definieren, damit die Informationen für das eigene Team, einen Nachfolger oder eine externe Partei, die die Verantwortung für das Backup übernehmen könnte, erhalten bleiben.

Dokumentieren Sie zunächst den Backup-Plan, den Sie mit Hilfe des vorhergehenden Kapitels erstellt haben.

- Was wird wo und wann gespeichert?
- Richtlinien für die Aufbewahrungszeit (z.B. für gesetzliche Anforderungen, Buchhaltung, usw.)
- Wer ist wofür verantwortlich, z.B. wer nimmt den USB-Stick und legt ihn in den Safe?
- Wer überprüft die Sicherung regelmäßig?
- usw.

Stellen Sie als nächstes einen Zeitplan auf, der Folgendes festlegt:

- Wie oft werden die Backups überprüft?
- Wie oft werden neue Daten, Anwendungen und Systeme in den Backup-Plan aufgenommen?

Notieren Sie sich außerdem die Kontaktdaten des Supports und des Kundenbetreuers Ihrer Backup-Lösung sowie eventuelle Lizenz- und Encryption-Keys.

Definieren Sie abschließend Ihren Wiederherstellungsplan. Welche Datenverlust-Szenarien sind real für Ihr Unternehmen und was ist jeweils zu beachten? Was muss getan werden, um die verschiedenen Daten innerhalb eines angemessenen Zeitraums wiederherzustellen (denken Sie an RTO und RPO)? Wo befinden sich die Daten/Images und in welcher Reihenfolge müssen diese wiederhergestellt werden?

Zusammengefasst, dokumentieren Sie alle Aspekte Ihres Backup-, Wiederherstellungs- und Testplans:

Backup-Plan	Wiederherstellungsplan	Test-Plan
Was wird wann und wo gesichert? Aufbewahrungsregeln Wer ist wofür verantwortlich? Verwaltung der Backup-Medien Regelmäßige Überprüfung Vertragsinformationen der Backup-Lösung und Kontaktdaten für deren Support Lizenz-, Encryption-Keys, usw.	Wiederherstellungsziele (RTO & RPO) Datenverlust-Szenarien Verfahren für die Wiederherstellung Spezielle Skripte und Tools Trainingsplan Rollen und Verantwortungen bei der Wiederherstellung Verfahren zur Aktualisierung der Dokumentation	Zeitplan/Häufigkeit der Tests Wann war der Restore-Test erfolgreich? Was wurde wiederhergestellt? Von wo? Wie lange hat es gedauert?

NICHT VERGESSEN!

Testen Sie Ihre Backups regelmäßig! Nichts ist schlimmer als ein beschädigtes oder anderweitig unbrauchbares Backup, das nicht wiederhergestellt werden kann. Außerdem sollte der Wiederherstellungsplan nicht nur einmal erstellt werden, sondern im Rahmen der regelmäßigen Tests mit den neuesten Änderungen aktualisiert werden.

Dokumentation des Übergabeprotokolls

Wenn Sie ein IT-Dienstleister sind oder eine IT-Abteilung in einem großen Unternehmen leiten, sollten Sie ein Übergabeprotokoll für die Übergabe der Verantwortung des Backups erstellen und dokumentieren.

Tipp für IT-Dienstleister

Wenn Sie einen Kunden an einen anderen Dienstleister übergeben, lassen Sie sich das Übergabeprotokoll von diesem unterschreiben, um somit Ihre Verantwortung zu übertragen.

ZUSAMMENFASSUNG

Ein Backup ist nur dann wertvoll, wenn es im Katastrophenfall alle relevanten Daten in der vorgegebenen Zeit wiederherstellen kann. Aus diesem Grund beginnt ein sicheres und zuverlässiges Backup nicht mit der Wahl des Speicherorts, sondern mit der Planung einer Backup-Strategie, die auf Ihre individuelle Umgebung zugeschnitten ist.

Durch eine umfassende Analyse Ihrer Umgebung (einschließlich Dateien, Hardware, Software, Speichergeräte und Anwendungen) können Sie bei der Entwicklung Ihrer Strategie leicht die wichtigsten Systeme und potenzielle Schwachstellen identifizieren. Und wenn Sie die geschäftlichen und rechtlichen Anforderungen sowie die Einschränkungen und Schwachpunkte Ihrer Umgebung kennen, können Sie eine effiziente Backup-Strategie entwickeln, die Datenverluste verhindert oder zumindest sicherstellt, dass verlorene Daten schnell wieder verfügbar sind, wodurch Ausfallzeiten reduziert werden.

Um nicht auf der Strecke zu bleiben, ist es auch wichtig, die Backup-Strategie von Zeit zu Zeit zu überarbeiten. Dabei sollten verschiedene Bedrohungsszenarien berücksichtigt, regelmäßige Wiederherstellungstests durchgeführt und die Wiederherstellungsanforderungen im Hinblick auf die Geschäftsziele neu bewertet werden.

Wenn eine Backup-Strategie sorgfältig geplant, durch flexible Technologie unterstützt und ordnungsgemäß verwaltet wird, trennt Unternehmen nach einem Datenverlust nur noch die für die Wiederherstellung benötigte Zeit von der Wiederaufnahme ihrer Geschäftstätigkeit.

> ***NovaBACKUP hat sich als hervorragendes Produkt erwiesen und der Kundensupport ist durchweg der beste und erfahrenste, mit dem ich je von einem Anbieter zu tun hatte.***

Lori Simmons
Support Services Engineer, Mytec Services

ÜBER NOVABACKUP

NovaBACKUP® (www.novabackup.de)

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 seinen Produkten finden Sie unter https://www.novabackup.de

Unser Service-Versprechen

Wir versprechen Ihnen, den Schutz und die Sicherheit Ihrer Daten so zu behandeln, als wären es unsere eigenen. Unser Ziel ist es, die Datensicherung so einfach und zuverlässig wie möglich zu gestalten. Sie können sich darauf verlassen, dass wir Sie professionell und fachkundig unterstützen, um Ihren Anforderungen an Ihre Datensicherung gerecht zu werden. Wenden Sie sich an unser Team, wenn Sie Unterstützung bei der Datensicherung und -wiederherstellung benötigen.

NovaBACKUP Europe GmbH
Marienstrasse 89, 30171 Hannover,
Deutschland

Tel.: +49 (40) 80811371

Email: kontakt@novabackup.de

www.novabackup.de