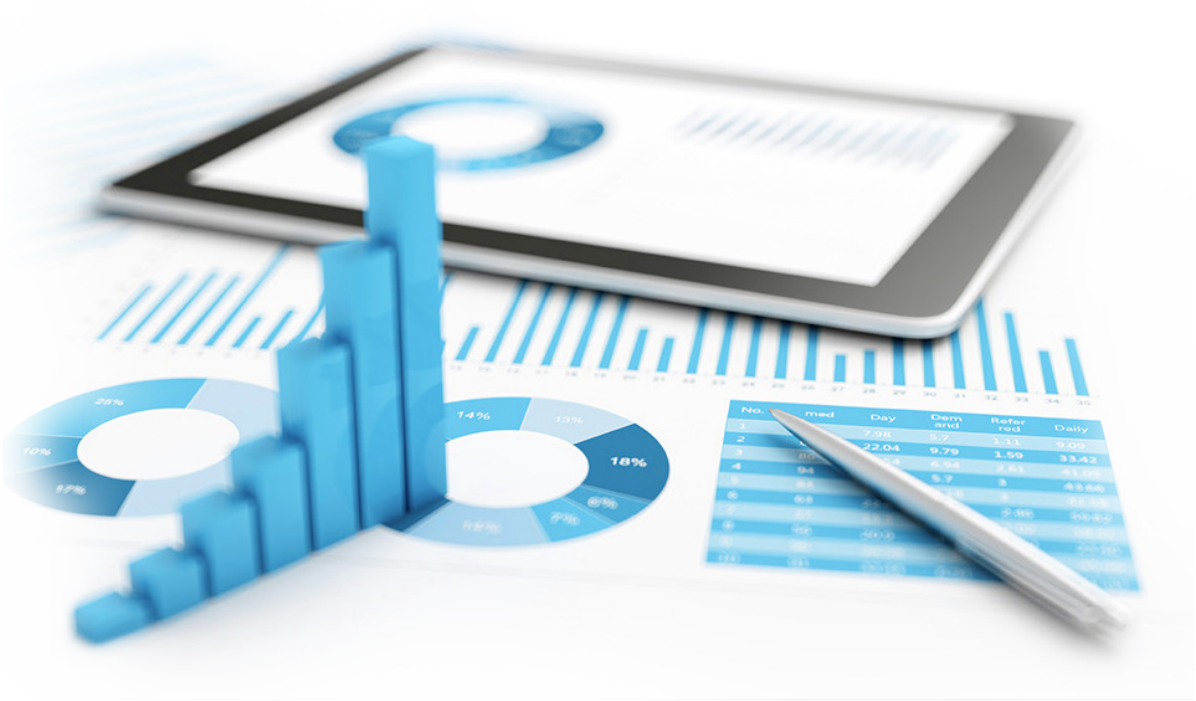
NOVASTOR
Backup wie für mich gemacht.

Leitfaden zum Erstellen eines Backup-Konzeptes

Exemplarische Anleitung zum Erstellen eines Backup-Konzeptes.

Stand: Mai 2018



Einleitung

Heutzutage liegt der Großteil der geschäftskritischen Informationen und Daten Unternehmen nur noch in digitaler Form vor. Der Verlust bestimmter Daten, oder sogar des gesamten Datenbestandes hat schwerwiegende Folgen - bis zum Bankrott des Unternehmens. Hinzu kommt, dass jeder Gewerbetreibende verpflichtet ist, geschäftliche Unterlagen über einen bestimmten Zeitraum aufzubewahren. Bei Verlust der Daten haftet der Geschäftsführer.

Datenverlust kann durch den Ausfall oder Fehlfunktion der IT ausgelöst werden, aber es gibt etliche weitere Bedrohungen geschäftskritischer Daten durch höhere Gewalt, Cyberkriminalität oder Bedienungsfehler. In jüngster Zeit nehmen die Angriffe auf Systeme und Daten durch Viren und Trojaner zu. Ransomware wie Locky, oder WannaCry sind sogenannte Verschlüsselungstrojaner, die Ihren gesamten Datenbestand verschlüsseln und dann für die Entschlüsselung Lösegeld fordern.

Nach einem Cyber-Angriff, Systemausfall oder Bedienungsfehler ermöglicht nur ein aktuelles und funktionierendes Backup aller wichtigen Daten und Systeme die umgehende Rückkehr zum Tagesgeschäft. Doch wodurch zeichnet sich eine aktuelle und funktionierende Datensicherung aus?

Ein effizientes und sicheres Backup beginnt nicht mit der Auswahl eines Sicherungsmediums, sondern mit der Planung des Backup-Konzeptes. Denn Backup stellt Unternehmen vor die große Herausforderung, Szenarien eines Datenverlustes möglichst vollständig und realistisch vorauszudenken.

Hat man sich einen Überblick verschafft, gilt es die Bedrohungen in geeignete Vorkehrungen zu übersetzen. Zum Beispiel schützt ein Backup auf einer direkt an den Rechner angeschlossenen Festplatte vor dem Verlust versehentlich gelöschter Daten; jedoch nicht vor Einbrechern, die sämtliche Hardware entwenden. Zu identifizieren sind sowohl die Ereignisse, die einen Datenverlust zur Folge hätten, als auch die Maßnahmen, die im jeweiligen Fall einen Restore erlauben würden.

Als wäre das Gedankenspiel um Datenverluste noch nicht genug, haben Gesetzgeber in Berlin und Brüssel Datenschutzverordnungen wie z.B. die EU - DSGVO erlassen und Pflichten für Unternehmer definiert. Wer Daten – insbesondere personenbezogene Daten - sichert, muss dabei gesetzlich vorgegebene Regeln befolgen. Aufsichtsbehörden wachen darüber und führen Unternehmensprüfungen durch.

In beiden Fällen hilft ein sorgfältiges Backup-Konzept. Ist das Konzept solide geplant und konsequent implementiert, trennt nur die Restore-Dauer Unternehmen nach einem Schadensfall von der Rückkehr zum Tagesgeschäft. Und stehen Prüfer vor der Tür, erfüllt die Vorlage des Backup-Konzeptes bereits einen wesentlichen Teil der Dokumentationspflicht.

Dieses Dokument hilft Ihnen, schnell und effizient ein umfassendes Backup-Konzept zu erstellen. Der Leitfaden erlaubt Ihnen, individuell alle wichtigen IT-Umgebungs- und Sicherheitsaspekte Ihrer IT sowie gesetzliche Vorgaben zu berücksichtigen.

Der generische Aufbau des Dokuments berücksichtigt unterschiedliche Komplexitätsstufen der IT-Umgebungen und variierende Anforderungen an Datensicherheit: Beim Durchlaufen des Leitfadens entscheiden Sie, welche Punkte für Ihren Anwendungsfall relevant sind. Sollten Sie mit den für Sie geltenden Anforderungen nicht ausreichend vertraut sein, sollten Sie einen externen IT-Berater oder NovaStor hinzuziehen.

Bestandsaufnahme

Um ein professionelles Backup-Konzept zu erstellen, müssen Sie einige Informationen zusammentragen, die Sie als Grundlage für Ihre Planung brauchen.

Die folgenden sechs Kategorien führen Sie durch alle wichtigen Themen und Fragestellungen für die Erstellung eines individuellen Backup-Konzeptes:

Aufnahme & Analyse der Geschäftsanforderungen > Identifikation der individuell greifenden Gesetze & Regelungen > Bestandsaufnahme der eingesetzten & geplanten IT-Systeme > Sicherheitsmaßnahmen > Organisation > Backup-Strategie

Aufnahme und Analyse der Geschäftsanforderungen

Wer seine Anforderungen nicht kennt, merkt erst bei einem Daten- oder Systemverlust dass wichtige Ziele des Backup nicht erfüllt wurden. Die Folge sind im besten Fall ein inakzeptabel langer Restore Prozess (RTO), im schlimmsten Fall ist überhaupt kein Restore mehr möglich.

❶ RTO (Recovery time objective)

- „Der RTO ist die maximal tolerierbare Länge eines Zeitraums, die ein Computer, IT-System, Netzwerk oder eine Anwendung ausfallen darf."
- Verfügbarkeitsanforderungen der IT-Anwendungen und der Daten
  - Hiervon ist maßgeblich abhängig, welche Backup-Strategie gewählt wird. Je höher zum Beispiel die Verfügbarkeitsanforderungen sind, desto kleiner sollte der Sicherungsintervall gewählt werden. Auch sollen die Sicherungen bei einem Datenverlust oder Systemausfall ohne Verzögerung zur Verfügung stehen.
- Reaktionszeiten im Desaster-Fall
  - Die Reaktionszeiten sind natürlich wieder maßgeblich von den Verfügbarkeitsanforderungen abhängig.
  - Am besten wird eine Liste von möglichen Desaster Fällen erstellt und man legt für jeden dieser Fälle entsprechende Reaktionszeiten fest. Sollten hierfür unterschiedliche Personen in Frage kommen, müssen auch die entsprechend mit aufgenommen werden.
- Rekonstruktionszeiten bei vorhandener Datensicherung
  - Als Basis hierfür dient wieder die Liste der möglichen Desaster Fälle. So kann man für jeden Desaster Fall auch abhängig von den Verfügbarkeitsanforderungen die zu erwartenden Rekonstruktionszeiten definieren.

❷ RPO (Recovery point objective)

- „Ist der Zeitraum, der zwischen zwei Backups liegen darf, um den Normalbetrieb nach dem Absturz eines Computers, IT-Systems oder Netzwerks sicherzustellen."
- Häufigkeit und Zeitpunkt der Datensicherung
  - Typischerweise werden geschäftskritische Daten einmal täglich gesichert. Manchmal ist es ratsam den Sicherungsintervall zu erhöhen. Beispielsweise ergibt es Sinn eine SQL Datenbank mehrmals am Tag zu sichern, da man nach einem Restore nur mit sehr hohem Aufwand die im Backup fehlenden Daten rekonstruieren kann.

❸ Vertraulichkeitsbedarf der Daten

- Zur Festlegung der Sicherheitsmaßnahmen für die Sicherungen ist die Vertraulichkeit der jeweiligen Daten festzulegen. Es muss also geklärt werden, ob bestimmte Daten z.B.
  - gesondert gesichert werden müssen
  - mit einem speziellen Passwort verschlüsselt werden müssen
  - bei der Auslagerung spezielle Regeln beachtet werden müssen

❹ Abhängigkeit der Organisation vom Datenbestand

- Die höchste Abhängigkeit des Unternehmens liegt bei den Daten, die bei Verlust zur Geschäftsaufgabe führen können - also essentielle Daten, ohne die das Geschäft nicht weitergeführt werden kann. Das sind in der Regel die Daten, die bei den Verfügbarkeitsanforderungen ganz oben auf der Liste stehen.

- Hierzu gehören auch Daten, die gesetzlichen Aufbewahrungs-bestimmungen unterliegen.

❺ Aufbewahrungsfristen

- Neben den gesetzlichen Vorgaben, die gleich noch in einem eigenen Kapitel behandelt werden, definieren sich die Aufbewahrungsfristen über die Art und Wichtigkeit der Daten

- Hierbei gilt zu beachten, dass ein Backup die Aufgabe hat, nach einem Datenverlust oder Systemausfall so schnell und so nah wie möglich auf den letzten Stand wiederherzustellen. Typischerweise ist das je nach Bedarf ein Zeitraum von 1-4 Wochen.

- Für Zeiträume darüber hinaus spricht man von Langzeit-Datenaufbewahrung. Hierfür müssen weitere Faktoren beachtet werden, zum Beispiel die Wahl eines haltbaren Mediums, seine Lagerung, Verifizierung usw. Dieses Dokument ist auf das Thema Backup Konzept fokussiert. Gerne beraten unsere Spezialisten Sie separat zum Thema Langzeitdatenaufbewahrung.

❻ Welche Backup Fenster stehen zur Verfügung?

- Bei den meisten Firmen steht die Nacht für Backups zur Verfügung und man hat in der Regel genügend Zeit für das Backup.

- Firmen, die im Schichtbetrieb bis hin zum 24/7 Betrieb arbeiten, müssen die Backup-Fenster auf die Produktionsabläufe abstimmen. Die Backup-Infrastruktur ist auf die spezifischen Anforderungen auszulegen, um Daten im laufenden Betrieb zu sichern und die produktiven Systeme so wenig wie möglich und so kurz wie möglich mit dem Backup zu belasten.

Welche gesetzlichen Vorgaben müssen eingehalten werden?

Die Einhaltung gesetzlichen Vorgaben zum Umgang mit Daten gehört zu den Geschäftsanforderungen. Die aus Gesetzen resultierenden Anforderungen ergänzen die Frage nach Restore-Fenstern um einen eigenständigen Anforderungskatalog. Im Folgenden wird die Berücksichtigung rechtsverbindlicher Aspekte im Datensicherungskonzept separat dargelegt.

❶ Gibt es vorgegebene Aufbewahrungszeiten für bestimmte Daten?

- Jeder Gewerbetreibende ist verpflichtet, geschäftliche Unterlagen über einen bestimmten Zeitraum aufzubewahren. Man unterscheidet dabei Fristen von sechs und zehn Jahren.
  - Unabhängig davon gibt es etliche weitere Dokumente wie Bilder oder Patente, die mit unterschiedlichen Aufbewahrungszeiten belegt sind.
  - Einen guten Überblick bietet z.B. diese Webseite der Handelskammer Hamburg

❷ Müssen personenbezogene Daten besonders behandelt werden?

- Die EU Datenschutz-Grundverordnung DSGVO vom 24. Mai 2016 regelt den Umgang mit personenbezogenen Daten. Ab 25. Mai 2018 ist die Anwendung der DSGVO rechtsverbindlich. Verstöße werden geahndet.

- Mehr Informationen hierzu:
  - DSGVO - Datenschutz-Grundverordnung
  - EU GDPR - General Data Protection Regulation

❸ Müssen Backups ausgelagert werden?

- Backups müssen räumlich von den Produktivsystemen getrennt sein.

- Experten empfehlen unter anderem die 3-2-1 Backup Strategie mit folgenden Vorgaben:
  - Halten Sie Ihre Daten 3-fach.
  - Speichern Sie Ihre Daten auf mindestens 2 Speicher-Technologien.
  - Lagern Sie mindestens 1 Backup extern.

- Ein Backup der geschäftskritischen Daten außerhalb der Geschäftsräume und damit räumlich getrennt von der produktiven Umgebungen aufzubewahren, ist also ein Muss. Das ausgela-

gerte Backup ist eventuell die einzige Chance, die Daten z.B. nach einem Brand, Einbruch mit Diebstahl oder Ransomware-Angriff wiederherzustellen.

- In den meisten Fällen werden für die Auslagerung portable Backup-Medien wie ein RDX, USB-Laufwerk, Band oder Cloud Backup genutzt.
- Wenn vorhanden, bietet sich ein zweiter Brandabschnitt für die Datensicherung an.

❹ Was ist in Bezug auf gesetzliche Vorgaben bei der Auslagerung von Backups zu beachten?

- Personenbezogene Daten dürfen nicht in fremde Hände gelangen.
  - Daher müssen ausgelagerte Backups verschlüsselt werden.
- Jeder Gewerbetreibende ist verpflichtet, geschäftliche Unterlagen über einen bestimmten Zeitraum aufzubewahren. Ein Verlust dieser Daten hätte rechtliche Konsequenzen.
  - Es sollten ausschließlich robuste und für den regelmäßigen Transport geeignete Datenträger genutzt werden, z.B. RDX oder Band-Medien.
  - Um die Lesbarkeit der Medien nicht zu gefährden, ist auf optimale Umgebungs- und Lagerbedingungen für die Backup-Medien zu achten.

Bestandsaufnahme der bereits eingesetzten und geplanten IT-Systeme

Die Bestandsaufnahme erfasst IT-Systeme, Anwendungen und Daten sowie die Backup-Anforderungen, die sich jeweils aus den geschäftlichen Anforderungen und gesetzlichen Regelungen ergeben. Ein kundenorientiertes und zukunftssicheres Backup-Konzept berücksichtigt neben dem Ist-Zustand die kurz- und mittelfristige Planung, um unnötige Folgekosten zu verhindern.

Die Bestandsaufnahme erfasst und klassifiziert sämtliche Systeme an allen Standorten des Unternehmens. Um auf Basis der Bestandsaufnahme Backup-Strategien zu definieren, bieten sich die folgenden vier Kategorien für die Klassifizierung der Geschäftsdaten an.

1. Geschäftskritisch – muss gesichert werden
2. Geschäftskritisch – unterliegt gesetzlichen Regelungen oder internen Regelungen
3. Nicht geschäftskritisch – soll aber auch gesichert werden
4. Nicht geschäftskritisch – keine Sicherung

Die Backup-Strategie muss alle geschäftskritischen Systeme und Daten berücksichtigen.

INFO Wir empfehlen zur Datenklassifikation die eingangs dargelegten Aspekte der Geschäftsanforderungen und gesetzlichen Regelungen heranzuziehen.

Checkliste für die Bestandsaufnahme

Um die IT-Infrastruktur eines Unternehmens vollständig zu erfassen, haben wir eine Checkliste entwickelt. Mit unserer Checkliste nehmen Sie die Unternehmens-IT so auf, dass Ihnen beim späteren Einrichten der Datensicherung mit NovaBACKUP alle relevanten Informationen direkt vorliegen.

Produktive Umgebung

- pro Standort und System
- aktuell + geplant
- kategorisiert (geschäftskritisch ja/nein)
  - Hosts
    - Plattform
  - Server
    - Physisch
    - Virtuell
  - Software
    - Betriebssystem
    - Applikationen
  - Netzwerk Anbindung
  - Art der Daten pro Maschine (File, DB, VM ...)
    - Datenvolumen aktuell
    - Datenwachstum pro Jahr
    - Änderungsvolumen pro Tag
    - Änderungszeitpunkte der Daten

Backup Infrastruktur

- Backup Software
  - Lizenzen
- Backup Server
- Backup Speicher
  - Lokal
  - Cloud
    - Welche Plattform
- Netzwerk Anbindung
  - Lokales Netzwerk
  - Wenn Cloud Backup
    - Verfügbare Internet-Bandbreite
  - Wenn andere Standorte
    - Welche Anbindung (WAN, VPN...)
    - Verfügbare Bandbreite
- Monitoring

Bedrohungsanalyse

Der Gesetzgeber verpflichtet Unternehmer und Unternehmen, angemessen für IT-Sicherheit und Datensicherung zu sorgen. Daher erfordert das Backup-Konzept eine Bedrohungsanalyse. Zu ermitteln sind die wichtigsten potentiellen Gefahren wie Hardware-Fehler, Diebstahl oder Cyber-Angriffe. Daraus leiten sich entsprechende Schutzmaßnahmen ab. Diese werden priorisiert und in Form von Sicherheitsrichtlinien festgehalten.

Mit Blick auf das Backup-Konzept dient die Bedrohungsanalyse dazu, passende Backup-Strategien und Speichertechnologien auszuwählen. Hierzu zählen die folgenden

❶ Auslagerung / räumlich getrennte Verwahrung von Sicherungsmedien

- Aufbewahrungsort der Backup-Datenträger
- In einer Vielzahl von Bedrohungsszenarien ermöglicht nur die Auslagerung einer Sicherung einen Restore nach dem Datenverlust. Eine Datensicherung ist getrennt von den produktiven Systemen bzw. außerhalb der Firmenräume zu lagern, um nach einem Desaster, das die produktive Umgebung betraf, ein unbeschädigtes Backup für das Desaster Recovery zur Verfügung zu haben.

❷ Verschlüsselung

- Personenbezogene Daten dürfen nicht in fremde Hände gelangen. Daher müssen Backups, die ausgelagert werden, zuverlässig verschlüsselt werden.

Ergänzende Sicherheitsmaßnahmen

Neben dem Backup tragen weitere Maßnahmen zur IT-Sicherheit bei. Hierzu zählen Zugriffskonzepte oder die Firewall, die zwar nicht Teil des Backup-Konzeptes sind, aber zum Schutz der Daten gehören und gleichermaßen fundiert geplant werden müssen.

Der Fokus dieses Dokuments liegt zwar auf dem Thema Backup, aber um den bestmöglichen „Rund-um-Schutz“ für die IT zu gewährleisten, führen wir hier einige Themen auf, die neben dem Backup maßgeblich zur IT-Sicherheit beitragen.

- Firewall
- Sicherheitslösung zum Schutz vor Viren und Trojanern
- Monitoring

Fragen Sie beim Hersteller Ihrer Wahl an, um für die jeweiligen Komponenten Info-Flyer oder Leitfäden zu erhalten und die Planung der IT-Sicherheit zu optimieren.

Zu den Themen, die im Maßnahmenkatalog aus der Bedrohungsanalyse nicht fehlen dürfen, zählen die folgenden.

- Zuweisung von Zugriffsberechtigungen durch Benutzer- und Rechteverwaltung
  - In vielen Unternehmen gibt es keine Rechteverwaltung und jeder hat volle Zugriffsrechte. Eine Rechteverwaltung hilft maßgeblich unautorisierte Zugriffe zu verhindern und auch die Verbreitung von Schadsoftware einzudämmen.
- Schutz vor Schadsoftware wie Ransomware
  - Hier hilft nur eine Kombination der oben aufgeführten Maßnahmen aus Firewall, Sicherheitslösungen, etc.
  - Speziell zum Thema Schutz gegen Ransomware finden NovaStors Partner in NovaStors Partnerportal ein gesondertes Dokument mit nützlichen Informationen.

Organisation

Neben dem technischen Teil des Backup definiert das Datensicherungskonzept etliche organisatorische Aspekte. Rund um die Datensicherung fallen einige essentielle Aufgaben an, für die Verantwortlichkeiten definiert und schriftlich festgehalten werden müssen.

❶ Übergabe-Protokoll

- Wenn Sie ein Dienstleister sind, der sich um die IT des Unternehmens kümmert, das Backup Konzept erstellt und die Backup Infrastruktur eingerichtet hat, sollten Sie ein Übergabe Protokoll erstellen.

  Aufgabe: Bei der Übergabe muss der Geschäftsführer Ihres Kunden bzw. des relevanten Unternehmensteils oder der Abteilung Ihres Kunden das Übergabe-Protokoll abzeichnen.

- Im Übergabe Protokoll sollten folgende Dinge enthalten sein:
  - Was wird wie, wann und wohin gesichert
  - Besondere Aufbewahrungsregeln
    - Ggf. die langfristige Vorhaltung von arbeitsfähigen Lesegeräten für die ursprünglich eingesetzte Backup-Technologie
  - Bestätigung der Lauffähigkeit des Backups zum Zeitpunkt der Übergabe
  - Vorgehensweise bei Ausfällen, verdächtigem Verhalten der Computer (Ransomware, Cyber-Angriff) usw.
  - Verantwortlichkeiten
    - Wer ist für was verantwortlich?
    - Backup-Medien Verwaltung
    - Regelmäßige Prüfung des Backups
    - Transportmodalitäten für das ausgelagerte Backup
    - Monitoring
  - Festlegung der Vorgehensweise für eine Wiederherstellung

❶ Übergabe-Protokoll

- Schulung und Sensibilisierung der Mitarbeiter
- Vertragsgestaltung (bei externen Archiven oder Cloud Backup)
- Restore/Recovery-Szenarien
- Restore-Übungen in angemessenen Abständen

Backup-Strategie

Gemäß den Bestandsaufnahmen sowie den zuvor ermittelten Vorgaben und Informationen kann jetzt die passende Backup-Strategie erstellt werden.

Anhand der „Bestandsaufnahme der bereits eingesetzten und geplanten IT-Systeme“ legen Sie jetzt fest, was, wie und wohin gesichert wird. Die folgende Checklist hilft Ihnen, alle wichtigen Informationen für die Backup-Strategie zu erfassen. Um Ihnen die Arbeit zu erleichtern, stellen wir mit diesem Dokument eine Excel-Liste zur Verfügung, in der Sie alle Informationen einheitlich für alle zu sichernden Daten eintragen können.

Wichtig! – Diese Liste wird für jede Maschine und jeden Backup-Typ durchlaufen.

- Maschinen Name
- Backup-Typ
  - Physische Maschine
  - Virtuelle Maschine(n)
  - Daten
  - Anwendungssicherung
- Klassifikation
  - geschäftskritisch
  - RTO (Recovery time objective)
  - RPO (Recovery point objective)
- Unterliegen die Daten einem Gesetz (besonderes Handhabung)
  - Hiervon ist abhängig, welche besonderen Maßnahmen wie Verschlüsselung oder Aufbewahrungszeiträume beim Backup berücksichtigt werden müssen.
- Backup Fenster
  - Hiervon ist maßgeblich abhängig, welche Strategie später bei der „Backup Methode“ gewählt wird
- Datenvolumen
  - Das gesamte Datenvolumen, das von dem jeweiligen „Backup-Typ“ gesichert wird.
- Änderungsvolumen basierend auf dem Backup-Zyklus

- Backup Medium Typ
  - Lokales Backup
  - Ausgelagertes Backup
- Anzahl der benötigten Backup-Medien
- Backup-Methode
  - Voll, inkrementell oder differentiell
  - Voll-Backup
    - Jedes Mal, wenn Die Sicherung ausgeführt wird, werden alle selektierten Daten gesichert.
  - Differentielles Backup
    - Es werden nur Daten gesichert, die sich seit der letzten Vollsicherung geändert haben oder neu hinzugekommen sind. Der Restore erfordert das Voll-Backup und das differentielle Backup des gewählten Wiederherstellungspunktes.
  - Inkrementelles Backup
    - Es werden nur Daten gesichert, die sich seit der letzten inkrementellen Sicherung geändert haben oder neu hinzugekommen sind. Der Restore erfordert das Voll-Backup und alle inkrementellen Sicherungen bis zum gewählten Wiederherstellungspunkt.
  - Verschlüsselung
  - D2D, D2D2D, D2D2T etc.
    - Ein Beispiel wäre D2D2T: Von der Disk (D2D2T) des Produktivsystems erfolgt ein Backup auf einen Disk-Speicher, z.B. ein NAS, (D2D2T) als lokales Backup. Für die Auslagerung erstellt z.B. der Backup Server eine Kopie der Sicherung auf einen portablen Backup Speicher, in unserem Beispiel ein Tape (D2D2T).
  - Zeitplanung / Refresh-Zyklen der Datensicherung
  - Alter/Anzahl der Backup Generationen
    - In der Backup Software kann definiert werden, ab welchem Alter oder welcher Backup-Anzahl , die ältesten Sicherungen aufgeräumt werden. Hiermit kann zum einen die Aufbewahrungsdauer festgelegt werden, gleichzeitig wird hierüber sichergestellt, dass auf dem Backup Medium jederzeit genug Speicherplatz für neue Sicherungen verfügbar ist.
    - Um zum Beispiel tägliche Backups über eine Arbeitswoche für den Restore zur Verfügung zu haben reichen 5 Wechselmedien, die täglich gewechselt werden und deren Sicherungen in der Folgewoche täglich überschrieben werden. Verfügen die Medien über ausreichende Kapazität, um mehrere Tages-Backups aufzunehmen, lässt man die Ba-

ckup Software Sicherungen nacheinander auf dasselbe Medium schreiben. Zusätzlich definiert man in der Backup Software nach welchem Alter/ welcher Anzahl die Medien aufgeräumt werden.

- Das Generationenprinzip „GFS“ ist auch unter der Bezeichnung „Großvater-Vater-Sohn“ geläufig. Das Backup besteht dabei aus drei Teilen, die in bestimmten Intervallen überschrieben werden. So umfasst zum Beispiel der „Sohn“ ein Tages-Backup, der „Vater“ ein Wochen-Backup und der Großvater ein Monats-Backup.

  Hier ein Beispiel: Bei einer 5-Tage-Woche würde an den ersten vier Werktagen pro Werktag eine Sicherung auf ein Medium geschrieben und wöchentlich von einer neuen Sicherung an eben diesem Werktag überschrieben. Für Montag bis Donnerstag würde man dementsprechend vier Medien benötigen. Am fünften Werktag würde die erste Wochensicherung stattfinden.

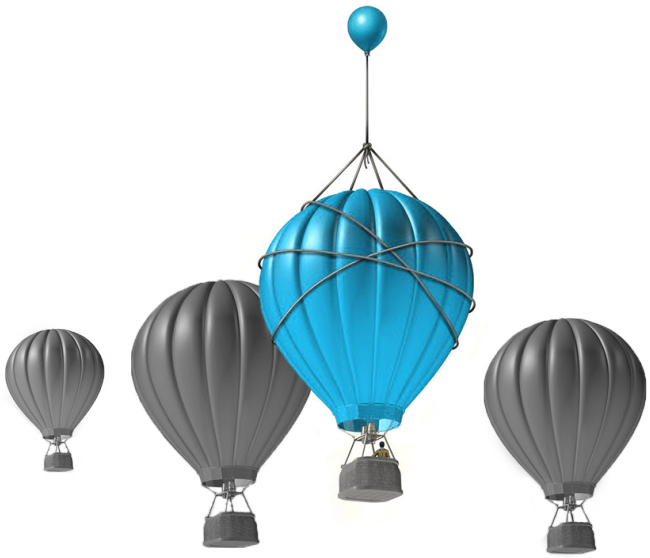
  Einmal pro Woche, wie gesagt jeweils am fünften Werktag, findet die automatische Wochensicherung statt. Diese wird erst nach der ersten Monatssicherung wöchentlich überschrieben. Bei einem vier-Wochen-Rhythmus würde man drei Medien für Wochensicherungen benötigen. In der vierten Woche würde die Monatssicherung erfolgen.

  Das letzte Wochen-Backup des jeweiligen Monats dient als Monatssicherung. Diese werden erst überschrieben, wenn der erste definierte Monatszyklus abgeschlossen ist. Legt man den Zyklus auf ein Jahr fest würde die erste Monatssicherung also im zwölften Monat überschrieben.

- Prozess Definitionen
  - Die folgenden Punkte beschreiben die zugehörigen Prozesse. Wenn mehr als ein System gesichert wird, gehört diese Angabe in das Übergabeprotokoll.
    - Medienwechsel Prozess
    - Auslagerungsmethode und Prozess
    - Aufbewahrungsprozess für bestimmte Medien
    - Monitoring und Reporting
    - Verantwortlichkeiten

Sie haben nun alle wichtigen Informationen für die Backup-Strategie erfasst.

Gleichzeitig liegen Ihnen nun die notwendigen Informationen zur Ermittlung des Lizenzbedarfs vor. Im letzten Schritt dienen die Informationen dazu, die eventuell bereits vorhandene Backup Infrastruktur daraufhin zu prüfen, ob alle Backup- Anforderungen und -Strategien abgedeckt sind - oder die Backup Infrastruktur an bestimmten Stellen aktualisiert oder erweitert werden muss. Beispielsweise ist zu prüfen, ob alle benötigten Backup-Speicher mit entsprechender Speicherkapazität vorhanden sind.



Schlusswort & Bitte um Feedback

Das Backup-Konzept gehört zur professionellen Abwicklung von Backup-Projekten und stellt gleichzeitig einen kostenpflichtigen Mehrwert dar.

NovaStor hat diesen Leitfaden verfasst, um IT-Systemhäusern das Erstellen eines Backup-Konzeptes zu erleichtern. Ihnen bleibt überlassen, ob Sie es nutzen möchten, um zu Ihre Leistung gegenüber dem Kunden kostenfrei in einem groben Übergabe-Protokoll zu dokumentieren – oder ein vollständiges Backup-Konzept kostenpflichtig bereitzustellen.

Selbst bei kleinen Installationen, bei denen nur ein Server auf einem lokal angeschlossenen Medium gesichert wird, lohnt sich das Übergabe-Protokoll, beispielsweise um dem Kunden zu verdeutlichen, dass er seine Sicherung selbst überwachen – oder Sie mit dem Monitoring beauftragen muss.

INFO

Nun zurück zu uns!

Haben wir unser Ziel erreicht? Bietet unser Leitfaden Ihnen die angestrebte Hilfestellung? Bewährt er sich in Ihrem Alltag?

NovaStors Team freut sich über Ihre Rückmeldung per Mail an partner@novastor.com

Über NovaStor

NovaStor ist Ihr Hamburger Hersteller von Backup & Restore Software und Experte für Datensicherungslösungen. NovaStors Backup- und Restore-Software für Unternehmen und Behörden sichert heterogene Netzwerkinfrastrukturen mit physischen und virtualisierten Umgebungen. NovaStors Lösungen unterstützen sämtliche Speichertechnologien von Disk über Tape bis Cloud.

Als deutscher Anbieter steht NovaStor mit seinen Backup & Restore Software Produkten wie mit seinen Dienstleistungen für höchste Qualität, Geschwindigkeit und Stabilität. NovaStors kostenoptimale Lösungen sind hersteller- und hardwareneutral. Getreu seiner Philosophie "Backup wie für mich gemacht" bietet NovaStor Kunden und Partnern technisch, wirtschaftlich und rechtlich optimale Lösungen zur Wiederherstellung ihrer Daten.

NovaStor ist inhabergeführt und mit rund 100 Mitarbeitern an drei Standorten in Deutschland (Hamburg), USA (Agoura Hills) und der Schweiz (Zug), sowie durch Partnerunternehmen in zahlreichen weiteren Ländern vertreten.

NOVASTOR
Backup wie für mich gemacht.

Made in Germany | 100% Hamburger Support

NovaStor Software GmbH
Neumann-Reichardt-Str. 27-33
D- 22041 Hamburg

Tel.: +49 (0)40 638 09 9988
Fax: +49 (0)40 638 09 29

Mail: kontakt@novastor.de

www.novastor.de

Zum Anfang »