Datensicherung / Wiederherstellung / Disaster Recovery

Eine Kundeninformation der

ITSM – Gesellschaft für
Informationstechnologie
und Services Meiß mbH
Elisabeth-Selbert-Straße 19a
40764 Langenfeld

Management Summary

Viele Unternehmen widmen dem Thema Datensicherung nicht genügend Aufmerksamkeit. Häufig wurde bei der Serverinstallation zwar eine Datensicherung eingerichtet, jedoch keine Datensicherungsstrategie etabliert. Meist fehlt auch ein Notfallwiederherstellungsleitfaden im Unternehmen. Oft erkennen die verantwortlichen Manager zu spät, dass solche Themen im Rahmen des Risikomanagements einen hohen Stellenwert einnehmen müssen – nämlich dann, wenn es zum endgültigen Verlust wichtiger Unternehmensdaten gekommen ist.

Die Methoden der Datensicherung sind häufig nicht ausreichend und konsequent genug umgesetzt, um eine reibungslose Wiederherstellung im Notfall zu gewährleisten.

ITSM empfiehlt die Implementierung einer mehrstufigen Datensicherungsstrategie. Hierbei werden erst alle Daten aller Server im Netzwerk auf einem Datensicherungsserver gesammelt, um diese anschließend auf Bänder zu duplizieren. Bänder haben den Vorteil, dass diese keinesfalls antiquierte Technik ein gutes Preis-/Leistungsverhältnis und eine lange Lebenszeit im Bereich der Einlagerung der Medien bietet.

Der Einsatz der Servervirtualisierung unterstützt die Datensicherungsstrategie, weil die Wiederherstellung von virtuellen Maschinen wesentlich schneller abläuft als die Wiederherstellung eines Servers aus einer auf Dateiebene erstellten Sicherung.

Die Datensicherungsmedien müssen regelmäßig außer Haus gelagert werden, damit diese bei einem Ereignis wie Brand oder Einbruch nicht zerstört werden und für eine Wiederherstellung zur Verfügung stehen. Externe USB-Festplatten würden bei diesem regelmäßigen Transport schnell einen mechanischen Defekt erleiden. Bänder sind wesentlich robuster.

Eine gute Datensicherungsstrategie muss aber auch einen Wiederbeschaffungsplan umfassen. Im Notfall muss das Unternehmen darauf vorbereitet sein, die komplette IT-Landschaft neu erstellen zu müssen. Hierzu ist nicht nur eine gute Dokumentation notwendig, sondern auch ein Beschaffungsleitfaden.

Die Vermeidung von Datenverlusten kann je nach Umfang der gewählten Maßnahmen kostspielig und aufwändig sein, aber in einigen Branchen kann der endgültige Verlust von Daten leicht zum Zusammenbruch eines Unternehmens oder zumindest zu einem hohen Image- und Umsatzverlust führen.

Eine mögliche Alternative kann die Übertragung der Aufgaben an einen Dienstleister sein, der eine angemessene Infrastruktur in einem deutschen Rechenzentrum unterhält und für eine regelmäßige Auslagerung der kritischen Daten sorgt. Bei diesem Szenario ist unbedingt darauf zu achten, dass es eine saubere Aufgabentrennung zwischen den Vertragspartnern gibt.

Einleitung

Der Verlust von Daten kann vielfältige Gründe haben: Anwender löschen unbeabsichtigt Dateien, Viren überschreiben wichtige Systemdaten, defekte Festplatten sorgen für einen Totalausfall, oder äußere Einflüsse wie Feuer, Hochwasser usw. zerstören die Serverumgebung. Häufig stehen Server auch nicht in besonders geschützten Räumen, so dass sie bei einem Einbruch durch Diebstahl oder Vandalismus ebenfalls gefährdet sind.

Dem Risiko des Datenverlusts wird häufig zu wenig Aufmerksamkeit gewidmet. Dabei kann der Verlust von Unternehmensdaten, die nicht wiederherstellbar sind, die Existenz eines Unternehmens gefährden.

Dieses White Paper soll mittelständischen Unternehmen als Leitfaden und Entscheidungsgrundlage für eine sichere und zuverlässige Datensicherungsstrategie dienen.

Datensicherung

Bei der Sicherung von Dateien kann zwischen folgenden Sicherungsmethoden unterschiedenen werden:

- Vollständige Sicherung
- Inkrementelle Sicherung
- Differenzielle Sicherung

Eine auf Dateiebene operierende Datensicherung sollte mindestens einmal wöchentlich eine vollständige Sicherung aller Dateien eines Servers beinhalten. Darüber hinaus sollte einmal täglich eine differenzielle Sicherung ausgeführt. Bei einer hohen Änderungsfrequenz kann auch mehrmals täglich eine inkrementelle Sicherung ausgeführt werden.

Es ist nicht ausreichend, nur definierte Verzeichnisse zu sichern, da Anwender und Programme häufig auch außerhalb dieser definierten Pfade Dateien unbemerkt ablegen. Fällt ein Server komplett aus und muss dieser aus der der Datensicherung wiederhergestellt werden, so ist es hilfreich, eine komplett Sicherung aller Dateien vorliegen zu haben.

Software und Server

Viele Betriebssysteme bringen bereits eine eingebaute Datensicherungssoftware mit. Diese Software unterliegt aber meist einigen Einschränkungen. So ist z.B. die gemeinsame Verwaltung mehrere Server nicht möglich. Eine professionelle Datensicherungssoftware unterstützt auch komplexe Datensicherungsprozesse wie z.B. die Duplizierung von angefertigten Backupsets auf weitere Medien oder auch die Verwendung von Agents, um Daten auf Anwendungsebene (z.B. Datenbanken) sichern zu können.

Ein dedizierter Datensicherungsserver sorgt dafür, dass die Datensicherung nicht durch Fremdsoftware negativ beeinflusst wird. Dies könnte z.B. in einer niedrigeren Performance resultieren.

Medien

- Optische Medien

  Optische Medien kommen für eine Datensicherung in Unternehmen aufgrund der geringen Speicherkapazität nicht in Frage.

- „In die Wolke“

  Immer wieder kommt die Frage auf, ob ein Online Backup nicht eine sinnvolle Alternative zur herkömmlichen Datensicherung ist. Unabhängig davon, in welcher Form dieses Online Backup umgesetzt werden soll, es scheitert meist an der benötigten Bandbreite beim Kunden vor Ort. Auch wenn mittlerweile flächendeckend Breitband Internetanschlüsse verfügbar sind, haben diese häufig einen wesentlich zu geringen Upload, um die Daten entsprechend zu einem Dienstleister ins Internet hochladen zu können.

Zur Veranschaulichung: Das Backup von 100 GB Daten bei einem Upload von 1 Mbit/s dauert ca. 9 Tage.

- Externe Festplatten

Grundsätzlich ist eine Datensicherung auf externe Festplatten nicht zu empfehlen, auch wenn der niedrige Kaufpreis zunächst verlockend ist. Aufgrund der physischen Eigenschaften einer Festplatte kann nicht garantiert werden, dass die Magnetisierung über lange Zeit außerhalb des Einsatzes der Festplatte bestehen bleibt. Des Weiteren sind externe Festplatten aufgrund ihrer mechanischen Eigenschaften sehr fehleranfällig (z.B. Schäden an den Schreib/Leseköpfen beim Transport, Schäden an der Elektronik). Beim Einsatz von externen Festplatten ist ein Generationenprinzip nur schwierig umsetzbar, da hierzu eine hohe Anzahl an Festplatten benötigt würde und die Festplatten den Ansprüchen auf eine Langzeiteinlagerung nicht genügen. Des Weiteren ist die Datenbandbreite im Vergleich zu anderen Datensicherungsmedien eher gering (USB2.0 max. 480Mbit/s).

- NAS

Ein Netzwerk Storage System ist ein geeigneter Speicherplatz in einer mehrstufigen Backupstrategie (Multi-Tier). Hierbei werden die Backups zuerst auf eine NAS abgelegt. Der Vorteil einer NAS ist, dass die Daten hier sehr schnell gespeichert werden können, ohne erst den Datenträger auf die richtige Position spulen zu müssen (s. Band).

Da eine NAS jedoch keinen Langzeitspeicher darstellt (kein Generationenprinzip und keine Auslagerung möglich), ist hier zwingend eine Auslagerung auf andere Speichermedien notwendig (z.B. Bänder).

Wenn es die bauliche Situation zulässt, kann ein zweites, gespiegeltes NAS an einem anderen Standort eine Alternative zu anderen Speichermedien sein. Hierbei ist zu beachten, dass in der Regel dann auch kein Generationenprinzip umgesetzt werden kann. Ein Unternehmen kann dieses Risiko akzeptieren und solche eine Backup-to-Disk-to-Disk Lösung umsetzen.

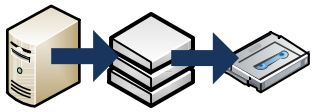
- Bänder

Die Datensicherung auf Bändern ist die klassische Methode. Die Bandtechnologie ist sehr ausgereift, wird kontinuierlich weiterentwickelt und ist keineswegs antiquiert. Gerade bei der Lagerung erreichen Bänder sehr gute Ergebnisse. Derzeit wird von einer Haltbarkeit von 30 Jahren ausgegangen.

Eine direkte Sicherung auf Bänder findet vor allem dann Einsatz, wenn eine hohe Transferrate gewährleistet ist. Wird über das Netzwerk gesichert, kann es zu dem sog. Start-Stopp-Betrieb des Laufwerks kommen. Das heißt: Werden die Daten über das Netzwerk nicht schnell genug geliefert, muss dass Bandlaufwerk anhalten (Stopp) und warten, bis wieder genügend Daten im Puffer sind, und kann erst dann fortfahren (Start). Dabei kommt es zu einer hohen mechanischen Belastung des Mediums und einer damit verkürzten Lebensdauer.

Hohe Transferraten sind vor allem in lokalen, schnellen Netzwerken oder im Bereich einer Multi-Tier Backupstrategie zu erreichen (z.B. Backup-to-Disk-to-Tape). Ein Start-Stopp-Betrieb kann die Lebensdauer von Bändern drastisch verkürzen.

Konzepte



- Backup-to-Tape (B2T oder D(isk)2T)

  Das Backup-to-Tape ist gut geeignet für eine Backupstrategie, bei der nur ein einzelner Server gesichert werden muss. Sobald jedoch mehrere Server gesichert werden sollen, bietet es sich an das Backup zuvor auf einem Festplattensystem zwischen zu speichern, damit die Start-Stopp-Problematik des Bandlaufwerks umgangen werden kann.

- Backup-to-Disk (B2D oder D2D)

  Beim Backup to Disk wird das Backup sofort auf eine Festplatte oder ein Festplattensystem geschrieben. Dieses Festplattensystem sollte sich nicht am gleichen Standort wie die Backuplösung befinden. Da hiermit jedoch kein Generationenprinzip umsetzbar ist, müssen die daraus resultierenden Risiken durch das Unternehmen abgewogen werden. Wird das Risiko akzeptiert, kann mit dieser Methode eine kostengüngstige Datensicherung durchgeführt werden.

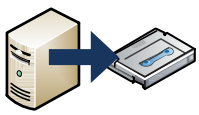
  Das Auslagern der Backupdaten mittels einer austauschbaren, externen Festplatte ist ab einer gewissen Datenmenge nicht mehr sinnvoll möglich. Des Weiteren sind externe Festplatten sehr stoßempfindlich.

- Backup-to-Disk-to-Tape (B2D2T oder D2D2T)

  Beim Backup-to-Disk-to-Tape können sehr hohe Datentransferraten erreicht werden, da die Daten von den zu sichernden Servern aus dem Netzwerk zuerst auf Festplattensystemen gesichert werden. Von dort aus werden die Daten sequenziell auf ein Band dupliziert.

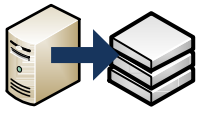
  Bei dieser Lösung können alle Vorteile beider Welten voll ausgeschöpft werden. Die Wiederherstellung der Daten kann sehr zeitnah erfolgen, da die Daten auf Festplatten vorliegen und auf der anderen Seite kann ein Generationenprinzip und die Auslagerung auf Bänder umgesetzt werden.

  B2D2T ist die bevorzugte Datensicherungsmethode für mittelständische Unternehmen.



Überwachung

Selbst die beste Datensicherungsstrategie ist wertlos, wenn sie nicht kontrolliert wird. Die Datensicherung muss regelmäßig auf Erfolg überprüft werden, und auch die Wiederherstellung muss regelmäßig getestet und geprobt werden.



Disaster Recovery

Der Begriff Disaster Recovery (Notfallwiederherstellung) bezeichnet Maßnahmen, die nach einem Unglücksfall in der Informationstechnik eingeleitet werden. Dazu zählt sowohl die Datenwiederherstellung als auch das Ersetzen nicht mehr benutzbarer Infrastruktur und Hardware.

Diese Maßnahmen müssen im Unternehmen definiert sein und regelmäßig geprüft und geübt werden. Hierzu gehören:

- Vorhalten von Hardware oder Beschaffung von Hardware im Notfall
- Erstellen und regelmäßige Prüfung des Wiederherstellungsleitfaden
- Prüfen der Dokumentation (Server, Netzwerk, Clients, Kennwörter, IP-Adressen)
- Regelmäßige Tests der Datenwiederherstellung
- Übung des Notfallszenarios

Virtualisierung

Die Servervirtualisierung kann im Rahmen der Datensicherung und insbesondere beim Disaster Recovery viel Zeit und Aufwand sparen.

Bei der Virtualisierung liegen alle Server in Form von virtuellen Maschinen vor. Diese virtuellen Maschinen sind Hardware unabhängig, da diese auf Treiberebene soweit abstrahiert sind, dass kein direkter Bezug mehr zur darunter liegenden Hardware besteht. Daher können diese virtuellen Maschinen auf nahezu beliebiger Hardware ausgeführt werden (die Voraussetzungen der Hypervisor-Hersteller müssen natürlich beachtet werden).

Alle gängigen Backupsoftware-Hersteller unterstützen die Sicherung von virtuellen Maschinen auf Basis einer Speicherabbildsicherung (Image Backup). Diese Speicherabbilde können sehr schnell auf anderer Hardware wiederhergestellt werden. Somit kann sehr viel schneller als mit einem File-Level Backup wieder ein betriebsbereiter Zustand erreicht wird.

Risikoübertragung auf einen Dienstleister

Eine zuverlässige, robuste Datensicherungsstrategie zu entwickeln, zu pflegen und auch im Unternehmensalltag umzusetzen, bedarf eines hohen Aufwands. Eine Alternative hierzu ist es, diese Aufgabe auf einen Dienstleister auszulagern.

Da dieser jedoch die Einhaltung der Vorgaben aus der Datensicherungsstrategie nur in den „eigenen vier Wänden“ gewährleisten kann, ist eine Auslagerung der Unternehmens IT in das Rechenzentrum dieses Dienstleisters sinnvoll. Der Dienstleister hält in der Regel eine professionelle IT-Infratruktur in diesem Rechenzentrum vor, die nicht nur vor dem Verlust von Daten durch eine optimale Datensicherungsstrategie geschützt ist, sondern auch durch weitere bauliche und organisatorische Maßnahmen, wie z.B. einem 24x7 Sicherheitsdienst und einer

Edelgas-Löschanlage. Diese Maßnahmen sind für mittelständische Unternehmen häufig zu kostenintensiv, um sie im eigenen Firmengebäude oder gar in gemieteten Räumen umzusetzen.

Durch diese Risikoübertragung auf den Dienstleister sinkt für den Auftraggeber das operative Risiko im Bereich der Datensicherung und Notfallwiederherstellung. Die Verantwortung dieser Maßnahmen liegt aber dennoch weiterhin beim Auftraggeber.

Glossar

Archivbit

Das Archivbit (auch Archiv-Attribut) ist ein Dateiattribut, das vom Betriebssystem bei neu angelegten oder veränderten Dateien gesetzt wird. Datensicherungsprogrammen kann hiermit signalisiert werden, dass diese Datei noch nicht gesichert wurde. Nach einer Sicherung sollte das Archivbit entsprechend wieder gelöscht und erst bei weiteren Veränderungen erneut gesetzt werden.

Archivierung

Die Begriffe Archivierung und Datensicherung werden häufig verwechselt. Beide Begriffe beschreiben ähnliche Technologien, verfolgen jedoch einen völlig gegensätzlichen Ansatz. Ein Archiv enthält diejenigen Daten, die sich nicht mehr ändern, sondern nur noch aufbewahrt werden. Hier geht es darum, die Daten über einen längeren Zeitraum geordnet abzulegen, um sie bei Bedarf gezielt wieder zu finden und darauf zugreifen zu können. Ein Backup wird hingegen vor allem von aktuellen und sich ständig ändernden Daten gemacht. Hier ist das oberste Ziel, im Falle eines Disasters die Daten möglichst vollständig und vor allem aber möglichst schnell wieder herzustellen. Backups sind der Schutz gegen Produktionsausfall.

Differenzielle Sicherung

Bei der differenziellen Sicherung werden alle Daten, die seit der letzten Vollsicherung geändert wurden oder neu hinzugekommen sind, gespeichert. Es wird also immer wieder auf der letzten Komplettsicherung aufgesetzt, wobei gegenüber einer neuen Vollsicherung Speicherplatz und Zeit gespart werden kann (sichert alle Dateien mit gesetztem Archivbit).

Generationenprinzip

Das Generationenprinzip stellt eine Strategie der Datensicherung dar. Es stellt sicher, dass immer mehrere Sicherungen in verschiedenen zeitlichen Abstufungen (Großvater, Vater, Sohn) vorhanden sind, um verschiedene Versionen für eine mögliche Wiederherstellung zur Verfügung zu haben. Sind die „Sohn“-Daten beschädigt, werden sie aus den „Vater“-Daten wieder erzeugt und die „Vater“-Daten gegebenenfalls aus den „Großvater“-Daten.

Ein übliches Generationenprinzip sieht wie folgt aus:

- Tägliche Sicherung (Werktags) auf Sohn-Medien (z.B. differenziell/inkrementell oder auch Vollsicherung)
  - Rotation der Medien jede Woche, d.h. es werden 5 Medien benötigt
- Wöchentliche Sicherung (Samstags) auf Vater-Medien (Vollsicherung)
  - Rotation der Medien jeden Monat, d.h. es werden 4 Medien benötigt
- Monatliche Sicherung (letzter Samstag im Monat) auf Großvater-Medien (Vollsicherung)
  - Rotation der Medien jedes Jahr, d.h. es werden 12 Medien benötigt

Nach diesem Prinzip könnte man stets auf eine Sicherung von

- jedem der letzten vier Werktage (Sohn-Sicherungen)
- jedem der letzten vier Freitage (Vater-Sicherungen)
- jedem der letzten zwölf Monatsenden (Großvater-Sicherungen)

Optional kann auch noch jedes Jahr ein Band reserviert und ausgelagert werden.

Inkrementelle Sicherung

Bei der inkrementellen Sicherung werden immer nur die Dateien gespeichert, die seit der letzten inkrementellen Sicherung, oder beim ersten Mal seit der letzten Komplettsicherung, geändert wurden oder neu hinzugekommen sind. Es wird also immer auf der letzten inkrementellen Sicherung aufgesetzt. Dieses Verfahren hat den Nachteil, dass bei einer Wiederherstellung die Daten in der Regel aus mehreren Sicherungen wieder zusammengesucht werden müssen. (sichert alle Dateien, die über ein gesetztes Archivbit verfügen und setzte dieses anschließend zurück).

Vollständige Sicherung

Bei der Vollsicherung werden die zu sichernden Daten vollständig auf das Sicherungsmedium übertragen und als gesichert im Dateisystem markiert (Archivbit wird zurückgesetzt).

Eine differenzielle oder inkrementelle Datensicherung sollte aufgrund der gleichen Auswahlliste wie die vollständige Datensicherung operieren.