Datensicherheit Grundlagen

1. Einleitung Datensicherung 3
1.1. Gefahren für Daten 3
1.2. Welche Daten sichert man 3
1.3. Begriffe 3
1.3.1. Hot Backup 3
1.3.2. Cold Backup 4
1.3.3. Volume Shadow Copy Service (VSS) 4
1.3.4. On-Site-Backup 4
1.3.5. Off-Site-Backup 4
1.4. Arten der Sicherungen 5
1.4.1. Vollsicherung 5
1.5. Differenzielle Datensicherung 5
1.6. Inkrementelle Datensicherung 5
1.7. Gesetzliche Verpflichtung 6
1.8. Datensicherungsstrategien 7
1.8.1. First in, first out (FIFO) 7
1.8.2. Generationen Prinzip 7
1.8.3. Die Türme von Hanoi 8
1.9 Medientypen der Datensicherung 9
1.8.4. Festplatten 9
1.8.5. Optische Medien 9
1.8.6. Wechselmedien Magnetbänder 9
1.8.7. Cloud Backup 10
1.8.8. Papier Ausdruck 10
1.9. Kosten für Datenverlust 10
1.9.1. Reproduzierbare Daten: 10

1.9.2. Nicht reproduzierbare Daten 11
2. Quellen 11

1. Einleitung Datensicherung

Datensicherung bedeutet, dass Daten für den Fall, dass die Datensicherheit gescheitert ist an einem Ort gespeichert sind, wo sie nicht beschädigt werden könnten. Diese gesicherten Daten können dann wieder in das vorhandene System eingespielt werden, in der Hoffnung, dass keine oder nur wenige Informationen verloren gegangen sind.
Egal, ob es sich um sensible Daten wie Forschungsergebnisse, Patienten-Daten, Kundeninformationen, Produktionsdaten oder um Medien wie Bilder, Videos oder Protokolle handelt, es ist ein Verlust mit möglichen Folgen. All diese Daten haben einen Wert, sei es ein realer bei Forschungsergebnissen oder ein ideeller bei Bildern oder Videos. Um diese Werte zu schützen ist es sinnvoll, für den Ernstfall vorzusorgen.

1.1. Gefahren für Daten

Nachstehend sind einige Gefahrenquellen für Daten angeführt:

- Hardware defekt → defekte Festplatte
- Software Problem → Schadsoftware, Fehler in der Software
- Diebstahl
- Feuer
- Naturkatastrophen

1.2. Welche Daten sichert man

Neben den Benutzerdaten werden auch Computersysteme wie Server (physisch oder virtuell) gesichert.
Die Daten, welche von Benutzern produziert werden, unterliegen einem ständigen Wandel. Diese sollen so oft wie möglich gesichert werden. Viele dieser Daten sind einmalig und bei einem Verlust nicht reproduzierbar (Bilder, Videos, usw.).

1.3. Begriffe

In diesem Abschnitt werden einige Begriffe aus der Datensicherung erläutert

1.3.1. Hot Backup

Der Begriff Hot Backup (Online- oder Live Backup) bedeutet, dass die Daten bei laufendem Betrieb gesichert werden können. Diese Art der Sicherung ist besonders geeignet für Systeme, auf denen viele Benutzerzugriffe erfolgen z.B. Datenbanken. Diese Systeme können während der Geschäftszeit nicht einfach abgeschaltet werden. Die Gefahr dabei ist aber, dass sich während des

Sicherungsvorgangs Daten ändern, wodurch es beim Wiederherstellen zu Inkonsistenzen kommen kann. Diese können dann wiederum zum Totalverlust der Informationen führen.

1.3.2. Cold Backup

Bei einem Cold Backup (Offline- oder zeitverzögerten Backup) wird das System für den Zeitraum der Sicherung eingefroren, so dass keine Änderungen an den Daten während des Backups gemacht werden.
Um trotzdem den Datenverlust klein zu halten, wird oft eine Mischung von Cold und Hot Backup verwendet, indem ein System gespiegelt (zwei oder mehr synchrone Speicher) und von Zeit zu Zeit die Synchronisierung angehalten wird. Ab diesem Zeitpunkt läuft eines der beiden Systeme aktiv weiter und das zweite wird via Cold Backup gesichert. Sobald die Sicherung abgeschlossen ist, wird das zweite System mittels eines Journals wieder mit dem ersten System synchronisiert (bis zur nächsten Sicherung). So kann je nach Sicherungsstrategie zu jedem gespeicherten Sicherungspunkt zurückgesprungen werden.

1.3.3. Volume Shadow Copy Service (VSS)

Dieses Verfahren ist seit Windows XP und ab dem Server 2003 verfügbar und erstellt sogenannte „Snapshots“. Diese ermöglichen es, dass das System nach einem System Fehler z.B. einem fehlerhaften Update wieder auf den ursprünglichen Zustand vor dem Update zurückgesetzt wird. VSS benötigt dafür natürlich einen Teil des Speicherplatzes.

1.3.4. On-Site-Backup

Bei dieser Art der Datensicherung ist der Ort der Datenhaltung und der der Sicherung identisch, was zwar die Geschwindigkeit der Datensicherung verbessert, jedoch die Gefahr erhöht, dass Daten und Sicherungen verloren gehen (Brand, Diebstahl, ...).

1.3.5. Off-Site-Backup

Hier ist der Ort der Datenhaltung und der Datensicherung getrennt. Zum Übertragen der Sicherungen werden schnelle Netzwerkverbindungen benötigt. Die Trennung der Datenhaltung erhöht die Sicherheit des Datenbestands.
In der Praxis wird eine Mischung der beiden Varianten durchgeführt, indem die Datensicherung an sich zwar On-Site erstellt wird, jedoch die Sicherung danach an einem anderen Ort gebracht wird. Z.B. es wird jeden Tag eine Sicherung gemacht, die der Chef dann am Abend mit nach Hause nimmt. Oder es wird zuerst eine ON-Side Sicherung erstellt, was sehr schnell geht und dann werden die Daten über eine Datenverbindung auf einen externen Speicher kopiert.

1.4. Arten der Sicherungen

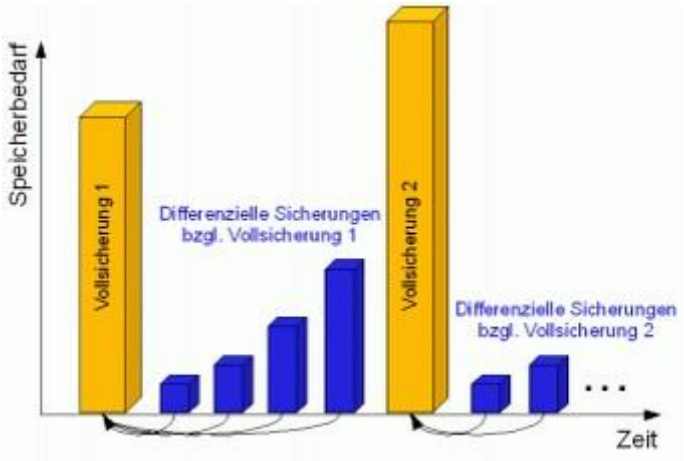
Grundsätzlich unterscheidet man zwischen zwei Arten der Datensicherung. Zum einen können alle Daten, die sich auf der Festplatte oder auf einem Netzlaufwerk befinden, komplett gesichert werden (vollständige Datensicherung oder Vollsicherung), zum anderen werden nur die Daten gesichert, die sich seit der letzten Vollsicherung geändert haben.

1.4.1. Vollsicherung

Bei einer Vollsicherung werden alle Daten des Systems gesichert. Das bedeutet aber nicht, dass bei einer Vollsicherung von einem Dateiserver auch das Betriebssystem mit gesichert werden muss. Hier kann durchaus eine eigene Sicherung vom Server mit den Einstellungen erstellt werden.

1.5. Differenzielle Datensicherung

Beziehen sich nachfolgende Backups (Sicherungen) immer auf die letzte Volldatensicherung, so nennt man dies „Differentielle Datensicherung“. Hierbei werden jedes Mal sämtliche Veränderungen seit der letzten Volldatensicherung erfasst.

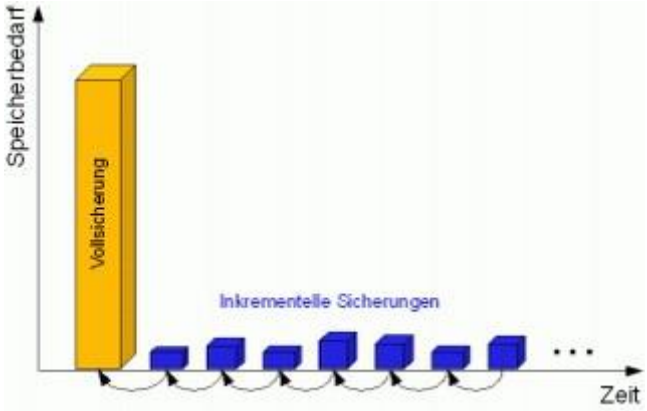


Bei der differenziellen Datensicherung benötigt man zum Wiederherstellen das entsprechende Vollbackup und das Differenzbackup für den entsprechenden Zeitpunkt. In der Abbildung wird jeden Sonntag ein Vollbackup und an Wochentagen ein Differenzbackup durchgeführt. Wenn die differenzielle Sicherung defekt ist, kann der Datenbestand für diesen Tag nicht mehr hergestellt werden. Bei einer defekten Vollsicherung ist der Verlust größer, weil die einzelnen Teilsicherungen nicht verwendet werden können.

1.6. Inkrementelle Datensicherung

Bei der inkrementellen Datensicherung werden immer nur diejenigen Daten gesichert, die sich seit dem Zeitpunkt der letzten Sicherung (Volldatensicherung oder letztes Inkrement) verändert haben. Da bei der inkrementellen Sicherung die Daten immer nur einmal gesichert werden, verringert sich der Speicherbedarf gegenüber der differenziellen Sicherung und der Vollsicherung.

Durch die Anzahl der Sicherungen steigt die Komplexität des Wiederherstellungsvorgangs im Vergleich zur differenziellen Sicherung, da zuerst die Vollsicherung und dann alle inkrementellen Sicherungen in der richtigen Reihenfolge eingespielt werden müssen. Genau diese erhöhte Komplexität ist auch die größte Gefahr, weil wenn ein Inkrement der Sicherung beschädigt alle folgenden Sicherungen nicht mehr verwendet werden können. Z.B. Wenn sie am Fr die Daten wiederherstellen möchten, brauchen sie die Vollsicherung vom So, das Inkrement von Mo, Di , Mi und Do. Ist jetzt das Inkrement von Mo beschädigt, verlieren Sie möglicherweise die Daten von einer kompletten Woche.



Da Sicherungssysteme immer ganze Dateien sichern und nicht nur die Änderungen aus einer Datei, ist dieses Verfahren auch nicht für große Dateien geeignet.
Wenn sie z.B. einen Film schneiden und jeden Tag eine geränderte Version abspeichern - also nur 1 Datei ändern - müsste immer wieder die ganze Datei gesichert werden. Daher hätte hier dieses Verfahren keinen Vorteil.

1.7. Gesetzliche Verpflichtung

Es gibt keine gesetzliche Regelung wie lange Backups in der IT aufbewahrt werden müssen. Es gibt aber gesetzliche Regelung wie lange Buchhaltungsdaten, Patientendaten oder Schülerdaten aufgehoben werden müssen. Hier liegt die Verantwortung für die ordnungsgemäße Aufbewahrung immer bei der Geschäftsführung, auch wenn diese die Aufgabe an Mitarbeiter delegiert werden.
Hier ein kleiner Auszug der Behaltefristen. Die ganze Liste finden sie bei der WKO:

- Steuerrechtliche Unterlagen 7 Jahre, ausgenommen die Behörde hat die Frist verlängert.
- Grundstücke 22 Jahre
- Gewährleistung 2 Jahre
- Daten zu Lohnsteuer und Abgabenpflicht 7 Jahre
- Daten zur Ausstellung eines Dienstzeugnisses 30 Jahre
- Ärztliche Aufzeichnungen 10 Jahre
- Krankengeschichte 30 Jahre, jedoch Röntgenbilder und Videos nur 10 Jahre
- Fahrtenbücher 2 Jahre

- Schulunterlagen
  - Schülerstammblätter 60 Jahre nach letztem Eintrag
  - Klassenbuch 3 Jahre
  - Schularbeiten 1 Jahr

1.8. Datensicherungsstrategien

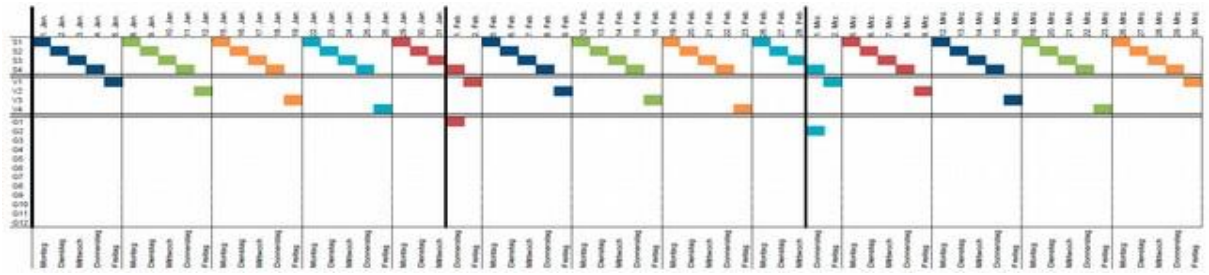
Um sicherzustellen, dass man möglichst jeden Datenzustand zu einem beliebigen Zeitpunkt wieder herstellen kann, gibt es unterschiedliche Strategien wie die Daten gespeichert werden. Denn oft ist es wichtig, einen Datenzustand wiederherzustellen. der nicht der letzte war, sondern einen früheren Zeitpunkt widerspiegelt.

1.8.1. First in, first out (FIFO)

Bei der FIFO Strategie speichert man eine frei gewählte Anzahl von Sicherungen. Wenn Sie also immer 10 Sicherungen haben möchten, wird nach dem Erstellen der 11 Sicherungen die älteste gelöscht. Der Vorteil bei dieser Art ist, dass der Speicherbedarf sehr gut berechnet werden kann. Es muss jedoch immer noch etwas mehr als 10 % Speicher frei sein, damit Sie zuerst die 11. Sicherung machen können und erst dann die älteste Sicherung löschen. Sie haben aber keine Möglichkeiten, frühere Zeitpunkte wieder herzustellen.

1.8.2. Generationen Prinzip

Die Generationen Strategie oder auch Großvater-Vater-Sohn Strategie genannt, funktioniert nach einem einfachen Muster. Wenn Sie jeden Tag eine Sicherung speichern, handelt es sich hier um den Sohn. Einmal pro Woche wird dann eine Sohn-Sicherung zum Vater und einmal im Monat eine Vater-Sicherung zum Großvater. Die Sohn Sicherungen werden dann immer nach einem Monat (5 Wochen) überschrieben (FIFO). Die Vater Sicherungen werden alle drei Monate (1 Quartal) überschrieben und die Großvater Sicherungen alle 12 Monate (1 Jahr).



Damit sind Sie in der Lage, den Datenzustand von jedem Tag des letzten Monats, jeder Woche (meist Sonntag) der letzten drei Monate und jedem Monatsende des letzten Jahres wieder herzustellen.

1.8.3.Die Türme von Hanoi

Diese Strategie basiert auf dem Spiel „Türme von Hanoi“. Damit kann man anhand einer relativ geringen Anzahl von Speichermedien eine relativ lange Zeitspanne von Datensicherungen gewährleisten.
Die Zeitspanne in Tagen, die mit einer Anzahl von n Speichermedien überbrückt werden kann, wird folgendermaßen berechnet: Tage = 2^{n-1} Nach der Zeitspanne wird auch das letzte Speichermedium wieder überschrieben. Es ist aber nicht immer möglich, jeden beliebigen Tag wieder herzustellen.

Drei Medien → Tage = $2^{3-1} = 4$

	Tage des Zyklus							
	1	2	3	4	5	6	7	8
Medium	A		A		**A**		A	
		B				**B**		
				C				C

Das bedeutet, dass sie am Tag 7 folgende Tagessicherungen **(Grün)** C Tag 4, A Tag 5 und B Tag 6 wiederherstellen können.

Vier Medien → Tage = $2^{4-1} = 8$

	Tage des Zyklus															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Medien	A		A		A		A		A		A		**A**		A	
		B				B				**B**				B		
				C								**C**				
								D								D

Das bedeutet, dass sie am Tag 14 folgende Tagessicherungen **(Grün)** A Tag 13, C Tag 12, B Tag 10 und D Tag 8 wiederherstellen können.

1.9 Medientypen der Datensicherung

Nachstehend werden Faktoren, die die Auswahl des richtigen Mediums beeinflussen angeführt:

- Digital oder analog
- Menge der Daten
- Art der Daten (Datenbank oder Einzeldokumente oder Filme)
- Zugriff auf Sicherung (Häufigkeit, Aufwand)
- Dauer der Sicherung (kurz oder lang)
- Technische Voraussetzung (können Daten noch gelesen werden)
- Geschwindigkeit der Sicherung (Wie lange dauert sichern und wiederherstellen)
- Wert der Daten (reproduzierbar oder nicht)
- Gesetzliche Voraussetzungen
- Sicherheit (Lagerung und Verschlüsselung)

1.8.4.Festplatten

Viele Datensicherungen werden heutzutage auf Festplatten gespeichert. Hierbei muss aber sichergestellt werden, dass Daten auch nach dem Archivieren der Platten noch gelesen werden können.
Die Vorteile sind die Geschwindigkeit, die Speicherkapazität und der Preis.
Die Nachteile sind, dass sich die Interfaces schnell ändern und die eher geringe Lebenserwartung von 5 -10 Jahren nicht zum Archivieren eignet.

1.8.5.Optische Medien

CD, DVD oder Blue Ray sind optische Speichermedien und werden nicht mehr so häufig für Sicherungen verwendet.
Vorteile sind der geringe Preis, dass die Daten oft nicht mehr veränderbar sind und die einfache Lagerung.
Die Nachteile sind, dass sich die Speichertechnologie oft ändert und die Lebenserwartung sehr unterschiedlich ist (5 bis vermutlich 100 Jahre) sowie die Speichermenge sehr begrenzt ist.

1.8.6.Wechselmedien Magnetbänder

Bandspeicher Systeme sind in der IT schon seit vielen Jahren bekannt und erprobt. Die Speicherkapazität beträgt derzeit bis zu 192 TB je Band mit einer Schreibrate von rund 280 MB/s.
Die Vorteile sind die Langlebigkeit und der Preis.
Der Nachteil ist die langsame Geschwindigkeit beim Wiederherstellen der Daten.

1.8.7. Cloud Backup

Cloudspeicher werden oft als Ergänzung verwendet. Es handelt sich hier weniger um ein eigenes Medium, sondern eher um eine Art der Vermarktung einer Dienstleistung. Bekannte Anbieter sind Microsoft, Amazon oder Google sowie regionale wie World4you oder Conova.
Für Unternehmen ist dabei zu beachten, welche Datenschutzbestimmungen eingehalten werden. Bei US-Anbieter arbeiten oft nach dem amerikanischen Recht und sind nicht mit geltenden europäischen Gesetzen kompatibel.
Die Vorteile sind die scheinbar unerschöpfliche Kapazität und die vermutliche Datensicherheit (nicht Datenschutz).
Die Nachteile sind der eher hohe Preis, die meist langsame Datenverbindung und der Datenschutz. Da es sich zudem um ein Mietmodel handelt, ist bei Nichtbezahlung die Datensicherheit auch nicht mehr gegeben.

1.8.8. Papier Ausdruck

Auch wenn schon seit vielen Jahren vom papierlosen Büro gesprochen wird, ist dieses immer noch nicht der Fall. Gerade Daten, die sehr lange gelagert werden müssen, werden auch heute noch auf Papier gedruckt, da selbst industriell hergestelltes (säurehaltiges) Papier eine Lebenserwartung von rund 70 Jahren hat. Alte Dokumente sind mehrere hundert Jahre haltbar.
Vorteil: sehr einfach in der Handhabung, keine technischen Hilfsmittel und lange Lebenserwartung.
Nachteil: großer Lagerbedarf, analoge Speicherung und langsame Schreib- Lesegeschwindigkeit.

1.9. Kosten für Datenverlust

Die Kosten für einen Datenverlust können enorm sein und es ist für jedem Unternehmer wichtig, diese zu kennen um das richtige Sicherungssystem auszuwählen.
Die Kosten hängen von der Art der Daten, (reproduzierbar sind oder nicht) ab.

1.9.1. Reproduzierbare Daten:

Anzahl der betroffenen Mitarbeiter mal Nutzungszeit pro Tag mal Kosten pro Mitarbeiter pro Tag mal die Tage plus die IT-Kosten für die Wiederherstellung eines funktionieren Ausgangspunkts ergibt den finanziellen Schaden. Hierbei sind andere Schäden wie Imageverlust, Kundenverlust oder eventuelle Strafen nicht berücksichtigt.
Bei 10 Mitarbeitern (Monatsgehalt € 1.500,- netto) in Vollzeit bei einem Datenverlust von 2 Tagen und Wiederherstellungskosten eines Ausgangspunkts von 10 Stunden einer IT Firma bedeutet das: € 1.500,- netto für den Mitarbeiter bedeuten für den Arbeitgeber rund € 3.200,- Personalkosten pro Monat (14 Gehälter + Arbeitgeberanteil). Bei rund 20 Arbeitstagen bedeutet das, dass jeder Tag den

Arbeitgeber rund € 160,- kostet. Vollzeit bedeutet 100% das entspricht dem Faktor 1 während Halbtags 50% entspricht 0,5.

Alles zusammen kostet dann:

10 x € 160,- x 1 (100%) x 2 Tage	+ 10 h x € 150,-	=
€ 3.200,-	+ € 1.500,-	= € 4.700,-

Wenn also nur rund 1 % der Daten in einem Jahr verloren gehen, wäre der direkte Schaden bereits rund € 4.700,-.

1.9.2. Nicht reproduzierbare Daten

Sie haben den Auftrag ein Event zu filmen und Fotos zu erstellen. Bei Verlust wird der Auftrag nicht bezahlt, also 100% Verlust!

2. Quellen

- die Grafiken stammen aus Wikipedia
- e-Teaching Homepage
- Moderne Betriebssystem
- Wikipedia
- IT Wissen Homepage
- Thomas Krenn Homepage
- WKO
- RIS