



## **Modul 143: Backup- und Restore-Systeme implementieren**

---

Grundlagen zur Datensicherung mit Beispielen,  
Repetitionsfragen und Antworten

---

Thomas Grosser und Johannes Scheuring

---



Modul 143: Backup- und Restore-Systeme implementieren

Grundlagen zur Datensicherung mit Beispielen, Repetitionsfragen und Antworten

Thomas Grosser und Johannes Scheuring

Grafisches Konzept: dezember und juli, Wernetshausen

Satz und Layout: Mediengestaltung, Compendio Bildungsmedien AG, Zürich

Illustrationen: Oliver Lüde, Winterthur

Druck: Edubook AG, Merenschwand

Redaktion und didaktische Bearbeitung: Johannes Scheuring

Artikelnummer: 12699

ISBN: 978-3-7155-7038-9

Auflage: 3., überarbeitete Auflage 2014

Ausgabe: U1114

Sprache: DE

Code: ICTW 047

Alle Rechte, insbesondere die Übersetzung in fremde Sprachen, vorbehalten. Der Inhalt des vorliegenden Buchs ist nach dem Urheberrechtsgesetz eine geistige Schöpfung und damit geschützt.

Die Nutzung des Inhalts für den Unterricht ist nach Gesetz an strenge Regeln gebunden. Aus veröffentlichten Lehrmitteln dürfen bloss Ausschnitte, nicht aber ganze Kapitel oder gar das ganze Buch fotokopiert, digital gespeichert in internen Netzwerken der Schule für den Unterricht in der Klasse als Information und Dokumentation verwendet werden. Die Weitergabe von Ausschnitten an Dritte ausserhalb dieses Kreises ist untersagt, verletzt Rechte der Urheber und Urheberinnen sowie des Verlags und wird geahndet.

Die ganze oder teilweise Weitergabe des Werks ausserhalb des Unterrichts in fotokopierter, digital gespeicherter oder anderer Form ohne schriftliche Einwilligung von Compendio Bildungsmedien AG ist untersagt.

Copyright © 2006, Compendio Bildungsmedien AG, Zürich

Dieses Buch ist klimaneutral in der Schweiz gedruckt worden. Die Druckerei Edubook AG hat sich einer Klimaprüfung unterzogen, die primär die Vermeidung und Reduzierung des CO<sub>2</sub>-Ausstosses verfolgt. Verbleibende Emissionen kompensiert das Unternehmen durch den Erwerb von CO<sub>2</sub>-Zertifikaten eines Schweizer Klimaschutzprojekts.

Mehr zum Umweltbekenntnis von Compendio Bildungsmedien finden Sie unter: [www.compendio.ch/Umwelt](http://www.compendio.ch/Umwelt)

# Inhaltsverzeichnis

---

<b>Vorwort</b>	<b>6</b>
<b>Über dieses Lehrmittel</b>	<b>8</b>
<b>Teil A Grundlagen der Datensicherung</b>	<b>11</b>
<b>Einleitung, Lernziele und Schlüsselbegriffe</b>	<b>12</b>
<b>1 Warum müssen Daten gesichert werden?</b>	<b>13</b>
1.1 Wert der Unternehmensdaten	13
1.2 Bedrohungen der Unternehmensdaten	13
1.3 Massnahmen zur Datensicherheit	14
1.4 Preloss oder Postloss	16
1.5 Betriebliche Rahmenbedingungen	17
1.6 Gesetzliche Vorschriften	17
<b>Repetitionsfragen</b>	<b>19</b>
<b>2 Was bedeutet Datensicherung?</b>	<b>20</b>
2.1 Welche Daten werden gesichert?	20
2.2 Was bedeuten «Backup» und «Restore»?	21
2.3 Backup ist nicht Archivierung	22
<b>Repetitionsfragen</b>	<b>23</b>
<b>3 Wo werden Daten gesichert?</b>	<b>24</b>
3.1 Magnetische Speichermedien	24
3.2 Optische Speichermedien	28
3.3 Übrige Speichermedien	29
<b>Repetitionsfragen</b>	<b>31</b>
<b>4 Welches Speichermedium wähle ich?</b>	<b>32</b>
4.1 Datenmenge	32
4.2 Speicherdauer	33
4.3 Wiederherstellungsdauer	33
4.4 Kosten	34
4.5 Technikwechsel	34
4.6 Haltbarkeit	35
4.7 Erweiterbarkeit	35
<b>Repetitionsfragen</b>	<b>36</b>
<b>Teil B Technologien und Organisation der Datensicherung</b>	<b>37</b>
<b>Einleitung, Lernziele und Schlüsselbegriffe</b>	<b>38</b>
<b>5 Arten der Datensicherung</b>	<b>39</b>
5.1 Einzelplatz-Backup	39
5.2 Automatischer Backup	39
5.3 LAN-Backup	40
5.4 Storage Area Network (SAN)	41
5.5 Online-Datensicherung	41
5.6 Backup als Cloud-Service	42
<b>Repetitionsfragen</b>	<b>42</b>
<b>6 Grosse Datenmengen sichern</b>	<b>43</b>
6.1 Voll-Backup ausführen	43
6.2 Differenzielle Datensicherung ausführen	43
6.3 Inkrementelle Datensicherung ausführen	44
<b>Repetitionsfragen</b>	<b>45</b>

<b>7</b>	<b>Wechselschema anwenden</b>	<b>46</b>
7.1	Wechselschema «Grossvater-Vater-Sohn»	46
7.2	Wechselschema «Turm von Hanoi»	47
	<b>Repetitionsfragen</b>	<b>49</b>
<b>8</b>	<b>Daten während des Systembetriebs sichern</b>	<b>50</b>
8.1	RAID einsetzen	50
8.2	USV einsetzen	52
	<b>Repetitionsfragen</b>	<b>53</b>
<b>Teil C</b>	<b>Datensicherungskonzept erstellen</b>	<b>55</b>
	<b>Einleitung, Lernziele und Schlüsselbegriffe</b>	<b>56</b>
<b>9</b>	<b>Zu sichernde Daten bestimmen</b>	<b>58</b>
9.1	Datenerhebung	58
9.2	Umgang mit streng vertraulichen Daten	60
9.3	Hilfsmittel	60
9.4	Reihenfolge der Wiederherstellung	60
	<b>Repetitionsfragen</b>	<b>61</b>
<b>10</b>	<b>Sicherungsmodalitäten festlegen</b>	<b>62</b>
10.1	Zeitpunkt des Backups bestimmen	62
10.2	Periodizität des Backups bestimmen	62
10.3	Art und Anzahl der Backups bestimmen	63
	<b>Repetitionsfragen</b>	<b>63</b>
<b>11</b>	<b>Speichermedien bestimmen</b>	<b>64</b>
11.1	Technische Aspekte beachten	64
11.2	Betriebswirtschaftliche Aspekte beachten	64
11.3	Ablauf eines mehrstufigen Backups	65
	<b>Repetitionsfragen</b>	<b>67</b>
<b>12</b>	<b>Sicherungssoftware bestimmen</b>	<b>68</b>
12.1	Datensicherung unter Windows-Systemen	68
12.2	Standard Unix-Tools	69
12.3	Kommerzielle Sicherungsprogramme	70
	<b>Repetitionsfragen</b>	<b>71</b>
<b>13</b>	<b>Aufbewahrung der Datenträger bestimmen</b>	<b>72</b>
13.1	Datenschutzaspekte beachten	72
13.2	Datenträger korrekt beschriften	73
13.3	Datenträger korrekt lagern	74
	<b>Repetitionsfragen</b>	<b>75</b>
<b>14</b>	<b>Verantwortung für das Backup und Restore festlegen</b>	<b>76</b>
14.1	Rollen und Verantwortungsbereiche	76
14.2	Benutzer schulen	77
	<b>Repetitionsfragen</b>	<b>77</b>

<b>Teil D</b>	<b>Backup- und Restore-System sicher betreiben</b>	<b>79</b>
	<b>Einleitung, Lernziele und Schlüsselbegriffe</b>	<b>80</b>
<b>15</b>	<b>Notfallmassnahmen planen</b>	<b>81</b>
15.1	Notfallhandbuch erstellen	81
15.2	Sofortmassnahmen	82
15.3	Regelungen für den Notfall	84
15.4	Wiederanlaufpläne für kritische Komponenten	85
15.5	Dokumentation	86
15.6	Beispiel eines Notfallhandbuchs	87
	<b>Repetitionsfragen</b>	<b>88</b>
<b>16</b>	<b>Backup- und Restore-System testen</b>	<b>89</b>
16.1	Tests planen und vorbereiten	89
16.2	Tests durchführen und dokumentieren	90
	<b>Repetitionsfragen</b>	<b>91</b>
<b>Teil E</b>	<b>Anhang</b>	<b>93</b>
	<b>Gesamtzusammenfassung</b>	<b>94</b>
	<b>Antworten zu den Repetitionsfragen</b>	<b>101</b>
	<b>Glossar</b>	<b>105</b>
	<b>Stichwortverzeichnis</b>	<b>110</b>

## Vorwort

---

### Liebe Leserin, lieber Leser

Vorweg schon einmal herzliche Gratulation! Sie haben sich für den Einsatz eines der aktuellsten Lehrmittel der Informatikausbildung entschlossen.

### An wen richtet sich die Lernwelt «Informatik»?

Die Lernwelt «Informatik» ist ausgerichtet auf die gültigen Modulbeschreibungen für die Informatik-Grund- und -Weiterbildung. Mit diesem Grundlagenbuch wenden wir uns deshalb an Auszubildende und Unterrichtende

- einer Informatiklehre,
- der Informatikmittelschulen,
- der höheren Berufsbildung und
- von Ausbildungsgängen und Schulungen in der Erwachsenenbildung.

Dank zahlreicher Beispiele, Grafiken, Abbildungen und Übungen mit kommentierten Lösungen eignet sich die Lernwelt «Informatik» auch für das Selbststudium.

### Wie Sie mit diesem Lehrmittel arbeiten

Dieses Arbeitsbuch bietet Ihnen mehr als nur einen Lerntext. Deshalb weisen unsere Bildungsmedien eine Reihe von Charakteristiken auf, die Ihnen Ihre Arbeit erleichtern:

- Das **Inhaltsverzeichnis** dient Ihnen als Orientierungshilfe und als Lernrepetition. Fragen Sie sich, was Sie von jedem Kapitel erwarten, und überprüfen Sie anschliessend an das Bearbeiten des Lerntexts, was Sie jetzt zu den einzelnen Teilen wissen.
- Wissen Sie gerne im Voraus, wofür Sie Ihre kostbare Zeit einsetzen? Kein Problem, lesen Sie die **Lernziele** vor der Lektüre des entsprechenden Teils. An gleicher Stelle finden Sie auch eine Auflistung der **Schlüsselbegriffe**.
- Die einzelnen Lerneinheiten werden durch eine **Zusammenfassung** abgeschlossen. Sie greift die wichtigsten Punkte des vorangegangenen Texts nochmals auf und stellt sie in den richtigen Zusammenhang.
- Nach dem Durcharbeiten der einzelnen Lerneinheiten können Sie anhand der **Repetitionsfragen** überprüfen, ob Sie das Gelernte verstanden haben. Die **Lösungen** zu diesen Repetitionsfragen finden Sie im Anhang des Buchs. Bitte beachten Sie, dass die Übungen nicht fortlaufend nummeriert sind; die Nummern dienen lediglich zum Auffinden der Lösung.
- Nutzen Sie das **Glossar**; schlagen Sie dort nach, wenn Sie einen Begriff nicht verstehen.
- Das **Stichwortverzeichnis** beschliesst das Lehrmittel. Sie können es benutzen, wenn Sie einzelne Abschnitte zu bestimmten Schlagwörtern nachlesen wollen.

### Wer steht hinter der Lernwelt «Informatik»?

Die erfahrenen Lehrmittelentwickler von Compendio Bildungsmedien haben die Lernwelt «Informatik» zusammen mit ausgewiesenen Fachleuten und Kennern der Informatikausbildung konzipiert und realisiert.

Dank gebührt allen, die trotz grossem Zeitdruck mit Rat und Tat am Konzept und an der Ausarbeitung mitgewirkt haben. Ganz speziell möchten wir uns bedanken bei Gabriel Weber, der für das Fachlektorat verantwortlich war.

### **In eigener Sache**

Haben Sie Fragen oder Anregungen zu diesem Lehrmittel? Sind Ihnen Fehler aufgefallen?  
Über unsere E-Mail-Adresse [postfach@compendio.ch](mailto:postfach@compendio.ch) können Sie uns diese gerne mitteilen.

Wir wünschen Ihnen mit diesem Lehrmittel viel Spass und Erfolg.

Zürich, im Dezember 2014

Thomas Grosser, Autor

Markus Kammermann, Fachlektor

Johannes Scheuring, Redaktor

### **Anmerkung zur 3. Auflage 2014**

Änderungen gegenüber der 2. Auflage beruhen auf der aktualisierten Modulidentifikation  
der ICT-Berufsbildung (Stand 14.01.2014, ICT-Modulbaukasten, Release 6).

## Über dieses Lehrmittel

### Inhalt und Aufbau dieses Lehrmittels

Sicherlich besitzen Sie einen Computer mit einem Internetanschluss. Wahrscheinlich schützen Sie Ihren Computer während des Surfens mittels einer Firewall oder zumindest mit einer Antivirensoftware. Damit ist mein Computer ausreichend geschützt, werden Sie wohl denken. Haben Sie sich schon Gedanken darüber gemacht, dass Sie oder eventuell jemand anderes aus Versehen Daten auf Ihrem Computer löschen könnte oder Ihre Hard-disk aus technischen Gründen nicht mehr funktionieren könnte? Stellen Sie sich vor, dass alle Ihre digitalen Fotos, alle Ihre Briefe, Mails und persönlichen Unterlagen, die Sie über eine längere Zeit erarbeitet haben, unwiderruflich zerstört sind. Um dies zu umgehen, können Sie Ihre kompletten Daten von Zeit zu Zeit auf einem Medium wie z. B. einer CD-ROM speichern.

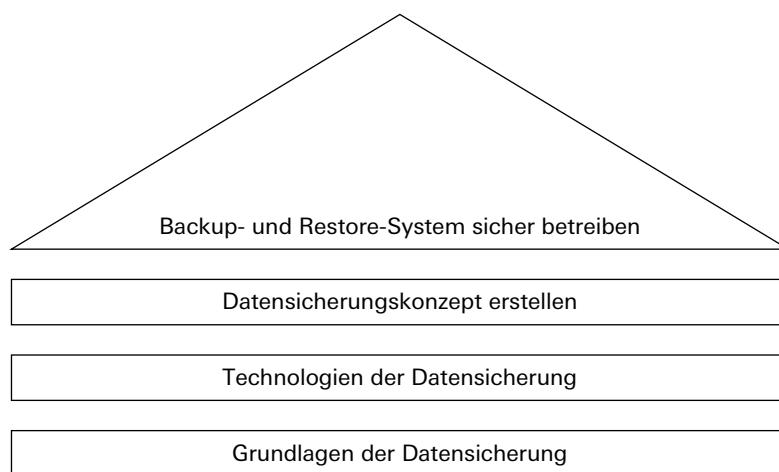
Unternehmen haben es aufgrund von sehr grossen Datenmengen nicht so einfach. Gehen Daten verloren, können ernsthafte Verluste entstehen. Gesetzliche Vorschriften, betriebliche Rahmenbedingungen und technische Aspekte müssen beachtet werden, um ein effizientes Backup- und Restore-Konzept aufzubauen. Dieses Lehrmittel vermittelt Ihnen die Kompetenz, für ein Unternehmen ein komplettes Backup- und Restore-System zu implementieren. Es ist wie folgt aufgebaut:

- Im **Teil A** beinhaltet die Grundlagen der Backup- und Restore-Systeme. Sie erfahren, wozu Daten geschützt werden müssen, und lernen die Begrifflichkeiten rund um die Thematik Datensicherung kennen. Zusätzlich erfahren Sie mehr über die unterschiedlichen Speichermedien sowie deren Einsatzmöglichkeiten.
- Im **Teil B** erfahren Sie mehr über die unterschiedlichen Datensicherungstechnologien. Sie lernen die unterschiedlichen Backup-Arten kennen und erfahren, wie grosse Datenmengen effizient gespeichert werden können.
- Im **Teil C** erklärt die Erstellung eines Datensicherungskonzepts. Sie lernen die unterschiedlichen Inhalte kennen, die beim Backup- und Restore-Konzept beachtet werden müssen.
- Im **Teil D** binden Sie Ihr Backup- und Restore-Konzept in den Betrieb ein. Sie erfahren, wie Ihr Konzept dokumentiert, getestet und integriert wird.
- Im **Anhang** finden Sie eine Gesamtzusammenfassung, die Antworten zu den Repetitionsfragen, ein Glossar zum Nachschlagen sowie das Stichwortverzeichnis.

Folgende Grafik fasst die Gliederung des Lehrmittels zusammen:

[0-1] Aufbau des Lehrmittels

---



**Dieses Lehrmittel liefert die Grundlage für den Erwerb folgender Kompetenzen**

---

1. Sie können anhand der Rahmenbedingungen und technischen Vorgaben ein Datensicherheitskonzept erstellen.
2. Sie können ein erstelltes Konzept auf seine Machbarkeit prüfen und ggf. überarbeiten.
3. Sie können Sicherungsprozeduren erstellen und testen sowie in die produktive Ablaufsteuerung integrieren und dokumentieren.
4. Sie können Sicherungs- und Wiederherstellungsprozesse durchführen und austesten.
5. Sie können Betriebs- und Wartungsdokumente nachführen.
6. Sie können Backup- und Restore-Systeme für den produktiven Betrieb freigeben.

**Technische Voraussetzungen**

---

Für eine gewinnbringende Bearbeitung der Thematik sind Grundkenntnisse im Bereich Hardware und Netzwerk notwendig.

## Nützliche Links zum Thema

Thema	Link	Beschreibung
ARCserve	<a href="http://www.arcserve.com/de">http://www.arcserve.com/de</a>	Homepage des Anbieters ARCserve für kommerzielle Sicherungsprogramme.
Arkeia	<a href="http://arkeia.com/de">http://arkeia.com/de</a>	Homepage des kommerziellen Softwareanbieters der Software Arkeia.
BackupExec	<a href="http://www.symantec.com/products/data-backup-software">http://www.symantec.com/products/data-backup-software</a>	Homepage des Anbieters Symantec für die kommerzielle Sicherungssoftware BackupExec.
Datenschutz-Gesetztestexte	<a href="http://www.admin.ch/ch/d/sr/c235_1.html">http://www.admin.ch/ch/d/sr/c235_1.html</a>	Gesetzliche Bestimmungen zum schweizerischen Datenschutz.
Datenschutz-Informationen	<a href="http://www.datenschutz.ch">http://www.datenschutz.ch</a>	Informationsseite zum schweizerischen Datenschutz.
Dir-IT	<a href="http://www.freeware.de/download/dir-it_65941.html">http://www.freeware.de/download/dir-it_65941.html</a>	Dir-IT kopiert die Dateinamen von beliebigen Verzeichnissen in jede gewünschte Anwendung.
DirPrinter	<a href="http://dirprinter.giga.de/">http://dirprinter.giga.de/</a>	Mit DirPrinter lassen sich Verzeichnisbäume oder Inhalte von Verzeichnissen erstellen.
IT-Grundschutz für Private	<a href="http://www.bsi-fuer-buerger.de">http://www.bsi-fuer-buerger.de</a>	Informationen über Bedrohungen und Massnahmen im Bereich Datensicherheit für Privatpersonen.
IT-Grundschutz für Unternehmen	<a href="http://www.bsi.de">http://www.bsi.de</a>	Informationen des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) über Bedrohungen und Massnahmen im Bereich der Datensicherheit für Unternehmen.
Speicherlösungen	<a href="http://www.speicherguide.de">http://www.speicherguide.de</a>	Umfangreiche Sammlung von Berichten rund um Backup und Restore.

## Nützliche Literatur zum Thema

Autor	Titel	ISBN / Auflage	Jahr
Cattini, Roland; Kammermann, Markus; Zaugg, Michael	CompTIA Server+	978-3-8266-9174-4	2011
Hagenbuch, Stefan; Weber, Gabriel	Server- und Systemadministration	978-3-7155-94494-1	2010
Kantantzis, Nikolaos; Scheuring, Johannes	Modul 141: Datenbanksysteme in Betrieb nehmen	978-3-7155-94494-1	2014

## **Teil A Grundlagen der Datensicherung**

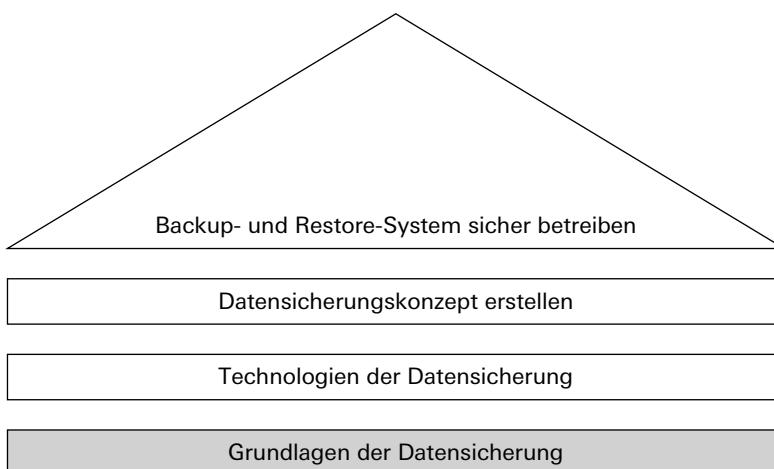
---

## Einleitung, Lernziele und Schlüsselbegriffe

### Einleitung

Unternehmen sehen sich einer wachsenden Zahl von Sicherheitsrisiken und Bedrohungen ausgesetzt. Daten sind ein wertvolles Kapital, das mit gezielten Massnahmen geschützt werden muss. Die Integration von Backup- und Restore-Prozeduren ist Teil des Sicherheitskonzepts eines Unternehmens. Die folgenden Grundlagen zeigen Ihnen auf, wozu Sie Ihre Daten schützen müssen. Sie lernen die Begriffe rund um das Thema Datensicherung kennen. Zusätzlich erfahren Sie, auf welchen Medien Sie Daten speichern können und worauf Sie bei der Auswahl dieser Speichermedien achten müssen. Folgende Grafik zeigt auf, wo Sie sich innerhalb des Lehrmittels befinden:

[0-2] Inhalt von Teil A



### Lernziele und Lernschritte

Lernziele	Lernschritte
<input type="checkbox"/> Sie erkennen den Wert der Daten für ein Unternehmen und wissen, mit welchen Massnahmen diese gegen Bedrohungen zu schützen sind.	Warum müssen Daten gesichert werden?
<input type="checkbox"/> Sie verstehen die verschiedenen Begriffe innerhalb von Backup und Restore.	Datensicherheit und Datensicherung
<input type="checkbox"/> Sie kennen die verschiedenen Speichermedien, auf denen eine Datensicherung möglich ist.	Worauf kann ich speichern?
<input type="checkbox"/> Sie kennen die verschiedenen Aspekte, auf die bei der Auswahl der Speichermedien geachtet werden muss.	Auswahl des Speichermediums

### Schlüsselbegriffe

Archivierung, Backup- und Restore-Konzept, Backup, Bauliche Massnahmen, Datenmenge, Datensicherung, Disaster Recovery, DSG, Höhere Gewalt, Image, Integrität, Kriminelle Handlung, Menschliches Versagen, OR, Organisatorische Massnahmen, Personelle Massnahmen, Postloss, Preloss, Restore, Speicherdauer, Speichermedien, Technische Massnahmen, Technisches Versagen, Verfügbarkeit, Vertraulichkeit, Wiederherstellungsdauer

## 1 Warum müssen Daten gesichert werden?

Und plötzlich ist alles schwarz. Der Computer hat sich verabschiedet, die Daten sind nicht mehr zu retten. Ein Albtraum sowohl in der Geschäftswelt als auch im Privatleben. Der Computer ist rasch ersetzt. Kosten doch die Geräte heutzutage nicht mehr alle Welt. Aber was ist mit den Daten?

### 1.1 Wert der Unternehmensdaten

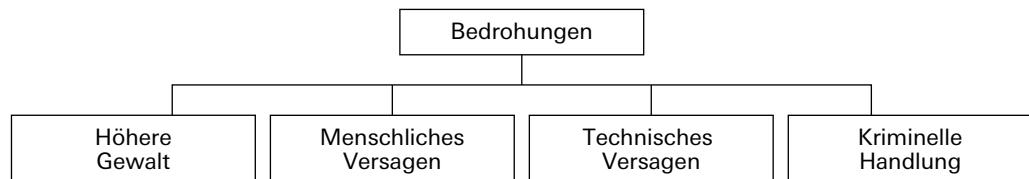
In der Geschäftswelt werden praktisch alle Vorgänge auf dem Computer erfasst, bearbeitet und gespeichert. Schnell sind so grosse Datenmengen vorhanden. Doch wie hoch ist der Wert dieser Daten? Sind noch Dokumente auf Papier vorhanden, können die Informationen nachträglich manuell wieder eingegeben werden. Der Aufwand hierfür kann genau berechnet und ausgewiesen werden. Doch wie berechnen Sie die Kosten für Daten, die Sie nicht mehr rekonstruieren können?

Stellen Sie sich vor, Ihre Hausbank verliert aus Versehen Kontodaten. Ihr Vermögen und das anderer Kunden ist plötzlich nicht mehr auffindbar. Sicherlich würden Sie nicht lange überlegen, Ihr Konto bei dieser Bank aufzulösen (was Sie ja aufgrund der Situation nicht einmal mehr machen müssten). Mit anderen Worten kann die Existenz eines Unternehmens von der sicheren Aufbewahrung und Rekonstruierbarkeit seiner Daten abhängen. Daten können daher unbezahlbar sein.

### 1.2 Bedrohungen der Unternehmensdaten

Die Werte in der ICT unterliegen einer ständigen Bedrohung. Diese Bedrohungen können verschiedene Ursachen haben. Nachfolgend werden die vier wesentlichen Ursachen von Bedrohungen vorgestellt.

#### [1-1] Gefahrenkategorien



#### 1.2.1 Höhere Gewalt

Bei der höheren Gewalt kommt die Bedrohung von aussen. Unternehmen haben auf diese Ereignisse meistens keinen Einfluss. Zu diesen Ereignissen werden nachfolgende Risiken gerechnet:

- Feuer, Explosion im Rechenzentrum oder in dessen Umgebung
- Naturkatastrophen wie Erdbeben, Überschwemmung oder Blitzschlag
- Stromausfall

### 1.2.2 Menschliches Versagen

Die Mehrheit der Zwischenfälle lässt sich auf menschliches Versagen zurückführen. Darunter gehören nachfolgende Risiken:

- Versehentliches Löschen von Daten
- Fehlerhaftes Programmieren
- Verlust der Vertraulichkeit durch herumliegende Daten
- Fehlende Dokumentation

### 1.2.3 Technisches Versagen

Beim technischen Versagen fallen technische Geräte wegen eines Defekts aus. Mögliche Gründe können wie folgt sein:

- Hardwaredefekt
- Softwarefehler
- Defekte an Systemen
- Defekte an Netzwerkkomponenten

### 1.2.4 Kriminelle Handlung

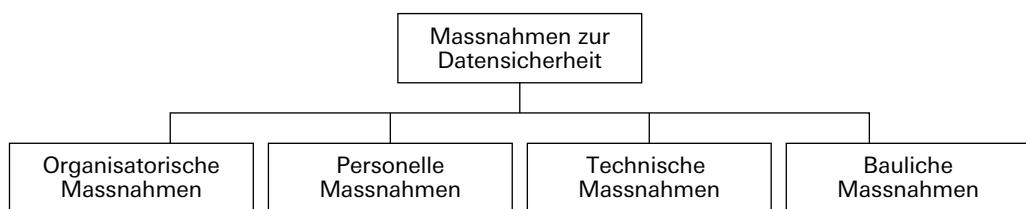
Im Gegensatz zum menschlichen Versagen löschen bzw. zerstören die Menschen Daten nicht unabsichtlich, sondern gewollt. Unter kriminellen Handlungen werden nachfolgende Risiken verstanden:

- Absichtliche Manipulation an Geräten, Programmen oder Daten
- Missbrauch vertraulicher Daten
- Diebstahl oder Kidnapping von Geräten, Programmen oder Daten
- Einbringen von bösartiger Software (Viren)
- Hacking, Industriespionage
- Vandalismus
- Sabotage

## 1.3 Massnahmen zur Datensicherheit

Durch gezielte Risikoanalyse von bestimmten Objekten werden unmittelbare Bedrohungen erkannt und abgeschwächt bzw. eliminiert. Diese Massnahmen lassen sich in organisatorische, personelle, technische und bauliche Massnahmen unterteilen.

#### [1-2] Massnahmenkategorien



### 1.3.1 Organisatorische Massnahmen

---

Bei den organisatorischen Massnahmen wird die Organisation des Unternehmens angepasst. Unter Organisation werden der Aufbau (z. B. das Organigramm) oder die Prozesse verstanden. Es fallen aber auch die Informationen an die Mitarbeitenden, z. B. mittels Weisung oder Schulung, darunter. Mögliche organisatorische Massnahmen sind:

- Dokumentation des Sicherheitskonzepts
- Herausgabe von Verhaltensweisungen
- Optimierung von Sicherheitsabläufen
- Erstellung von Arbeitsbeschreibungen
- Schulung der Anwender bzw. Benutzer

### 1.3.2 Personelle Massnahmen

---

Personelle Massnahmen umfassen Massnahmen, bei denen das Personal, also die Mitarbeitenden, direkt betroffen sind. Mögliche personelle Massnahmen sind:

- Einstellen eines Sicherheitsverantwortlichen
- Zuteilung von Mitarbeitenden in andere Abteilungen bzw. Funktionen
- Entlassung von Mitarbeitenden, z. B. nach krimineller Aktivität

### 1.3.3 Technische Massnahmen

---

Hier wird die Datensicherheit mithilfe technischer Massnahmen im ICT-System sichergestellt. Mögliche technische Massnahmen sind:

- Datensicherung (Backup & Restore)
- Anmeldung durch Passwort
- Verschlüsselung von Daten
- Firewall
- Antivirenprogramme

#### ▷ Hinweis

Wie Sie sehen, ist das Backup & Restore eine technische Massnahme zur Datensicherung. Die Datensicherung wiederum ist ein Teilbereich der Datensicherheit.

### 1.3.4 Bauliche Massnahmen

---

Bei den baulichen Massnahmen wird die Datensicherheit mittels Umbau der Infrastruktur gewährleistet. Mögliche bauliche Massnahmen sind:

- Blitzschutz einbauen
- Feuerschutz installieren
- Einbruchsschutz einbauen
- Alarmanlage installieren

## 1.4 Preloss oder Postloss

Massnahmen dienen einerseits dazu, Bedrohungen vor dem Entstehen bereits zu eliminieren (**Preloss**). Andererseits können Massnahmen auch dazu dienen, im Falle eines Ereignisses die Weiterführung zu gewährleisten (**Postloss**).

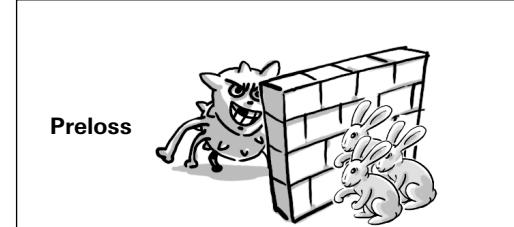
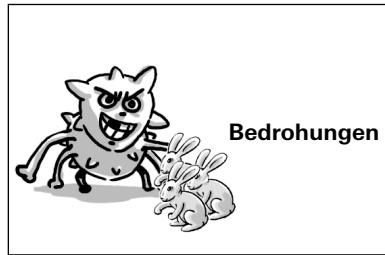
Preloss	Postloss
Dies sind Massnahmen, die die Eintrittswahrscheinlichkeit eines Ereignisses verhindern sollen. Es sind also präventive Massnahmen zur Reduktion der Eintrittswahrscheinlichkeit einer Bedrohung.	Dies sind Massnahmen, die zur Schadensbegrenzung beitragen. Es sind also restriktive Massnahmen zur Begrenzung der Schadengröße.

### Beispiel

Beim Auto wird ein ABS installiert, damit der Fahrer auch in schwierigen Lagen sein Auto steuern kann. Unfälle können so verhindert werden. Das ABS stellt eine Preloss-Massnahme dar. Die Unfallabteilung in einem Spital ist eine Postloss-Institution. Sie versucht, den Schaden zu begrenzen. Damit im Falle eines Unfalls die Kosten gedeckt sind, werden Unfallversicherungen abgeschlossen. Bei der Versicherung handelt es sich um eine finanzielle Postloss-Massnahme. Sie verhindert keinen Schaden, sondern nur die finanziellen Auswirkungen.

Das in diesem Lehrmittel behandelte Thema «Datensicherung» ist eine Massnahme im Bereich Postloss. Eine Datensicherung dient dazu, bereits gelöschte bzw. zerstörte Daten wiederherstellen zu können.

[1-3] Preloss oder Postloss



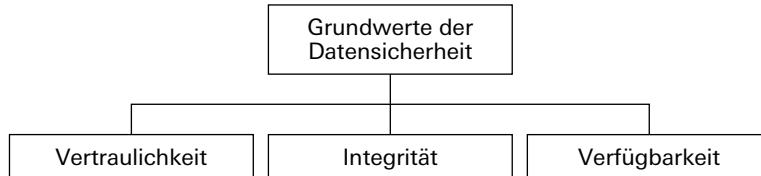
## 1.5 Betriebliche Rahmenbedingungen

---

Praktisch alle Geschäftsprozesse starten mit der Aufnahme von Daten und enden mit dessen Speicherung. Ein Ausfall der Systeme und somit das Wegfallen der Datenverarbeitung zieht den Stillstand des Unternehmens mit sich. Datensicherheit ist gegeben, wenn die folgenden drei Grundwerte eingehalten werden:

[1-4] Grundwerte der Datensicherheit

---



### 1.5.1 Vertraulichkeit

---

Die Daten werden unter Einhaltung des Datenschutzgesetzes (siehe Kap. 1.6.2, S.16) bearbeitet. Mit geeigneten Massnahmen wird verhindert, dass unberechtigte Personen Zugriff auf nicht für sie bestimmte Daten haben, beispielsweise durch Verschlüsselung der Daten.

### 1.5.2 Integrität

---

Unter Integrität wird die Korrektheit und Vollständigkeit von Informationen und Daten verstanden. Beispielsweise die korrekte Schreibweise der Nachnamen der Kunden. Zudem sind die Daten frei von Manipulation.

### 1.5.3 Verfügbarkeit

---

Ein System muss immer dann verfügbar sein, wenn der Benutzer damit arbeiten möchte. Natürlich gelten hier die Regelungen zur Wartung der Systeme zwischen Anbieter der Systeme und dem Benutzer. So wird z. B. abgemacht, dass die Computer während den Büroarbeitszeiten 99.9% zur Verfügung stehen.

## 1.6 Gesetzliche Vorschriften

---

Der Schutz der Daten ist ebenfalls gesetzlich vorgeschrieben. In der Schweiz sind in Bezug auf Datensicherheit v. a. das Obligationenrecht (OR) sowie das Datenschutzgesetz (DSG) relevant.

### 1.6.1 Obligationenrecht (OR)

---

Jedes Unternehmen ist gesetzlich dazu verpflichtet, seine Daten auf bestimmte Zeit, i. d. R. 10 Jahre, aufzubewahren. Diese Daten können auf Papier oder elektronisch gesichert werden. Das Unternehmen hat also Sorge zu tragen, dass Ihre Daten während der gesetzlich vorgeschriebenen Zeit aufbewahrt werden und während dieser Zeit jederzeit gelesen werden können. Die dazugehörige GeBüV von 2002 regelt die Grundsätze für eine ordnungsgemäße Aufbewahrung sowie die zulässigen Datenträger im Detail.

### 1.6.2 Datenschutzgesetz (DSG)

Daten über natürliche und juristische Personen sind sensibel und müssen daher geschützt werden. Sie wären bestimmt auch nicht erfreut, wenn jeder Ihre Krankenakte oder Ihre Lohndaten einsehen könnte. Der Umgang mit Personendaten ist im **DSG** geregelt. Das Schweizer Datenschutzgesetz will in erster Linie die Persönlichkeit und die Grundrechte von Personen schützen, über die Daten bearbeitet werden. **Besonders schützenswert** sind gemäss Art. 3 Abs. c DSG folgende Personendaten:

- Religiöse Ansichten, z. B. Zugehörigkeit zu einer Landeskirche
- Weltanschauliche Ansichten
- Politische Ansichten und Tätigkeiten
- Gesundheit, z. B. der Blutwert eines Patienten
- Intimsphäre
- Rassenzugehörigkeit

Sobald ein Unternehmen Personendaten speichert und bearbeitet, muss dem Datenschutz besondere Beachtung geschenkt werden. Gemäss Art. 7 DSG müssen angemessene technische und organisatorische Massnahmen getroffen werden, um solche Daten gegenüber unbefugter Bearbeitung zu schützen. Für die Planung und Umsetzung geeigneter Schutzmassnahmen bietet die **Verordnung zum Datenschutzgesetz (VDSG)** eine Hilfestellung. In Art. 9 VSDG<sup>[1]</sup> heisst es unter anderem:

*«Der Inhaber der Datensammlung trifft insbesondere bei der automatisierten Bearbeitung von Personendaten die technischen und organisatorischen Massnahmen, die geeignet sind, namentlich folgenden Zielen gerecht zu werden:*

- a. *Zugangskontrolle: unbefugten Personen ist der Zugang zu den Einrichtungen, in denen Personendaten bearbeitet werden, zu verwehren;*
- b. *Personendatenträgerkontrolle: unbefugten Personen ist das Lesen, Kopieren, Verändern oder Entfernen von Datenträgern zu verunmöglichen;*
- c. *Transportkontrolle: bei der Bekanntgabe von Personendaten sowie beim Transport von Datenträgern ist zu verhindern, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können;*
- d. *Bekanntgabekontrolle: Datenempfänger, denen Personendaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden, müssen identifiziert werden können;*
- e. *Speicherkontrolle: unbefugte Eingabe in den Speicher sowie unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten sind zu verhindern;*
- f. *Benutzerkontrolle: die Benutzung von automatisierten Datenverarbeitungssystemen mittels Einrichtungen zur Datenübertragung durch unbefugte Personen ist zu verhindern;*
- g. *Zugriffskontrolle: der Zugriff der berechtigten Personen ist auf diejenigen Personendaten zu beschränken, die sie für die Erfüllung ihrer Aufgabe benötigen;*
- h. *Eingabekontrolle: in automatisierten Systemen muss nachträglich überprüft werden können, welche Personendaten zu welcher Zeit und von welcher Person eingegeben wurden.»*

[1] Stand per 1. Dezember 2010.

Daten sind unbezahlbar und sind konstant verschiedenen **Bedrohungen** ausgesetzt:

- Höhere Gewalt
- Menschliches Versagen
- Technisches Versagen
- Kriminelle Handlung

Mit **organisatorischen, personellen, technischen und baulichen Massnahmen** können die Daten geschützt werden. Aus betrieblichen Gründen ist darauf zu achten, dass Daten jederzeit und in korrekter Weise den Mitarbeitenden zur Verfügung stehen. Bei einem Verlust könnte die Existenz des Unternehmens bedroht sein. Zudem existieren auch **gesetzliche Vorschriften zur Datenhaltung und -sicherung**.

## Repetitionsfragen

- 
- 1 In welche vier Ursachen werden Bedrohungen eingeteilt?
- 
- 7 Nennen Sie zwei Beispiele für technische Massnahmen zur Datensicherheit.
- 
- 13 Sie nehmen ein Grippe-Medikament ein, weil Sie Fieber haben. Handelt es sich dabei um eine Massnahme im Bereich Preloss oder Postloss? Begründen Sie Ihre Antwort.
- 
- 19 Im Rahmen der Datensicherheit lassen sich drei Grundwerte unterscheiden. Wie heißen diese?
-

## 2 Was bedeutet Datensicherung?

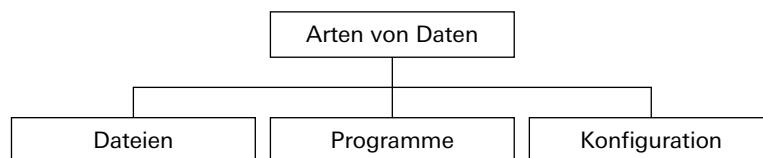
Im vorherigen Kapitel 1, S. 13 haben Sie einen Überblick über die verschiedenen Bedrohungen und Massnahmen der Datensicherheit erhalten. In diesem Kapitel erfahren Sie nun, wie die Begriffe «Backup» und «Restore» einzuordnen sind.

### 2.1 Welche Daten werden gesichert?

Durch technisches Versagen, versehentliches Löschen oder durch Manipulation können gespeicherte Daten unbrauchbar werden bzw. verloren gehen. Während z. B. eine Firewall das Eindringen von unberechtigten Personen von Anfang an verhindert, geht es bei der Datensicherung darum, bereits zerstörte Daten nachträglich (Postloss) wiederherzustellen. Die Zerstörung der Daten geschieht in vielen Fällen nicht absichtlich oder bösartig. Vielfach löschen interne Mitarbeitende versehentlich bei der täglichen Arbeit Dateien.

Wenn wir von Daten sprechen, sind nicht nur von uns erstellte Dateien wie z. B. ein Brief im Textverarbeitungsprogramm gemeint, sondern jegliche Software und deren Einstellungen (Konfiguration):

[2-1] Arten von Daten



#### 2.1.1 Dateien

Unter Dateien versteht man Software, die Sie selbst erstellt und auf dem Computer gespeichert haben. Das könnten Texte, Bilder, Tabellen, Datenbanken oder andere Dokumente sein. Dateien sind unmittelbar gefährdet, da sie nur einmalig vorliegen und deren Verlust vielfach endgültig ist.

#### 2.1.2 Programme

Unter Programmen versteht man Software, die Funktionen ausführt, z. B. ein Tabellenkalkulationsprogramm. Werden Dateien des Betriebssystems und der installierten Programme beschädigt (oder verändert), kann das dazu führen, dass ein Anwendungsprogramm oder auch das Betriebssystem nicht mehr wie vorgesehen funktioniert. Trotzdem müssen diese Dateien oft nicht zwingend gesichert werden. Denn meistens gibt es fürs Betriebssystem Reparaturmechanismen oder man installiert das Betriebssystem mit den Original-CDs neu. Auch Anwendungsprogramme, z. B. die Textverarbeitung, können jederzeit vollständig deinstalliert und vom Original wiederhergestellt werden.

#### 2.1.3 Konfigurationen

Unter Konfiguration versteht man Eintragungen in Dateien, die das Verhalten der Programme festlegen. Zum Beispiel das Datumsformat wird in den USA und in der Schweiz unterschiedlich festgelegt. Wenn Sie Programme auf Ihre Bedürfnisse hin verändert haben, dann sollten Sie die sogenannten Konfigurationsdateien ebenfalls speichern, weil Ihre Änderungen darin abgespeichert sind. Dazu zählen z. B. Einträge in Wörterbüchern,

Einstellungen im Desktop, Favoriten im Browser etc. Ihre Konfigurationsdateien verschwinden, wenn Sie das Betriebssystem oder die Anwendungsprogramme komplett neu aufspielen.

## 2.2 Was bedeuten «Backup» und «Restore»?

---

Für die Datensicherung werden häufig die englischen Begriffe «Backup» (Datensicherung) und «Restore» (Wiederherstellung) verwendet. Das primäre Ziel eines Backup- und Restore-Vorgangs besteht darin, Datenverluste zu verhindern.

### 2.2.1 Backup

---

Ein **Backup** wird meistens durch eine Sicherungskopie erreicht. Bei der Erstellung einer Sicherungskopie wird zu einem bestimmten Zeitpunkt ein Duplikat der Daten erstellt, auf das bei Bedarf zurückgegriffen werden kann. Von besonders wichtigen Daten wird i. d. R. nicht nur ein Duplikat erstellt, sondern mehrere, die an verschiedenen Orten aufbewahrt werden.

### 2.2.2 Restore

---

Die Umkehrung des Backup-Vorgangs nennt man **Restore**. Bei diesem Vorgang werden die gesicherten Daten wiederhergestellt. Das heisst, die gespeicherten bzw. duplizierten Daten werden von der Sicherungskopie in das laufende System zurückgespielt (kopiert).

### 2.2.3 Image

---

Wenn gar nichts mehr geht, hilft nur noch eine Neuinstallation des Computers. Es ist denkbar, dass das Betriebssystem nicht mehr zu retten ist. Die Basis ist so in Mitleidenschaft gezogen, dass nur noch eine komplette Neuinstallation hilft. Damit aufwendige Einstellungen und die Installation von individuellen Treibern nicht gemacht werden müssen, wurden vorgängig neben den Daten auch die Programme sowie deren Konfiguration gespeichert. Eine solche Kopie wird auch **Image** genannt. Die nachfolgende Tabelle vergleicht die Wiederherstellung eines Computers nach einem Totalausfall mit und ohne Image-Sicherung.

Schritt	Ohne Image	Mit Image
1	Neuinstallation des Betriebssystems	Wiederherstellung des kompletten Systems
2	Neuinstallation der Anwendungsprogramme	
3	Benutzereinstellungen vornehmen	
4	Wiederherstellung der Dateien	

### 2.2.4 Disaster Recovery

---

Ein **Disaster Recovery** (Notfall-Wiederherstellung) umfasst alle Massnahmen, die nach einem Unglücksfall in der Informationstechnik eingeleitet werden. Dazu gehören sowohl die Datenwiederherstellung als auch der Ersatz nicht mehr benutzbarer IT-Infrastrukturen und Anwendungen.

### 2.2.5 Backup- und Restore-Konzept

Beim **Backup- und Restore-Konzept** geht es darum, dass sich eine Privatperson oder ein Unternehmen Gedanken zur Datensicherung und -aufbewahrung macht und diese Aspekte schriftlich in einem Konzept festhält. Dazu gehört es, die sieben W-Fragen zu klären.

W-Frage	Beschreibung / Beispiele
Was?	Welche Daten werden gesichert?
Wann?	Tagsüber, in der Nacht, online oder offline
Wie oft?	Stündlich, täglich, wöchentlich
Wie viel?	Wie viele verschiedene Sicherungen werden aufbewahrt?
Wer?	Wer trägt die Verantwortung für Sicherung und Kontrolle?
Wie?	Welches Medium wird eingesetzt, welche Software?
Wo?	Wie ist die Aufbewahrung geregelt bzw. wo werden die Daten aufbewahrt?

### 2.2.6 Backup- und Restore-System

In Unternehmen sind Daten überall im Netzwerk verteilt. Zudem bestehen unterschiedliche Bedürfnisse, die ein einzelnes Medium nicht gewährleisten kann. Beispielsweise dauert ein Restore ab einem Band, das in einem feuerfesten Tresor aufbewahrt wird, länger als von einer im Netz angeschlossenen Festplatte. Dafür ist das Band im Tresor sicherer als die Festplatte im Netz.

Durch diese unterschiedlichen Bedürfnisse werden komplexe Systeme mit unterschiedlichen Medien, Rollen (z. B. Backup-Verantwortlicher) sowie Abläufen, ein sogenanntes **Backup- und Restore-System**, aufgebaut. Das Backup- und Restore-System ist demnach die Umsetzung bzw. der Betrieb des Backup- und Restore-Konzepts.

## 2.3 Backup ist nicht Archivierung

Ein Backup hat zum Ziel, gelöschte bzw. zerstörte Daten bei Bedarf wiederherzustellen und so einen reibungslosen Geschäftsbetrieb zu gewährleisten. Bei der **Archivierung** hingegen werden gesetzliche Anordnungen befolgt. Gesetzlich ist es vorgeschrieben, gewisse Daten für eine definierte Zeit aufzubewahren, d. h., zu archivieren.

Was	Dauer	Gesetz
Geschäftsbücher, Buchungsbelege	10 Jahre	Obligationenrecht (OR)

Archivdaten werden i. d. R. auf ein separates Medium geschrieben und aus Platzgründen vom ursprünglichen Laufwerk wieder gelöscht. Beim Archiv gelten nachfolgende Aspekte:

- Gesetzlich vorgeschrieben
- Nachvollziehbarkeit der Geschäftsvorfälle, Beweismittel
- Kosten- und Platz einsparung durch Auslagerung

Der Preiszerfall bei den Harddisks hat dazu geführt, dass diverse Unternehmen Daten nicht mehr archivieren (vom Originalspeicherort entfernen), sondern nur noch Sicherheitskopien anlegen. Die in diesem Lehrmittel vorgestellten Medien und Konzepte können nicht nur beim Backup und Restore, sondern auch bei der Archivierung angewendet werden. In der folgenden Tabelle sehen Sie die wesentlichen Unterschiede zwischen Backup und Archiv:

Aspekt	Backup	Archiv
<b>Ziel</b>	Falls Daten ungewollt zerstört oder gelöscht werden, können diese aufgrund von vorher hergestellten Kopien wiederhergestellt werden.	Geschäftsdaten einer entsprechenden Periode werden nach den gesetzlichen Regeln aufbewahrt.
<b>Dauer</b>	Kurz- bis mittelfristig. In der Regel von einigen Wochen bis einige Monate.	Langfristig. In der Regel über mehrere Jahre je nach gesetzlicher Aufbewahrungsfrist.
<b>Original-daten</b>	Die Daten bleiben auf dem System bestehen. Der Backup kopiert lediglich die Daten.	Die Originaldaten werden verschoben. Archivierung bedeutet also, dass die ehemaligen produktiven Daten vom System entfernt werden.

In diesem Kapitel haben Sie unterschiedliche Begriffe kennengelernt:

- Ein **Backup** ist die Ausführung einer Sicherheitskopie. Sinn und Zweck des Backups ist, die Daten im Falle eines Verlusts gesichert zu haben.
- Ein **Restore** ist der Vorgang, gesicherte Daten wieder zurückzuholen.
- Ein **Image** ist eine komplette Kopie eines Systems (Programme, Konfiguration und Daten), damit eine Inbetriebnahme schneller durchgeführt werden kann.

Der Begriff **Disaster Recovery** bezeichnet alle Massnahmen, die nach einem Unglücksfall in der Informationstechnik eingeleitet werden. Dazu zählt sowohl die Datenwiederherstellung als auch das Ersetzen nicht mehr benutzbarer Infrastruktur, Hardware und Organisation.

Ein **Backup- und Restore-Konzept** ist ein schriftliches Konzept, bei dem alle relevanten Informationen zur Datensicherung definiert und dokumentiert werden. Aufgrund unterschiedlicher Bedürfnisse werden danach **Backup- und Restore-Systeme** mit diversen Medien, Rollen (z. B. Backup-Verantwortlicher) und Abläufen aufgebaut.

Mittels **Backup** sollen unfreiwillig gelöschte oder zerstörte Daten wiederhergestellt und ein durchgängiger Systembetrieb gewährleistet werden. Mittels **Archivierung** hingegen werden gesetzliche Anordnungen befolgt.

## Repetitionsfragen

- 
- 25 Erklären Sie in einfachen Worten die Begriffe Backup und Restore.
- 
- 31 Was versteht man unter einer Konfiguration?
- 
- 37 Was ist der Unterschied zwischen Backup und Archivierung?
- 
- 43 Ein Bestandteil eines Backup- und Restore-Konzepts ist die Antwort auf die Frage «Wo?». Erklären Sie, was damit gemeint ist.
-

## 3 Wo werden Daten gesichert?

In diesem Kapitel lernen Sie mehrere **Speichermedien** kennen, die sich für ein Backup und Restore eignen. Historisch kann zwischen magnetischen und optischen Speichermedien unterschieden werden. In jüngster Zeit wurden diese Technologien kombiniert, um die jeweiligen Vorteile zu nutzen und die jeweiligen Nachteile zu minimieren.

### 3.1 Magnetische Speichermedien

Die magnetische Speicherung von Information erfolgt auf magnetisierbarem Material. Dieses kann auf Bänder, Karten, Papier oder Platten aufgebracht werden. Magnetische Medien werden i. d. R. mittels eines Lese-/Schreibkopfs gelesen respektive geschrieben. Wir unterscheiden hier zwischen rotierenden Platten(stapeln), die mittels eines beweglichen Kopfs gelesen und geschrieben werden (z. B. Festplatte), und nicht rotierenden Medien, die üblicherweise zum Lesen / Schreiben an einem feststehenden Kopf vorbeigeführt werden (z. B. Magnetbänder).

#### 3.1.1 Removable Disk Storage (RDX)

Das Removable Disk Storage (RDX) ist ein externes Laufwerk, in das man die einzelnen Datenträger einschieben kann. Bei den Datenträgern selber handelt es sich um 2.5-Zoll-SATA-Festplatten mit Kapazitäten von 160 GByte bis 2 000 GByte. Dem Laufwerk selber ist es dabei egal, welche Datenträger man verwendet. Da es sich um Festplatten handelt, ist das Laufwerk nicht abhängig von der gewählten Datenträgergrösse.

[3-1] RDX-Kassette



### 3.1.2 Festplatte

Festplatten sind aufgrund der grossen Speicherkapazität bei immer günstigeren Preisen ein kommendes Speichermedium für Backups. Eine Festplatte besteht aus mehreren magnetischen Platten, die über bewegliche Leseköpfe die Daten direkt speichern und abrufen. Dabei unterscheiden wir zum Einen zwischen den häufig im privaten Umfeld eingesetzten einzelnen Platten (meist als externe USB-Laufwerke) und den im betrieblichen Umfeld verwendeten Netzwerkfestplatten, entweder als direkt am Server angeschlossene oder über das Netzwerk verbundene Systeme.

[3-2] Festplatte



#### Direct Attached Storage (DAS)

Beim DAS handelt es sich um Festplatten, die direkt am Server angeschlossen werden, aber nicht im Servergehäuse integriert sind. Der Vorteil sind der geringe zusätzliche Hardwareaufwand und die rasche Speicherung von Daten aufgrund der Anbindung über Systembusse wie SAS. Da die Disks direkt angeschlossen werden, benötigen sie zudem kein zusätzliches Betriebssystem, sondern werden über den vorhandenen Server verwaltet.

#### Network Attached Storage (NAS)

Beim NAS handelt es sich um einen spezialisierten Fileserver. Soll ein Festplattenspeicher mit den darauf abgelegten Dateien auf dem kompletten Netzwerk zur Verfügung stehen, muss das Speichersystem zunächst direkt an das Netzwerk angeschlossen sein und zusätzlich Methoden beherrschen, die die Dateien auf diesem Speicherplatz im angebundenen Computernetz zur Verfügung stellen. Man spricht dann von einem Speicher, der an ein Netz angeschlossen ist, einem «Network Attached Storage». NAS-Systeme werden also direkt am Netzwerk angeschlossen und arbeiten autonom, ohne einen dedizierten PC oder Server zu benötigen. Die Dateisysteme des NAS, also alle dort angelegten Dateien und Verzeichnisse, erscheinen auf dem Zielsystem wie eine eingebundene Freigabe bzw. wie ein lokales Dateisystem.

[3-3] Network Attached Storage (NAS)



### 3.1.3 Magnetband

Magnetbänder können für sehr grosse Datenmengen genutzt werden. Die Kapazität von Bändern hängt vom verwendeten Standard (AIT, DAT, DDS usw.) ab und reicht von ca. 120 MByte bis hin in den dreistelligen GByte-Bereich. Dank laufender Entwicklung steigert sich die Speicherkapazität konstant.

Bei **Bandlaufwerken** werden die Daten auf ein Magnetband geschrieben, das auf- und abgespult wird. Aus diesem Grunde können die Bänder nur sequenziell speichern und gelesen werden. Suchen Sie auf einem Band eine bestimmte Datei, muss eventuell das komplette Band zuerst abgespult werden, was viel Zeit benötigt.

[3-4] Magnetbänder



Bandlaufwerke sind seit Jahren im Einsatz und haben sich bei der Langzeitarchivierung bewährt. Um den Aufwand mit dem manuellen Wechseln von Bändern zu minimieren, wurden spezielle Bandmagazine entwickelt. Diese Magazine umfassen mehrere Bänder, die als ein Laufwerk angesprochen werden können. Somit sind hohe Speicherkapazitäten vorhanden, was das Bandlaufwerk besonders für Unternehmen mit grossem Backup-Umfang attraktiv macht. Beim automatischen Wechsel mittels Bandmagazin wird zwischen **Autoloader** und **Library** unterschieden:

Autoloader	Library
Autoloader haben i. d. R. nur ein Bandlaufwerk und nur wenige Magnetbänder (8, 10 bis 16). Die Bänder sind ähnlich einem Karussell angeordnet.	Libraries können mehrere Dutzend Bandlaufwerke haben, in die Roboterarme Magnetbänder aus Magnetbandmagazinen einlegen. Solche Magazine umfassen durchaus mehrere Tausend Magnetbänder.

[3-5] Library



Nachfolgend werden häufig eingesetzte Bandtechnologien näher erklärt.

**Digital Audio Tape (DAT) und Digital Data Storage (DDS)**

Das DAT-Verfahren stammt aus dem Audiobereich und wurde erst später für die Datensicherung nutzbar gemacht. Unter dem Begriff DDS (Digital Data Storage) wurde von HP und Sony 1989 ein aus dem DAT abgeleitetes Verfahren zur Speicherung von Daten entwickelt. Bei DDS-1 bis DDS-5 wird ein etwa 4 mm breites Magnetband (Bandbreite) in einer Kassette benutzt, bei DDS-6 ist es 8 mm breit. Die Kapazität beträgt bis zu 160 GByte.

**Advanced Intelligent Tape (AIT)**

Advanced Intelligent Tape (AIT) stammt nicht originär aus dem Computersektor, sondern aus der Videotechnik (Video 8). Der Vorteil von AIT gegenüber DDS waren von Beginn an die höhere Schreib- und Lesegeschwindigkeit sowie der in der Bandkassette integrierte Chip, der einen Katalog der Sicherungen enthält und damit den Zugriff wesentlich beschleunigt. Die Kapazität beträgt bis zu 4 TByte.

**Digital Linear Tape (DLT)**

Mit DLT-Medien können Daten im Vergleich mit anderen Technologien schneller übertragen werden. Die Laufwerke besitzen eine zuschaltbare Hardwarekompression, mit der die zu sichernden Daten komprimiert werden können. Die Kapazität beträgt bis zu 800 GByte.

**Linear Tape Open (LTO)**

Linear Tape Open (LTO) wurde von IBM, HP und Quantum als Gemeinschaftsprojekt erarbeitet. Eine Besonderheit von LTO ist, dass es von Anfang an nicht als Lösung eines einzelnen Herstellers geplant war. So werden heute von über 30 Herstellern Magnetbänder und fast allen Robotik-Herstellern Autoloader und Libraries für LTO angeboten. Diese werden vom Urheberkonsortium zertifiziert.

## 3.2 Optische Speichermedien

---

Die optische Speicherung nutzt Filter-, Reflexions- und Beugungseigenschaften von verschiedenen Materialien.

### 3.2.1 CD-ROM

---

Eine **CD-ROM** ist ein Datenträger, der bis zu 700 MByte aufnehmen und einmal oder mehrfach beschrieben werden kann. Eine **CD-R** ist eine CD, die einmal beschrieben werden kann, wobei R für Read (engl. für lesen) steht. Eine **CD-RW** ist eine CD, deren Daten gelöscht werden können und die sich bis zu 1 000x neu beschreiben lässt, wobei RW für Rewriteable (engl. für: wiederbeschreibbar) steht.

[3-6] CD-R

---



### 3.2.2 DVD

---

Eine **DVD** ist ein Datenträger, der wie eine CD aussieht, aber über eine deutlich höhere Speicherkapazität verfügt und vielfältiger nutzbar ist. Die Abkürzung DVD steht für Digital Versatile Disc (engl. für digitale, vielseitige Scheibe). Eine DVD hat den gleichen Durchmesser wie eine CD, umfasst aber 4.7 GByte. Ermöglicht wird dies durch eine höhere Datendichte und zwei parallele Datenschichten. Bei einer DVD können zudem beide Seiten beschrieben werden.

### 3.2.3 Blu-ray Disc (BD)

---

Eine **Blu-ray Disc (BD, BRD oder Blu-ray)** ist ein digitaler optischer Datenträger, der als High-Definition-Nachfolger der DVD entwickelt wurde und im Vergleich zu dieser eine erheblich höhere Datenrate und Speicherkapazität von bis zu 50 GByte bietet. Zudem wurde bei der Blu-ray-Entwicklung darauf geachtet, dass die Oberfläche kratzresistent ist, was ein grosser Vorteil gegenüber der CD-ROM bzw. DVD ist. Der Name Blu-ray stammt vom blauvioletten Laserstrahl, der zum Lesen der Disc benutzt wird. Er hat eine Wellenlänge von nur 405 Nanometern und ermöglicht somit eine höhere Speicherdichte.

Die Standard-Disk hat einen Durchmesser von 12 cm und kann als Single Layer oder Dual Layer Disc erworben werden. Die Kapazität der Single Layer Disc beträgt 25 GByte, die Kapazität der Dual Layer bis 50 GByte. Die Schreibgeschwindigkeiten liegen bei 4.5 MByte/s bei 1x und gehen zurzeit bis 12x-Geschwindigkeit. Eine Dual Layer Disc kann demnach in 15 Minuten mit 50 GByte Daten beschrieben werden.

### 3.3 Übrige Speichermedien

Die übrigen Medien basieren auf elektronischer Speicherung oder bestehen aus einer Mischung von magnetischen und optischen Techniken.

#### 3.3.1 Flash-Speichermedien

Bei den Flash-Speichermedien gibt es verschiedene Hersteller und Formate. Bekannt und weitverbreitet sind Speicherkarten namens **Compact Flash (CF)** und **Secure Digital (SD)**. Damit solche Speicherkarten gelesen werden können, gibt es sogenannte Kartenleser. Die meisten Kartenleser sind multiformatfähig, damit man beim Wechsel eines Kartenformats nicht auch noch den Kartenleser austauschen muss. Flash-Speicherkarten eignen sich nicht für die Sicherung grosser Datenmengen, weil der Speicherplatz für ein vollwertiges Backup nicht ausreicht. Sie bieten aber genügend Platz, um wichtige Dokumente oder Daten wie z. B. Systemeinstellungen und Kontaktadressen unterzubringen und jederzeit auf sich zu tragen.

[3-7] Compact Flash Card



#### 3.3.2 USB-Datenträger

Der **USB-Datenträger** (oft auch **USB-Stick** genannt) ist ein kleines Gerät, das sich bequem mittragen lässt. Im Handel sind diese Sticks in unterschiedlichen Größen zu haben. Der Vorteil vom USB-Datenträger ist, dass keine Mechanik zum Speichern notwendig ist, da diese auf elektronischer Basis gespeichert werden. Dadurch sind Daten auf dem USB-Datenträger rasch gespeichert. Die Speicherkapazität der USB-Datenträger nimmt rasant zu. Damit lassen sie sich nicht nur für den Transport von Daten, sondern auch als Datenbank oder Sicherungsmedium einsetzen.

[3-8] USB-Stick



#### 3.3.3 Magneto Optical Disk (MOD)

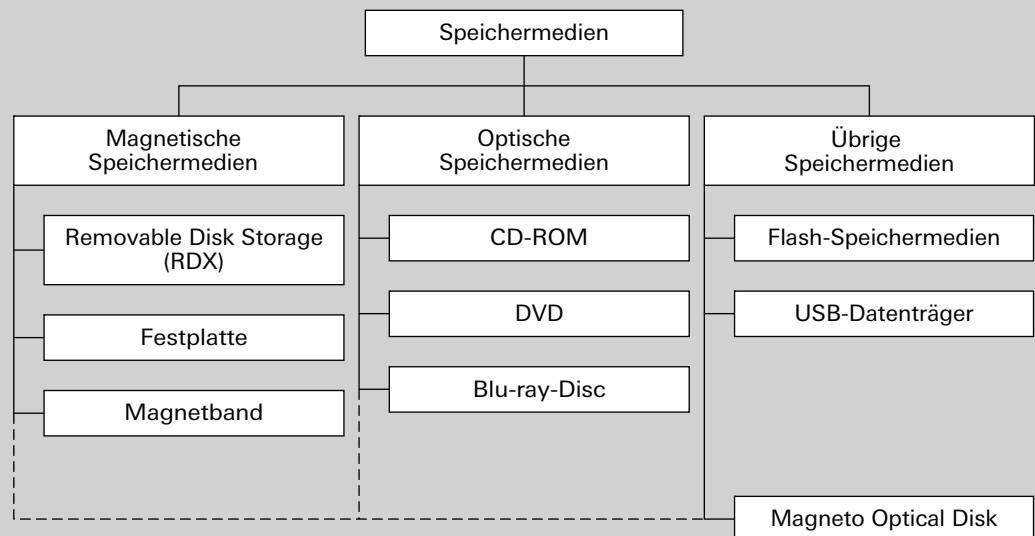
Die **Magneto Optical Disk (MOD)** ist ein rotierendes Speichermedium, das optisch gelesen und magnetisch beschrieben wird. Die Speicherkapazität dieser Medien hängt vom Durchmesser, von der Spurdichte, der Bitdichte und der Sektorgrösse ab. Heutige Speichermedien umfassen bis zu 5 GByte. Die Magneto Optical Disk vereint die Vorteile der magnetischen und optischen Speichermedien und ist deshalb sehr sicher.

[3-9] Magneto Optical Disk



Historisch kann zwischen magnetischen und optischen Speichermedien unterschieden werden. In jüngster Zeit wurden diese Technologien kombiniert, um die jeweiligen Vorteile zu nutzen und die jeweiligen Nachteile zu minimieren. Hier ein Überblick über die wichtigsten **Speichermedien**:

Speichermedien im Überblick



Jedes Speichermedium hat seine Vor- und Nachteile und nicht alle Datenträger eignen sich für einen vollständigen Backup. Hier die wichtigsten **Merkmale**:

Medium	Kapazität	Vorteile	Nachteile
Festplatten	2–200 GByte und grösser	Grosse Kapazität, schneller Zugriff	Rotierender Lese- und Schreibkopf erhöht das Abnutzungsrisiko
Magnetbänder	120 MByte bis 400 GByte und grösser	Grosse Kapazität, lange haltbar	Sequenzieller Zugriff
CD	650–700 MByte	Mittlere Kapazität, geringe Kosten	CD-Brenner erforderlich
DVD	4.7 GByte	Grosse Kapazität	DVD-Brenner erforderlich
USB-Datenträger	1 000 GByte und grösser	Keine Mechanik, rasche Übertragung, einfach verwendbar	Hoher Preis im Verhältnis zur Kapazität
Magneto Optical Disk	Bis 5 GByte	Vereinte Vorteile von magnetischen und optischen Speichermedien	Spezielles Gerät erforderlich

## Repetitionsfragen

- 
- 49 Ein Unternehmen entscheidet sich für die Datensicherung auf Festplatte. Welchen Vorteil hat die Festplatte gegenüber den Magnetbändern?
- 
- 2 Bei welchem Speichermedium werden die Daten sequenziell beschrieben und abgerufen?
- 
- 8 Nennen Sie zwei Vorteile der Blu-ray Disc gegenüber einer CD-ROM.
- 
- 14 Wofür steht der Zusatz RW bei einer CD-ROM?
-

## 4 Welches Speichermedium wähle ich?

Die Auswahl an Speichermedien für Backup- und Restore-Systeme ist riesig. Nach welchen Kriterien können Sie das passende Speichermedium auswählen? In diesem Kapitel werden wichtige **Einflussfaktoren bzw. Auswahlkriterien** vorgestellt, die bei dieser Entscheidung hilfreich sind.

### 4.1 Datenmenge

Die Menge der zu speichernden Daten hat einen grossen Einfluss auf die Auswahl des Speichermediums. Müssen Sie z. B. die Datenmenge von 1 TByte auf CD-ROMs mit einer Kapazität von jeweils 700 MByte speichern, brauchen Sie rund 1 498 Stück davon. Würde man diese Datenträger (inklusive Hüllen) stapeln, kommen Sie auf eine Höhe von rund 15 Metern. Haben Sie so viel Platz? Während für den Privatgebrauch CD-ROMs oder DVDs als Speichermedien u. U. reichen, sind für grosse Datenmengen eines Unternehmens Speichermedien mit höheren Kapazitäten notwendig. Für die Abschätzung der benötigten Speicherkapazitäten und -medien müssen Sie folgende **Einflussfaktoren** berücksichtigen:

- **Wachstum pro Jahr:** In Betrieben werden laufend neue Daten produziert. Dieses Wachstum an Daten muss bei der Planung bereits eingeplant werden.
- **Geplante Jahre:** Die Anzahl Jahre, die das Backup-System im Einsatz ist, wird ebenfalls eingerechnet. Da sich die Backup-Systeme konstant weiterentwickeln, lohnt sich ein Wechsel auf ein neues System.

Die Anzahl benötigter Speichermedien kann anhand folgender Formel berechnet werden:

$$\frac{\text{Heutiger Speicherbedarf} + (\text{Wachstum pro Jahr} \cdot \text{geplante Jahre})}{\text{Speicherkapazität des Speichermediums}} = \text{Anzahl Medien}$$

Zur einfacheren Berechnung empfiehlt es sich, alle Speichergrößen in die gleiche Einheit zu verwandeln (z. B. in MByte). Dabei gelten folgende Gleichungen:

Abkürzung	Grösse
1 KByte	1 Kilobyte
1 MByte	1 Megabyte
1 GByte	1 Gigabyte
1 TByte	1 Terabyte
	1 024 Bytes
	1 024 KB = 1 048 576 Bytes
	1 024 MB = 1 073 741 824 Bytes
	1 024 GB = 1 099 511 627 776 Bytes

#### Beispiel

Die aktuelle Datenmenge eines Unternehmens liegt bei 1 TByte und nimmt jährlich um 10 GByte zu. Geplant ist, dass die Speichermedien während der nächsten 5 Jahre eingesetzt werden.

Externe Wechselfestplatten à 1 TByte	CD-ROMs à 700 MByte
$\frac{1024 \text{ GByte} + (10 \text{ GByte} \cdot 5 \text{ Jahre})}{1024 \text{ GByte}} = 1.04$	$\frac{1048576 \text{ MByte} + (10240 \text{ MByte} \cdot 5 \text{ Jahre})}{700 \text{ MByte}} = 1571.1$

Für dieses Vorhaben müssten Sie ca. zwei Festplatten (oder gleich eine grössere) oder ungefähr 1 572 CD-ROMs zur Verfügung stellen. Dabei wurde lediglich eine Vollsicherung ohne Wechselschema (vgl. Kap. 7, S. 46) berücksichtigt. Kämen diese Aspekte noch hinzu, wäre bald das Vielfache der Speichermedien erforderlich.

## 4.2 Speicherdauer

Speichermedien unterscheiden sich auch in Bezug auf Schreibgeschwindigkeiten. Die Formel zur Berechnung der Speicherungsdauer lautet wie folgt:

$$\frac{\text{Datenmenge}}{\text{Speichermenge pro Sekunde}} = \text{Speicherdauer in Sekunden}$$

### Beispiel

Miriam Meier möchte die Datenmenge von 600 MByte auf einer externen Festplatte mit einem USB-3.0-Anschluss und einer Speichergeschwindigkeit von 60 MByte pro Sekunde sichern. Entsprechend obiger Formel rechnet sie mit einer Speicherdauer von 10 Sekunden.

Die **Speichermenge pro Sekunde** hängt also von der Schreibgeschwindigkeit und vom Anschluss des Speichermediums ab (z. B. USB-Anschluss). Die Schreibgeschwindigkeit ist jeweils in der Produktbeschreibung des Herstellers ersichtlich. Die Speicherdauer ist insoweit von grosser Bedeutung, als ein Backup i. d. R. nach Arbeitsschluss ausgeführt und vor Arbeitsbeginn am nächsten Tag abgeschlossen sein muss. Dauert ein Backup länger als die zur Verfügung stehende Zeit, muss ein schnelleres Speichermedium oder eine andere Methode der Datensicherung ausgewählt werden.

## 4.3 Wiederherstellungsdauer

Bei der Auswahl eines Speichermediums muss neben der Speicherdauer der Zeitbedarf berücksichtigt werden, um gesicherte Daten wiederherzustellen. Dabei spielen neben der Lesegeschwindigkeit folgende **Aspekte** eine zentrale Rolle:

- Eine sequenzielle Speicherung auf Magnetbändern hat den Nachteil, dass der Zugriff erschwert ist. Weil die Daten in diesem Fall der Reihe nach auf die Bänder gespeichert werden, können sie auch nur der Reihe nach abgerufen werden. Demgegenüber kann auf Daten, die auf der Festplatte abgelegt sind, direkt und wesentlich schneller zugegriffen werden.
- Nicht immer sind die Speichermedien konstant mit dem Netzwerk verbunden und aus Sicherheitsgründen werden sie manchmal in einem Tresor eingeschlossen. Muss das Speichermedium für einen Restore erst aus dem Tresor geholt werden, kostet das Zeit.
- Auch die Art der Datensicherung (vgl. Kap. 5, S. 39) beeinflusst die Wiederherstellungsdauer. Wenn z. B. wöchentlich ein Voll-Backup und täglich eine inkrementelle Datensicherung durchgeführt wird, müssen bei einem Restore zuerst der Voll-Backup und danach alle inkrementellen Datensicherungen wiederhergestellt werden.

## 4.4 Kosten

---

Bei der Berechnung der Kosten für Backups sollten diese Faktoren berücksichtigt werden:

- Neben den reinen Kosten für das Speichermedium sind v. a. die Kosten für das Laufwerk sowie die Anzahl der benötigten Speichermedien in die Überlegungen einzubeziehen.
- Speichermedien können sich abnutzen und sollten bei Bedarf ersetzt werden.
- Hinzu kommen die Lagerkosten für einen eigenen oder gemieteten (Bank)tresor sowie einem Lagerraum (vgl. Kap. 13, S. 72).
- Auch Arbeitsschritte wie das Einrichten, Wechseln und eventuell das Speichern (Backup) nehmen Arbeitszeit in Anspruch. Zudem wird für den Restore eine gewisse Zeit benötigt.
- Bei regelmässigen Tests bzw. Stichproben der Backups fallen ebenfalls Arbeitsstunden an (vgl. Kap. 16, S. 89).

## 4.5 Technikwechsel

---

Von Zeit zu Zeit ändern sich Datenformate bzw. die Spezifikationen von Speichermedien. Beim Backup (aber v. a. bei der Archivierung) auf ein gewisses Speichermedium müssen Sie deshalb immer darauf achten, dass die Daten auch dann zurückgespielt werden können, wenn die Hardware defekt ist und Ihre eingesetzte Hardware nicht mehr gekauft werden kann.

### Beispiel

Sie haben einen Teil der Unternehmensdaten auf 3.5-Zoll-Disketten gespeichert. Wenn Sie nun gezwungen sind, das Diskettenlaufwerk zu ersetzen, wäre dies heute nur noch schwer möglich.

### 4.5.1 Welche Probleme verursachen lange Aufbewahrungszeiten?

---

Wenn wir eine Datei in einer Umgebung speichern und in derselben Umgebung gleich wieder aufrufen, dann sind die Entstehungs- und die Nutzungsumgebung identisch. Das geht problemlos. Wenn wir versuchen, diese Datei auf einem anderen Rechner zu öffnen, dann bringen wir die Datei in eine andere Umgebung. Die Wahrscheinlichkeit, dass wir die Datei in einer anderen Umgebung noch lesen können, hängt davon ab, wie weit sich diese Umgebungen unterscheiden. Handelt es sich um das gleiche Betriebssystem, sind die gleichen Anwenderprogramme installiert, ist die gleiche Hardware vorhanden?

Irgendwann wird auch der robusteste Computer nicht mehr funktionieren oder aber die neuste Technik wird irgendwann veraltet sein. Irgendwann wird auch das langlebigste Magnetband nicht mehr lesbar sein und irgendwann wird es möglicherweise unser Programm nicht mehr geben. Somit ist diesem Zeitfaktor v. a. bei der Archivierung besondere Beachtung zu schenken.

### 4.5.2 Wie schützen Sie sich vor den Folgen des Technikwechsels?

---

Denken Sie bei jedem Technikwechsel in Ihrem Unternehmen auch an die gesicherten bzw. archivierten Daten. Dabei ist zu prüfen, ob die Daten in der neuen Umgebung lesbar gemacht werden können. Eventuell ist zu überprüfen, ob alle alten Daten ins neue Format zu übertragen und neu zu speichern sind. Dies ist ein durchaus übliches Verfahren, das in vielen Systemumgebungen durchgeführt wird. Das regelmässige Umkopieren gehört zur jährlichen oder zweijährlichen Sicherungskontrolle und dient der Langzeitarchivierung.

## 4.6 Haltbarkeit

---

Hieroglyphen auf Papyrus und oder in Stein gemeisselt überdauerten Jahrhunderte, sogar Jahrtausende. Daher sind uns wertvolle und interessante Informationen über die alten Ägypter und deren Kultur erhalten geblieben. Wäre das auch der Fall gewesen, wenn zur Zeit der Pharaonen bereits digitale Speichermedien existiert hätten? Sehr wahrscheinlich könnten wir uns nicht mehr an den historischen Zeugnissen erfreuen, da Dateien auf den uns bisher bekannten Speichermedien eine derart lange Periode nicht überstehen würden.

Der Gesetzgeber schreibt für alle wichtigen Geschäftsdaten und Finanzunterlagen i. d. R. eine Aufbewahrungspflicht von zehn Jahren vor. Dies gilt auch für elektronisch archivierte und gespeicherte Informationen. Folgende Tabelle zeigt die ungefähre bzw. durchschnittliche Haltbarkeit diverser Speichermedien auf:

Medium	Dauer
Stein / Papyrus	2 200+ Jahre
Disketten	10–30 Jahre
Festplatten: <ul style="list-style-type: none"><li>• Im laufenden Betrieb</li><li>• Als Archivierungsmedium</li></ul>	<ul style="list-style-type: none"><li>• 2–10 Jahre</li><li>• 10–30 Jahre</li></ul>
Magnetbänder	30+ Jahre
CD-ROM	10–50 Jahre

Die effektive Haltbarkeit der einzelnen Speichermedien hängt stark davon ab, wie sie in der Praxis behandelt und gelagert werden. Dabei sind sie unbedingt vor schädlichen Umweltinflüssen zu schützen. Vergleichen Sie dazu auch das Kapitel 13.3, S. 74.

Werden Speichermedien zur Langzeitarchivierung verwendet, ist es von Vorteil, die abgespeicherten Daten von Zeit zu Zeit auf neue Speichertechnologien zu übertragen. Für die Aufbewahrung wichtiger Unternehmensdaten ist eine redundante Datenhaltung auf verschiedenen Speichermedien ratsam.

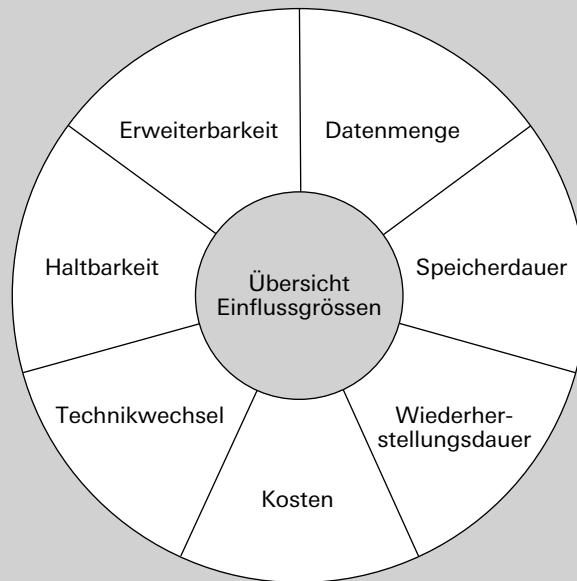
## 4.7 Erweiterbarkeit

---

Die Datenmenge, die die Mitarbeitenden eines Unternehmens produzieren, steigt kontinuierlich an. Daher ist es wichtig, dass sich auch die Speichermedien dieser Entwicklung anpassen können. Um die Daten schnell wieder finden zu können, ist es erforderlich, dass die Suche mehrere Kriterien einschließt. Für den Fall, dass dem Benutzer der Dateiname entfallen ist, sollte ebenfalls eine Suchoption für den Inhalt definiert sein.

Die **Wahl des Speichermediums** ist von den Bedürfnissen des Unternehmens abhängig.  
Bei der Entscheidung müssen folgende **Einflussfaktoren** berücksichtigt werden:

Einflussfaktoren für Speichermedien



## Repetitionsfragen

- 
- 20 Wie viele DVDs brauchen Sie, um eine Datenmenge von 1 TByte zu speichern?
- 
- 26 Wie lange müssen Sie warten, bis eine Datenmenge von 1 GByte auf einer Blu-ray Disc mit 10x-Geschwindigkeit gespeichert ist?
- 
- 32 Sie arbeiten in einem grossen Unternehmen mit riesigen Datenbeständen. Welche beiden Speichermedien eignen sich für Backups am besten?
- 
- 38 Warum müssen bei den archivierten Dateien von Zeit zu Zeit die Datenformate angepasst werden?
-



## **Teil B Technologien und Organisation der Datensicherung**

---

## Einleitung, Lernziele und Schlüsselbegriffe

### Einleitung

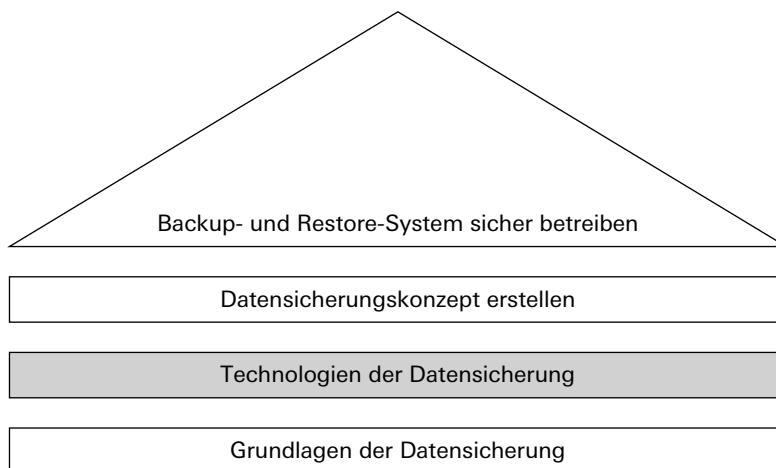
Innerhalb eines Unternehmens werden laufend neue Daten erzeugt und bestehende Daten verändert oder gelöscht. Meist sind diese Daten auf unterschiedlichen Systemen gespeichert und es dürfen keine Datenverluste in Kauf genommen werden.

Welche Technologien können nun eingesetzt werden und wie muss ich ein Unternehmen organisieren, um ein «wasserdichtes» Backup- und Restore-System aufzubauen bzw. zu betreiben? In diesem Kapitel erfahren Sie mehr darüber,

- welche Backup-Arten Ihnen zur Verfügung stehen,
- wie Sie riesige Datenmengen speichern können,
- für welche Situation sich welches Wechselschema eignet,
- wie Sie Backups während des laufenden Systembetriebs organisieren.

Folgende Grafik zeigt auf, wo Sie sich innerhalb des Lehrmittels befinden:

[4-1] Inhalt von Teil B



### Lernziele und Lernschritte

Lernziele	Lernschritte
<input type="checkbox"/> Sie kennen die verschiedenen Backup-Arten mit ihren Vor- und Nachteilen.	Welche Backup-Arten gibt es?
<input type="checkbox"/> Sie kennen verschiedene Möglichkeiten, grosse Datenmengen innerhalb einer gegebenen Zeit zu sichern.	Wie speichere ich grosse Datenmengen?
<input type="checkbox"/> Sie können eine systematische Backup-Planung mithilfe bekannter Wechselschemen planen.	Mit welchem Wechselschema soll ich arbeiten?
<input type="checkbox"/> Sie können Massnahmen treffen, Daten auch während des Betriebs vor Verlust zu schützen.	Wie stelle ich die Sicherung während des Betriebs sicher?

### Schlüsselbegriffe

Automatischer Backup, Cloud-Service, Differenzielle Datensicherung, Einzelplatz-Backup, Grossvater-Vater-Sohn, Inkrementelle Datensicherung, LAN-Backup, Offline-USV, Online-Sicherung, Online-USV, RAID, SAN, Turm von Hanoi, Voll-Backup, Wechselschema

## 5 Arten der Datensicherung

Nicht nur die Bedürfnisse, auch die Technologien und die Methoden der Datensicherung haben sich in den letzten Jahren stark gewandelt. Während früher die Sicherung lokaler Datenbestände einzelner Geräte (PC, Server) bzw. deren Speichermedien im Vordergrund stand, gilt es heute, riesige Datenbestände vernetzter Systeme zu sichern, die ggf. über mehrere Standorte verteilt sind. In diesem Kapitel wird diese Entwicklung nachgezeichnet und die wichtigsten Backup-Arten werden Ihnen vorgestellt.

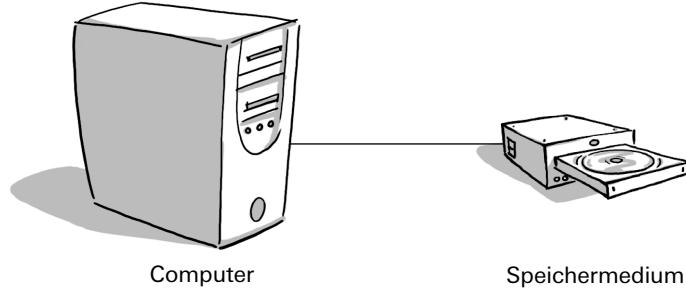
### 5.1 Einzelplatz-Backup

Beim Einzelplatz-Backup wird ein Speichermedium direkt mit dem Computer verbunden. Die Daten werden dabei vom Computer direkt auf dieses Medium gesichert. Sobald das Speichermedium voll ist, wird manuell ein weiteres leereres Medium eingelegt.

#### Beispiel

Im privaten Bereich können mittels des Einzelplatz-Backups z. B. die Daten auf eine CD-ROM gebrannt werden. Sobald eine CD voll ist, wird eine neue eingelegt.

[5-1] Einzelplatz-Backup

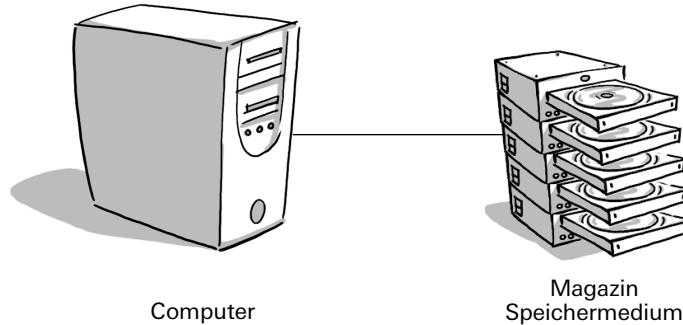


In Unternehmen werden Daten i. d. R. auf zentralen Datenservern gesammelt. Dabei werden riesige Mengen an Daten aufbewahrt. Der grosse Nachteil beim Einzelplatz-Backup liegt darin, dass der Aufwand für das ständige Wechseln der Speichermedien zu aufwendig ist.

### 5.2 Automatischer Backup

Um den grossen Wechselaufwand vom Einzelplatz-Backup zu umgehen, stehen automatische Backups zur Verfügung. Beim automatischen Backup werden die Speichermedien, z. B. Bänder, in Magazinen (Autoloader oder Library) verwaltet. Die darauf abgestimmte Datensicherungssoftware organisiert den täglichen Wechsel der Bänder oder sorgt dafür, dass bei vollem Band ein Folgeband automatisch geladen wird.

[5-2] Automatischer Backup



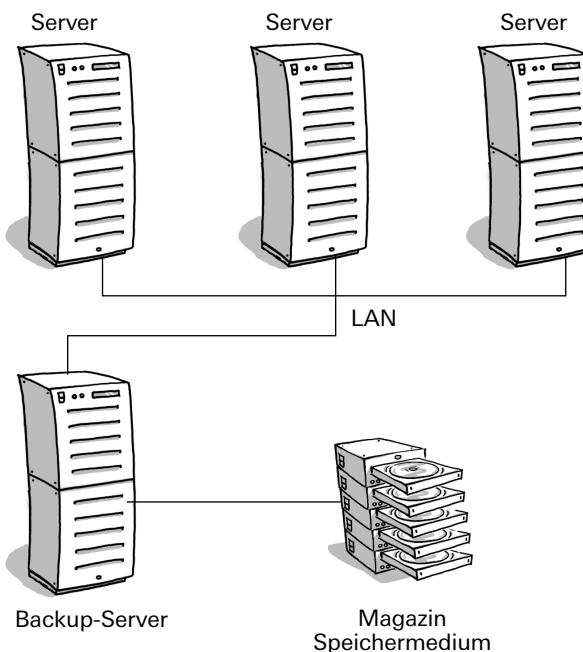
Der automatische Backup ist eine gute Lösung, um den Aufwand für das manuelle Wechseln zu umgehen. Ebenfalls können auf einem Magazin komplett Serverinhalte ohne manuelles Eingreifen abgespeichert werden. Die Vorteile des automatischen Backups:

- Höhere Speicherkapazität
- Unternehmenskritische Daten werden automatisch geschützt
- Der Backup wird automatisch gestartet und geht nicht vergessen
- Das Personal wird entlastet und kann sich auf die Kontrolle der Backups konzentrieren

### 5.3 LAN-Backup

Mit der Einführung eines lokalen Netzwerks (LAN) entstand das Bedürfnis, von jedem beliebigen Host im Netzwerk Daten auf einen Server zu übermitteln und dort zu sichern. Dieser Datenverkehr belastete jedoch das LAN zusätzlich. Ein **LAN-Backup** schafft hier Abhilfe. Dieses bezeichnet nicht etwa eine Datensicherung über das LAN, sondern den Aufbau eines eigenen LANs für die Datensicherung. Ausgehend vom Server wird dazu rückwärtig ein zweites Netzwerk für die Datensicherung aufgebaut. So können die Clients und Server im LAN ohne zusätzlichen Traffic und im LAN arbeiten.

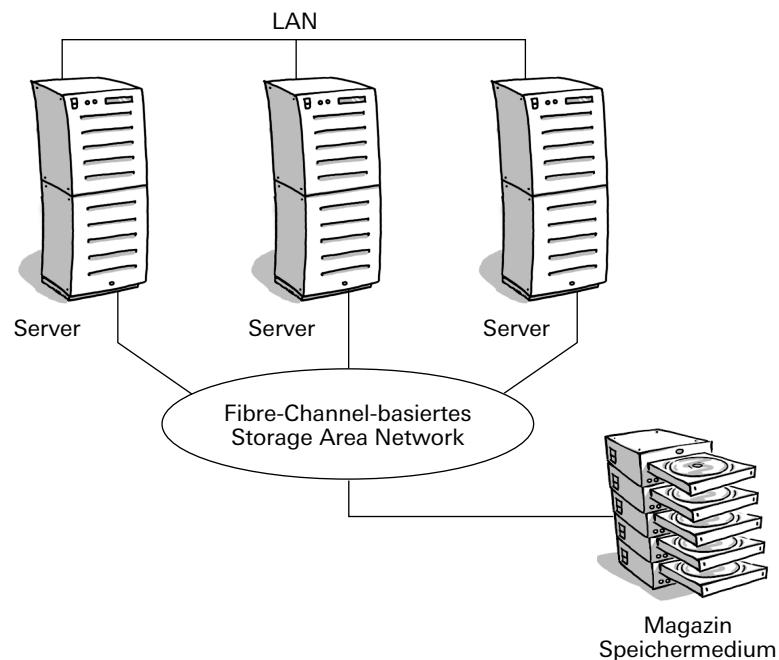
[5-3] LAN-Backup



## 5.4 Storage Area Network (SAN)

Ein Storage Area Network ist ein Speichernetz, das entweder über Fibre Channel oder über iSCSI realisiert wird. Diese Technologie erlaubt es, spezifische Backup-Speichermedien wie z. B. Bandeinheiten oder Plattensysteme mit einem Netzwerk zu verbinden. Zentraler Vorteil eines SAN ist die rasche Übertragung riesiger Datenmengen über grosse Distanzen hinweg. Zudem sorgen die verwendeten Protokolle für einen sicheren Betrieb des Datentransfers. Aufgrund einer redundanten Auslegung der Verbindungen und Geräte bietet ein SAN zudem eine wesentlich höhere Verfügbarkeit.

[5-4] Storage Area Network



## 5.5 Online-Datensicherung

Über leistungsstarke Internetverbindungen und verschlüsselte Leitungen können Daten schnell und sicher an einen entfernten Ort kopiert und dort gespeichert werden. Der Vorteil dieser Technologie ist ein hoher Sicherheitsstandard, weil spezialisierte Anbieter über gut ausgerüstete Rechenzentren und gut ausgebildete Mitarbeitende verfügen. Zudem schafft die räumliche Distanz bei lokalen Ereignissen eine höhere Datensicherheit. Darüber hinaus entfällt bei der **Online-Datensicherung** der Aufwand für den Aufbau und Betrieb einer eigenen Infrastruktur zur Datensicherung bzw. -archivierung. Eigene Mitarbeitende bzw. eigene Hardware ist für diese Zwecke nicht mehr notwendig. Gerade für kleinere bis mittlere Unternehmen ist dies ein gutes Argument für eine Online-Sicherung.

## 5.6 Backup als Cloud-Service

Zahlreiche Unternehmen nutzen die Möglichkeiten des **Cloudcomputings** und lassen ihre Daten durch einen externen Service Provider sichern. Auf diese Weise müssen sie keine(n) eigene(n) Datenserver installieren und betreiben. Bezahlt wird nur der benutzte Speicherplatz beim Service Provider. Dabei werden die Unternehmensdaten so gespeichert und bereitgestellt, als ob der bzw. die Datenserver im eigenen Unternehmen stehen würde(n). Daher braucht das jeweilige Unternehmen auch kein Backup- und Restore-Konzept mehr.

Es gibt verschiedene Möglichkeiten, wie eine Datensicherung ausgeführt werden kann. In der Regel wird die **Art der Datensicherung** durch den Datenumfang und die Grösse des Unternehmens bzw. durch die Betriebsorganisation vorgegeben:

- Beim **Einzelplatz-Backup** wird ein Speichermedium direkt mit dem Computer verbunden und die Daten werden vom Computer direkt auf dieses Medium gesichert.
- Beim **automatischen Backup** steht ein System zur Verfügung, das den Austausch der Medien automatisch vornimmt.
- Beim **LAN-Backup** wird ausgehend vom Server rückwärtig ein zweites, separates Netzwerk aufgebaut, auf dem die Sicherung durchgeführt wird. Dadurch können die Clients und Server im LAN wie gewohnt arbeiten und der Sicherungsrhythmus wird nicht von der Netzwerkbelaestung im LAN bestimmt.
- Beim **Storage Area Network (SAN)** wird über Glasfaserkabel oder iSCSI ein ganzes Speichernetzwerk realisiert.
- Bei der **Online-Datensicherung** werden Daten via Internet transportiert und gesichert.
- Beim **Backup als Cloud-Service** werden die Daten durch einen externen Service Provider gesichert und bei Bedarf zur Verfügung gestellt.

## Repetitionsfragen

- 44 Nennen Sie vier Vorteile eines automatischen Backups gegenüber einem manuellen Backup.
- 50 Weshalb ist ein Einzelplatz-Backup für grosse Unternehmen mit riesigen Datenbeständen nicht geeignet?
- 3 Das komplette Backup- und Restore-Handling kann auch extern vergeben werden. Nennen Sie zwei Gründe, die für diese Möglichkeit sprechen.

## 6 Grosse Datenmengen sichern

Einige Unternehmen haben eine beträchtliche Menge an Daten gesammelt. Die Sicherung aller Daten würde sehr lange dauern und viel Speicherplatz benötigen. Es macht somit keinen Sinn, täglich eine vollständige Datensicherung durchzuführen, da die im Vergleich zur Vorversion geänderten Daten i. d. R. nur einen geringen Prozentsatz des gesamten Datenbestands ausmachen. Sogenannte «ergänzende Backups» dauern nicht so lange, belasten nicht die Performance des Netzwerks und schonen die Hardware.

### 6.1 Voll-Backup ausführen

Bei der vollständigen Datensicherung (**Voll-Backup**) wird der komplette Datenbestand bei jedem Backup-Durchlauf gespeichert.

Vorteil	Nachteil
Alle Daten liegen komplett vor. Sie müssen bei der Wiederherstellung der Dateien nicht lange suchen.	Je nachdem, wie viele Daten Sie speichern, kann die Volldatensicherung sehr zeitaufwendig sein und viel Platz auf dem Speichermedium verbrauchen.

Ein Voll-Backup benötigt zwar viel Speicherplatz, ist aber die notwendige Voraussetzung für eine differenzielle oder eine inkrementelle Datensicherung, die nachfolgend vorgestellt werden.

### 6.2 Differenzielle Datensicherung ausführen

Als Basis für die **differenzielle Datensicherung** wird zuerst ein Voll-Backup durchgeführt. Dies z. B. über das Wochenende. Danach werden bei jeder differenziellen Datensicherung alle Daten gesichert, die sich seit der letzten Volldatensicherung verändert haben. So werden am Montag die Daten gespeichert, die am Montag neu erstellt oder geändert wurden. Am Dienstag werden die Daten gespeichert, die am Montag und am Dienstag neu erstellt oder geändert wurden.

Vorteil	Nachteil
Die Wiederherstellung der Daten ist im Bedarfsfall unkomplizierter und schneller als bei der inkrementellen Datensicherung. Sie müssen lediglich die letzte Volldatensicherung und die aktuelle differenzielle Datensicherung parat haben.	Gegenüber der inkrementellen Datensicherung braucht die Speicherung der Daten mehr Zeit und Platz auf den Speichermedien.

Nachfolgend wird das Funktionsprinzip einer differenziellen Datensicherung dargestellt. Dabei wird ersichtlich, dass der Speicherbedarf täglich ansteigt, weil bei jeder Speicherung alle Daten seit dem letzten Voll-Backup gesichert werden.

#### [6-1] Differenzielle Datensicherung (Funktionsprinzip)

Voll-Backup (Freitag): 

Montag: 

Dienstag: 

Mittwoch: 

Donnerstag: 

Voll-Backup Freitag: 

### 6.3 Inkrementelle Datensicherung ausführen

Auch bei der **inkrementellen Datensicherung** muss zuerst eine Volldatensicherung erstellt werden. Danach werden nur noch die Dateien gesichert, die sich seit der letzten Volldatensicherung bzw. seit der letzten inkrementellen Datensicherung verändert haben. So werden am Montag die Daten gespeichert, die am Montag neu erstellt oder geändert wurden. Am Dienstag werden die Daten gespeichert, die am Dienstag neu erstellt oder geändert wurden.

Vorteil	Nachteil
Sie sparen gegenüber der differenziellen Datensicherung Zeit für die Datensicherung sowie Platz auf den Speichermedien.	Was Sie an der Zeit bei der Datensicherung einsparen, müssen Sie im Zweifelsfall bei der Wiederherstellung der Daten einplanen. Denn im Bedarfsfall müssen Sie zunächst die letzte Volldatensicherung auf das System übertragen. Anschliessend müssen alle nach der Volldatensicherung angefertigten inkrementellen Datensicherungen eingespielt werden.

Nachfolgend wird das Funktionsprinzip einer inkrementellen Datensicherung dargestellt. Dabei wird ersichtlich, dass der Speicherbedarf bzw. die Speichermenge gegenüber einer differenziellen Datensicherung geringer ist, da nur die geänderten Daten gesichert werden.

#### [6-2] Inkrementelle Datensicherung (Funktionsprinzip)

Voll-Backup (Freitag): 

Montag: 

Dienstag: 

Mittwoch: 

Donnerstag: 

Voll-Backup Freitag: 

Der Unterschied zwischen einem differenziellen und einem inkrementellen Backup soll anhand der folgenden **Vergleichstabelle** verdeutlicht werden:

Tag	Was wurde geändert	Differenziell	Inkrementell
Freitag	–	Voll-Backup	Voll-Backup
Montag	Datei1 wurde geändert	Sichern der Datei1	Sichern der Datei1
Dienstag	Datei2 wurde geändert	Sichern der Datei1 und Datei2	Sichern der Datei2
Mittwoch	Datei3 wurde geändert	Sichern der Datei1, Datei2 und Datei3	Sichern der Datei3
Donnerstag	Datei1 wurde nochmals geändert	Sichern der Datei1, Datei2 und Datei3	Sichern der Datei1
...			

Unternehmen haben i. d. R. sehr grosse Datenbestände, die aus technischen und finanziellen Gründen nicht immer mittels **Voll-Backup** gesichert werden können. Beispielweise würde der Voll-Backup aufgrund der grossen Datenmenge länger dauern, als Zeit zur Verfügung steht. Stattdessen können die Daten differenziell oder inkrementell gesichert werden.

Als Basis für eine **differenzielle Datensicherung** dient der Voll-Backup. Danach werden bei jeder differenziellen Datensicherung nur noch diejenigen Daten gesichert, die sich seit der letzten Volldatensicherung geändert haben.

Bei einer **inkrementellen Datensicherung** wird zuerst ebenfalls ein Voll-Backup durchgeführt. Danach werden nur noch diejenigen Dateien gesichert, die sich seit der letzten Voll-datensicherung bzw. seit der letzten inkrementellen Datensicherung geändert haben.

## Repetitionsfragen

- 
- 9 Sie legen viel Wert darauf, Dateien bei Verlust innerhalb kürzester Zeit wiederherzustellen. Nach welchem Wechselschema (differenziell oder inkrementell) organisieren Sie Ihren Backup und warum?
- 
- 15 Warum ist es für Unternehmen mit vielen Daten nicht möglich, nur mit Voll-Backups zu arbeiten?
- 
- 21 In Ihrem Unternehmen sichern Sie die Daten am Freitagabend mittels Voll-Backup. Unter der Woche sichern Sie die Daten inkrementell. Nun stürzte am Mittwochmorgen früh zu Arbeitsbeginn das komplette System ab und die Daten müssen komplett eingespielt werden. Beschreiben Sie Ihr Vorgehen.
-

## 7 Wechselschema anwenden

Die Verwendung eines einzelnen Mediums zur Datensicherung birgt die grosse Gefahr, dass es trotz des Backups früher oder später zu Datenverlusten kommen kann. Allein der Systemabsturz während einer Sicherung kann den einzigen Backup vernichten. Bei der Entwicklung einer Backup-Strategie ist deshalb darauf zu achten, dass der Zugriff auf ältere Versionen der gesicherten Daten jederzeit gewährleistet ist. Immerhin kann eine Datei zum Zeitpunkt der aktuellen Sicherung bereits korrupt oder durch Viren verseucht sein. Um diesen Umständen Rechnung zu tragen, wurden diverse **Wechselschemata** entwickelt. Diese haben den Vorteil, dass auf gesicherte Daten auch noch über einen längeren Zeithorizont zurückgegriffen werden kann. Im Folgenden werden zwei Wechselschemata näher vorgestellt, die problemlos auf die individuellen Bedürfnisse eines Unternehmens zugeschnitten werden können.

### 7.1 Wechselschema «Grossvater-Vater-Sohn»

Ein häufig verwendetes Wechselschema ist das Prinzip «Grossvater-Vater-Sohn». Dieser Plan nutzt täglich ein Set an Speichermedien (Sohn), ein wöchentliches Set (Vater) und ein monatliches Set (Grossvater).

[7-1] Beispiel für Wechselschema «Grossvater-Vater-Sohn»

Monat						
Sonntag	Montag	Dienstag	Mittwoch	Donnerstag	Freitag	Samstag
			1 Inkrementell Sohn Mittwoch	2 Inkrementell Sohn Donnerstag	3 Vollsicherung Vater Woche 1	4
5	6 Inkrementell Sohn Montag	7 Inkrementell Sohn Dienstag	8 Inkrementell Sohn Mittwoch	9 Inkrementell Sohn Donnerstag	10 Vollsicherung Vater Woche 2	11
12	13 Inkrementell Sohn Montag	14 Inkrementell Sohn Dienstag	15 Inkrementell Sohn Mittwoch	16 Inkrementell Sohn Donnerstag	17 Vollsicherung Vater Woche 3	18
19	20 Inkrementell Sohn Montag	21 Inkrementell Sohn Dienstag	22 Inkrementell Sohn Mittwoch	23 Inkrementell Sohn Donnerstag	24 Vollsicherung Vater Woche 4	25
26	27 Inkrementell Sohn Montag	28 Inkrementell Sohn Dienstag	29 Inkrementell Sohn Mittwoch	30 Inkrementell Sohn Donnerstag	31 Vollsicherung Vater Woche 5 + Grossvater Monat 1	

Im obigen Wechselschema werden vier Medien jeweils mit den Tagen gekennzeichnet, an denen eine Datensicherung läuft (Montag, Dienstag, Mittwoch und Donnerstag). Typischerweise wird innerhalb dieser Gruppen eine inkrementelle oder eine differenzielle Datensicherung gefahren. Die Sohn-Speichermedien werden in jeder Woche an den dafür gekennzeichneten Tagen wieder benutzt und bleiben somit für eine Woche bestehen.

Ein Satz «Vater» mit bis zu fünf Wochensets wird mit Woche 1, Woche 2, Woche 3, Woche 4 und Woche 5 beschriftet. Wöchentlich wird eine vollständige Vater-Datensicherung durchgeführt. Dies geschieht an einem Tag, an dem kein «Sohn-Backup» läuft. In diesem Beispiel der Freitag. Die Speichermedien «Vater» werden nach einem Monat wieder benutzt.

Schliesslich werden Grossvater-Speichermedien als Monatssets mit Monat 1, Monat 2 bis Monat 12 gekennzeichnet. Diese Speichermedien werden i. d. R. für ein Voll-Backup am letzten Geschäftstag des Monats benutzt. Die entsprechenden Bänder werden einmal pro Jahr überschrieben. Das bedeutet konkret für eine Fünftagewoche:

- Für die ersten vier Werkstage werden die Sohn-Bänder eingesetzt.
- Am letzten Werktag wird ein Vater-Band eingesetzt.
- An jedem Freitag (also vier Mal im Monat) wird das Vater-Band eingesetzt.
- Am letzten Tag des Monats wird jeweils ein Grossvater-Band eingesetzt.

Dadurch ergibt sich durch Rotation ein folgerichtiges Sicherungsprinzip, da einzelne Daten rückwirkend bis zu einem Jahr wiederhergestellt werden können.

## 7.2 Wechselschema «Turm von Hanoi»

---

Um einen Kompromiss zwischen der Anzahl der vorgehaltenen Datensicherungen und der zur Verfügung zu stellenden Hardware zu erreichen, wird oft das Wechselschema «Turm von Hanoi» verwendet. Bei diesem Verfahren werden unterschiedliche Speichermedien nach vorher festgelegten Tagen eingesetzt.

### Beispiel

- Das erste Medium wird jeden zweiten Tag (1, 3, 5, 7, 9, ...) verwendet.
- Das zweite Medium wird jeden vierten Tag (2, 6, 10, ...) verwendet.
- Das dritte Medium wird jeden achten Tag (4, 12, 20, ...) verwendet.

Mit n Speichermedien kann man somit  $2^{n-1}$  Tage auskommen, bis das letzte Medium überschrieben worden ist. Somit hat man bei 3 Medien noch Backups von vor 4 Tagen, am 5. Tag wird der Backup C überschrieben. Bei 4 Medien hat man 8 Tage, bis am 9. Tag Medium D überschrieben wird, und bei 5 Medien hat man 16 Tage, bis am 17. das Medium E überschrieben wird, usw. Mit jedem zusätzlichen Set verdoppelt sich also der Zeitraum einer möglichen Rücksicherung von Daten. Die Sets A und B umfassen die aktuellen Sicherungskopien. Entsprechend findet man auf D und E weiter zurückliegende Sicherungen. Bei welchen Sets eine Vollsicherung stattfindet, liegt im Ermessen vom Backup-Verantwortlichen.

In der folgenden Beispieldiagramm wird ein Set mit fünf Speichermedien zusammengestellt. Jedes Set enthält Speicherplatz, um die zu sichernde Datenmenge aufzunehmen. Der Ablauf des Wechselgeschehens ist nun wie folgt.

[7-2] Beispiel für Wechselschema «Turm von Hanoi»

Monat						
Sonntag	Montag	Dienstag	Mittwoch	Donnerstag	Freitag	Samstag
			1 Set A	2 Set B	3 Set A	4 Set C
5 Set A	6 Set B	7 Set A	8 Set D	9 Set A	10 Set B	11 Set A
12 Set C	13 Set A	14 Set B	15 Set A	16 Set E	17 Set A	18 Set B
19 Set A	20 Set C	21 Set A	22 Set B	23 Set A	24 Set D	25 Set A
26 Set B	27 Set A	28 Set C	29 Set A	30 Set B	31 Set A	

Erläuterungen zum obigen Wechselschema:

- Begonnen wird am Tag 1 mit dem Set A. Das Set A wird dann periodisch jeden 2. Tag eingesetzt.
- Am Tag 2 wird Set B benutzt. Ab dem 6. Tag wiederholt sich der Einsatz vom Set B alle 4 Tage.
- Am Tag 4 wird zum ersten Mal das Set C benutzt. Dessen Einsatz wiederholt sich alle 8 Tage.
- Am Tag 8 beginnt der Lebenszyklus des Sets D.
- Alle 16 Tage wird Set D verwendet. Zusätzlich wird ein Set E im Wechsel zu D benutzt.

Damit auf Datensicherungen möglichst lange zurückgegriffen werden kann, werden häufig folgende **Wechselschemata** eingesetzt.

- **Grossvater-Vater-Sohn:** Bei diesem Verfahren wird ein tägliches Set (Sohn), ein wöchentliches Set (Vater) und ein monatliches Set (Grossvater) an Speichermedien eingesetzt. So steht jederzeit eine Datensicherung zur Verfügung, die über ein Jahr zurückreicht.
- **Turm von Hanoi:** Dieses Verfahren wird verwendet, um einen guten Kompromiss zwischen der Anzahl der vorgehaltenen Datensicherungen und der zur Verfügung zu stellenden Hardware zu erreichen. Mit n Speichermedien kann man dabei  $2^{n-1}$  Tage auskommen, bis das letzte Medium überschrieben wird. Somit hat man bei 3 Medien noch Backups von vor 4 Tagen, am 5. Tag wird der Backup C überschrieben. Bei 4 Medien hat man 8 Tage, bis am 9. Tag Medium D überschrieben wird, und bei 5 Medien hat man 16 Tage, bis am 17. das Medium E überschrieben wird, usw. Mit jedem zusätzlichen Set verdoppelt sich also der Zeitraum einer möglichen Rücksicherung von Daten.

## Repetitionsfragen

---

- 27** Sie arbeiten mit dem Wechselschema «Grossvater-Vater-Sohn». Ein Mitarbeiter möchte einen Restore von einer Word-Datei mit dem Stand vor 3 Monaten. Ab welchem Band (Grossvater, Vater oder Sohn) müssen die Daten zurückgeholt werden? Begründen Sie kurz Ihre Antwort.
- 
- 33** Was ist der Hauptzweck eines Wechselschemas für Datensicherungen?
- 
- 39** Sie setzen bei Ihnen das Wechselschema «Turm von Hanoi» mit 6 Medien ein. Nach wie vielen Tagen werden die Bänder jeweils wieder überschrieben?
-

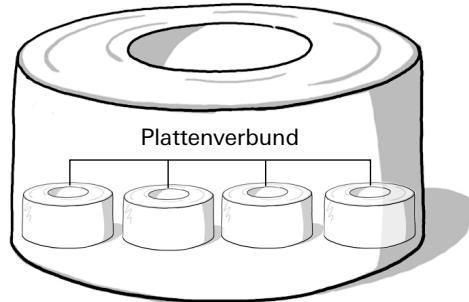
## 8 Daten während des Systembetriebs sichern

Wenn Sie auf Ihrem Computer arbeiten, speichern Sie automatisch Ihre Daten auf Ihrer lokalen Festplatte oder auf einer Festplatte im Netzwerk. In der Nacht werden diese Daten i. d. R. mittels Backup gesichert. Was passiert nun aber, wenn Ihre Festplatte tagsüber einen technischen Defekt hat oder der Strom ausfällt? In solchen Fällen wären die Daten, die Sie seit dem letzten Backup erstellt haben, verloren. Eine mögliche Lösung, dieses Risiko zu minimieren, besteht im Einsatz von RAID-Systemen zur Datenspeicherung.

### 8.1 RAID einsetzen

**RAID (Redundant Array of Independent Disks)** sind mehrere unabhängige Festplatten, die zu einem logischen Laufwerk verbunden werden. Die Daten werden redundant gespeichert, d. h., sie werden so gespeichert, dass sie bei einem Hardwarefehler wiederhergestellt werden können. Die Benutzer greifen nun nicht mehr auf die einzelnen Festplatten zu, sondern auf das logische Laufwerk, das eine virtuelle Festplatte darstellt. Fällt eine Festplatte in diesem Verbund aus, werden die verlorenen Daten mittels der doppelt gespeicherten Daten der noch funktionierenden Festplatten rekonstruiert. Das Ziel von RAID ist die Erhöhung der Verfügbarkeit. Allerdings kann RAID keine Daten wiederherstellen, die von den Benutzern gelöscht oder durch ein Ereignis wie Viren, Diebstahl oder Feuer zerstört wurden. Deshalb benötigt man immer auch einen Backup, um das System vor diesen Bedrohungen zu schützen.

[8-1] RAID

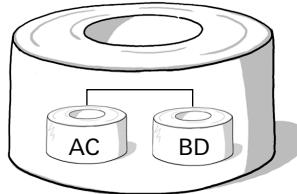


Es existieren verschiedene RAID Levels. Nachfolgend werden die drei wichtigsten RAID Levels näher vorgestellt, nämlich RAID 0, RAID 1 und RAID 5.

#### 8.1.1 RAID 0: Data Striping

Bei RAID 0 handelt es sich noch um keine Massnahme zur Erhöhung der Datenverfügbarkeit. Es ist eine Technik, um die Schreib- und Lesegeschwindigkeit zu steigern. Die Nutzdaten werden in kleine Blöcke aufgeteilt und abwechselnd auf die verschiedenen Platten verteilt. Damit kann auf zwei oder mehr Festplatten parallel zugegriffen werden. Somit wird die Schreib- und Lesegeschwindigkeit erhöht.

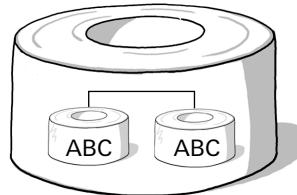
[8-2] Prinzip von RAID 0



### 8.1.2 RAID 1: Drive Mirroring / Drive Duplexing

In einem RAID-1-System werden identische Daten auf zwei Festplatten gespeichert (100% Redundanz). Fällt eine der beiden Festplatten aus, arbeitet das Betriebssystem mit der verbleibenden Festplatte weiter. Obwohl RAID 1 die optimale Ausfallsicherheit bietet, wird RAID 1 meist nur in kleinen Servern eingesetzt, da die doppelte Plattenkapazität notwendig ist.

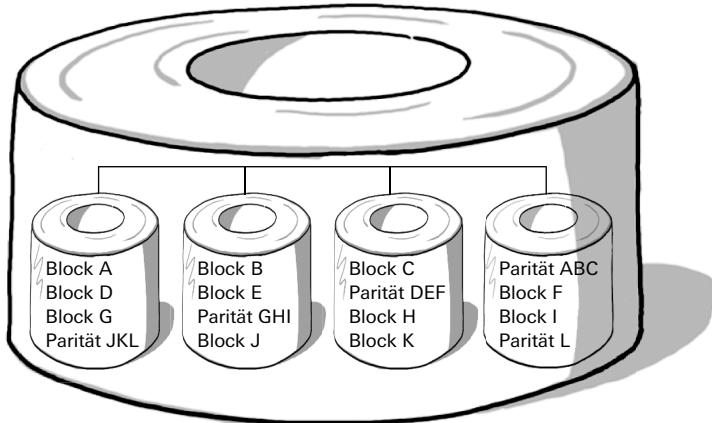
[8-3] Prinzip von RAID 1



### 8.1.3 RAID 5: Block Striping mit verteilter Parity

In einer RAID-5-Konfiguration werden die Daten in einzelne Blöcke aufgeteilt und dann abwechselnd auf die Datenlaufwerke des Plattenverbunds geschrieben (ABC bzw. DEF etc.). Zusätzlich wird nun je ein Paritätsblock gebildet, der abwechselnd auf je einer der Festplatten abgespeichert wird. Mit dieser Paritätsinformation ist es möglich, die verloren gegangenen Daten im Falle eines Festplattenausfalls zu berechnen.

[8-4] Prinzip von RAID 5



## 8.2 USV einsetzen

Bei einem Stromausfall verliert auch das wirksamste Backup-Konzept seinen Nutzen. Zur Behebung dieser Schwachstelle kann eine **unterbruchsfreie Stromversorgung (USV)** eingesetzt werden. Eine USV verhindert zudem folgende Phänomene der Netzspannung:

Begriff	Beschreibung
<b>Spannungsspitze</b>	Ein kurzfristiger Höchststand der durchschnittlichen Netzspannung, der Gerätekomponenten beschädigen oder zerstören kann.
<b>Spannungsseinbruch</b>	Ein kurzfristiger Einbruch der durchschnittlichen Netzspannung. Wird meist durch das Einschalten von Elektrogeräten verursacht.

Zuverlässig funktionierende ICT-Systeme und auch ein zuverlässiges Backup- und Restore-System brauchen eine konstante Stromspannung. Um dies zu gewährleisten, muss innerhalb des Unternehmens eine Lösung gefunden werden. Im Handel werden verschiedene Systeme von USV-Anlagen angeboten. Nachfolgend wird die Funktionsweise der Offline- sowie der Online-USV-Anlage näher erklärt.

### 8.2.1 Offline-USV-Anlagen

Bei einer **Offline-USV** wird die angeschlossene Stromlast im normalen Betrieb direkt vom Netz versorgt. Tritt ein Netzfehler auf, übernimmt nach einer Umschaltzeit von 1 bis 10 Millisekunden eine Batterie mit Wechselrichter die Aufgabe der Stromversorgung. Ein solches Vorgehen wird auch **Mitlaufbetrieb** oder **Standby-USV** genannt, weil die angeschlossenen Geräte den Strom direkt ab Netz beziehen und erst beim Auftreten eines Problems auf die USV umgeschaltet wird. Offline-USV-Anlagen arbeiten also nur bedingt unterbrechungsfrei und filtern Netzstörungen im Normalbetrieb nur unzureichend. Sie sind durch folgende Vor- und Nachteile gekennzeichnet:

Vorteile	Nachteile
Kostengünstiger als Online-USV-Anlagen.	Nur bedingt unterbruchsfreie Stromversorgung.
Ausreichende Leistung für Büro und kommerzielle Umgebung ohne kritische Daten und Systeme.	Im Falle eines Ausfalls ist nur ein begrenzter Zeitraum an Stromversorgung gewährleistet.

### 8.2.2 Online-USV-Anlagen

Das Prinzip der **Online-USV** basiert darauf, dass die Verbraucher den Strom immer direkt ab Wechselrichter beziehen. Die Online-USV-Anlage bezieht dabei den Strom über das Netz und lädt dabei konstant die Batterien auf. Wenn Sie zu Hause an einem am Stromkreis angeschlossenen Notebook mit eingesetzter Batterie arbeiten, haben Sie das gleiche Prinzip. Das Notebook bezieht den Strom ab Batterie. Fällt der Strom aus oder ziehen Sie den Stromstecker raus, läuft das Notebook weiter. Stecken Sie den Stromstecker wieder ein, wird die Batterie wieder geladen. Ein solches Vorgehen wird auch **Dauerbetrieb** genannt, weil die Geräte den Strom über die Online-USV-Anlage beziehen. Diese ist somit dauerhaft in Betrieb. Online-USV-Anlagen bieten eine hohe Sicherheit und sind v. a. bei wichtigen Daten und empfindlichen Systemen zu empfehlen. Sie sind durch folgende Vor- und Nachteile gekennzeichnet:

Vorteil	Nachteil
Sehr hohe Sicherheit.	Teurer als Offline-USV-Anlagen.
Ein Stromausfall hat keinen Einfluss auf die Systeme mehr.	Die Batterie nutzt sich rasch ab und muss von Zeit zu Zeit erneuert werden.

In der Regel wird der Backup in der Nacht ausgeführt. Die Mitarbeiter verändern jedoch konstant die Daten auf den Systemen. Würde nun eine Festplatte während des Tages ausfallen, wären diese auf dem Backup nicht vorhanden. Aus diesem Grunde sollte neben einem Backup- und Restore-Konzept ebenfalls ein **RAID-System** betrieben werden.

**RAID** steht für «Redundant Array of Independent Disks». Es handelt sich dabei also um mehrere unabhängige Festplatten, die zu einem logischen Laufwerk verbunden werden. Die Daten werden dabei **redundant** gespeichert, d.h. so gesichert, dass sie bei einem Hardwarefehler wiederherstellt werden können. Die Benutzer greifen dabei nicht mehr auf einzelne Festplatten zu, sondern auf das logische Laufwerk, das eine virtuelle Festplatte darstellt. Fällt eine Festplatte in diesem Verbund aus, werden die verlorenen Daten mittels der doppelt gespeicherten Daten der noch funktionierenden Festplatten rekonstruiert.

Um Datenverluste aufgrund eines Stromausfalls zu vermeiden, empfiehlt es sich, eine **unterbruchsfreie Stromversorgung (USV)** einzusetzen.

## Repetitionsfragen

- 
- 45 Warum ist RAID 0 nicht für die konstante Datensicherung bei einem Festplattendefekt zu empfehlen?
- 
- 51 Welches ist der wesentliche Vorteil von RAID 5 gegenüber RAID 1?
- 
- 4 Worin besteht der Hauptunterschied zwischen einer Offline-USV-Anlage und einer Online-USV-Anlage?
-



## **Teil C Datensicherungskonzept erstellen**

---

## Einleitung, Lernziele und Schlüsselbegriffe

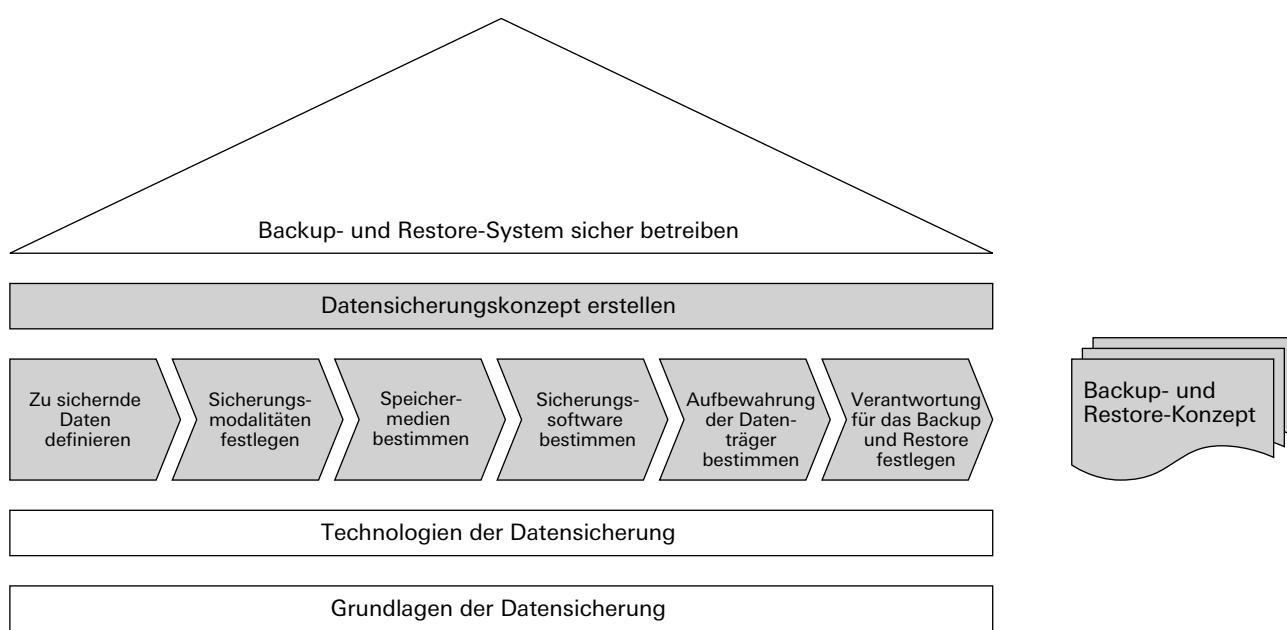
### Einleitung

Beim Entwurf eines Datensicherungskonzepts müssen folgende Aspekte geklärt werden:

- Zu sichernde Daten definieren
- Sicherungsmodalitäten festlegen
- Speichermedien bestimmen
- Sicherungssoftware bestimmen
- Aufbewahrung der Datenträger bestimmen
- Verantwortung für das Backup und Restore festlegen

In diesem Teil des Lehrmittels werden diese Aspekte vertieft und Sie erfahren mehr über die Aufgaben und Arbeiten, die mit dem Entwurf eines Backup- und Restore-Konzepts zusammenhängen. Folgende Grafik zeigt auf, wo Sie sich innerhalb des Lehrmittels befinden:

[8-5] Inhalt von Teil C



## Lernziele und Lernschritte

---

Lernziele	Lernschritte
<input type="checkbox"/> Sie können die für den Backup relevanten Daten erheben und Anforderungen aufnehmen.	Zu sichernde Daten bestimmen
<input type="checkbox"/> Sie können festlegen, wann und wie oft ein Backup durchgeführt wird und wie viele verschiedene Sicherungen aufbewahrt werden.	Sicherungsperiodizitäten festlegen
<input type="checkbox"/> Sie können Bedürfnisse an ein Backup aufnehmen und daraus die sinnvollen Speichermedien festlegen.	Speichermedium bzw. Kombination der Speichermedien festlegen
<input type="checkbox"/> Sie können je nach eingesetztem Betriebssystem die Software für den Backup ausführen.	Sicherungssoftware bestimmen
<input type="checkbox"/> Sie kennen die verschiedenen Aspekte, die bei der Lagerung von Speichermedien beachtet werden müssen.	Lagerort und Lagerungsart festlegen
<input type="checkbox"/> Sie können die verschiedenen Aufgaben innerhalb des Backup- und Restore-Konzepts unterschiedlichen Rollen zuteilen.	Verantwortliche für den Backup zuteilen

## Schlüsselbegriffe

---

Archivierung, Datenart, Datenerhebung, Datenowner, Datenträgerbeschriftung, Datenträgerkontrolle, Datenträgerlagerung, Datenumfang, Datenwachstum, Konfigurationseinstellungen, Lizzenzen, Mehrstufiger Backup, Netzauslastung, Operator, Originaldateien, Periodizität, Schreibschutz, Sicherungsmodalitäten, Sicherungssoftware, Speicherort, Streng vertrauliche Daten, Systemowner, Verfügbarkeit, Zugriffsrechte, Zutrittskontrolle

58

## 9 Zu sichernde Daten bestimmen

Zu Beginn Ihres Backup- und Restore-Konzepts müssen Sie sich einen Überblick über die zu sichernden Daten und deren Umfang machen. Dabei sind die Bedürfnisse der Datenbesitzer aufzunehmen und daraus entsprechende Massnahmen abzuleiten. Die Datenaufnahme gibt Ihnen wichtige Erkenntnisse, welche Daten auf welche Arten gesichert werden müssen.

## 9.1 Datenerhebung

Um Daten in ein Backup- und Restore-Konzept aufnehmen zu können, muss vorerst bekannt sein, wo sich die Daten zurzeit befinden (Speicherort), wie umfangreich diese sind und allenfalls wie sich die Datenmenge entwickeln wird.

«Datei-Leichen» können mit Regeln und Kommunikation minimiert werden: Es gibt Unternehmen, die für Dateien respektive Verzeichnisse ein **Haltbarkeits- oder Verfallsdatum** verlangen. Dateien, die dieses Datum überschreiten, werden (bei Bedarf an Speicherplatz) gelöscht. So können z.B. umfangreiche, «alte» Verkaufspräsentationen automatisch gelöscht werden. Ebenfalls von Bedeutung ist, ob es sich um Dateien, Programme oder um Konfigurationen handelt (siehe Kap. 2.1, S. 20).

Um diese Informationen festzuhalten, entwerfen Sie am einfachsten ein **Datenerhebungsformular**, mit dem Sie systematisch die verschiedenen Datenbesitzer anfragen können. Ein solches Formular kann beispielsweise wie folgt aufgebaut werden:

## [9-1] Formular für die Datenerhebung (Beispiel)

Daten						
Nr.	Speicherort	Daten	Verfügbarkeits- anforderungen / Res- tore innerhalb von:	Heutige Grösse	Wachstum / Veränderung pro Jahr	Archivierung
1			<input type="checkbox"/> Immer verfügbar <input type="checkbox"/> 2–4 h <input type="checkbox"/> 1 Tag <input type="checkbox"/> 2 Tage			<input type="checkbox"/> Nein <input type="checkbox"/> Ja, Dauer ..... Jahre
2			<input type="checkbox"/> Immer verfügbar <input type="checkbox"/> 2–4 h <input type="checkbox"/> 1 Tag <input type="checkbox"/> 2 Tage			<input type="checkbox"/> Nein <input type="checkbox"/> Ja, Dauer ..... Jahre
3			<input type="checkbox"/> Immer verfügbar <input type="checkbox"/> 2–4 h <input type="checkbox"/> 1 Tag <input type="checkbox"/> 2 Tage			<input type="checkbox"/> Nein <input type="checkbox"/> Ja, Dauer ..... Jahre
4			<input type="checkbox"/> Immer verfügbar <input type="checkbox"/> 2–4 h <input type="checkbox"/> 1 Tag <input type="checkbox"/> 2 Tage			<input type="checkbox"/> Nein <input type="checkbox"/> Ja, Dauer ..... Jahre
...			<input type="checkbox"/> Immer verfügbar <input type="checkbox"/> 2–4 h <input type="checkbox"/> 1 Tag <input type="checkbox"/> 2 Tage			<input type="checkbox"/> Nein <input type="checkbox"/> Ja, Dauer ..... Jahre

<b>Programme</b>		
Programm	Original und Lizenz	Falls ja: Wo sind die Datenträger zurzeit gelagert? Falls nein: Wo sind die Programme zurzeit gespeichert?
Betriebssystem	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Office-Werkzeuge	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
...	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
<b>Konfigurationen</b>		
Konfiguration für	Erwünscht	Falls erwünscht: Wo gespeichert?
Betriebssystem	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Office-Werkzeuge	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Browser	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Mail	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
...	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	

Durch das Ausfüllen dieses Formulars gewinnen Sie folgende **Informationen**, die Sie für das Backup- und Restore-Konzept benötigen.

Inhalt	Beschreibung
<b>Speicherort</b>	Hier wird festgehalten, auf welchem Server, auf welchem Laufwerk und in welchem Verzeichnis die Daten zu finden sind.
<b>Datenart</b>	Hier wird festgehalten, um welche Art von Daten es sich handelt. Falls nicht alle Dateien in diesem Ordner gespeichert werden müssen, sind die zu sichernden Dateien aufzulisten.
<b>Verfügbarkeit und Restore innert</b>	Hier wird festgehalten, wie rasch die Daten im Falle eines Verlusts wieder verfügbar sein müssen. Je nach Dauer sind verschiedene Massnahmen zu treffen.
<b>Datenumfang und Datenwachstum</b>	Hier wird festgehalten, wie umfangreich der Datenbestand ist und mit welchem Zuwachs an Daten gerechnet wird. Aufgrund dieser Information können gezielt Speichermedien mit ausreichender Kapazität gewählt werden.
<b>Archivierung</b>	Hier wird festgehalten, ob die Daten archiviert werden müssen. Eine Datenarchivierung hat ebenfalls einen Einfluss auf die Wahl des Speichermediums. Denn nicht alle Speichermedien sind für eine lange Archivierung geeignet.
<b>Originaldateien und Lizzen</b>	In den meisten Fällen sind für Programme die Originale sowie Lizizen vorhanden. Somit können diese Programme bei einem Computerabsturz einfach wieder installiert werden. Dieses Vorgehen hat den Vorteil, dass Programme nicht speziell gesichert werden müssen. Dennoch benötigt eine Installation i. d. R. viel Zeit. Darum besteht die Möglichkeit, ganze Kopien von Festplatten zu erstellen, die bei Bedarf rasch wieder zurückgespielt werden können.
<b>Konfigurations-einstellungen</b>	Benutzer stellen ihr Betriebssystem sowie ihre Programme nach ihren Bedürfnissen ein. Viele Benutzer benötigten dafür viel Zeit und haben sich derart an diese Einstellungen gewöhnt, dass es viel Zeit kosten würde, diese neu zu erstellen. Aus diesem Grunde werden i. d. R. die Konfigurationen auch zentral auf Servern gespeichert.

## 9.2 Umgang mit streng vertraulichen Daten

---

In manchen Abteilungen werden Daten erfasst und bearbeitet, die streng vertraulich sind. Zum Beispiel sind in der Personalabteilung Informationen über die Gehälter aller Mitarbeitenden vorhanden. Diese Daten werden i. d. R. auf speziellen Servern verwaltet, auf die lediglich bestimmte Mitarbeitende Zugriff haben. Alle Schutzmassnahmen helfen nichts, wenn die Daten mittels Backup anschliessend für alle offenliegen.

Um **streng vertrauliche Daten** trotzdem in ein Sicherheitskonzept zu integrieren, müssen die gleichen Sicherheitsregeln auch für die Daten auf den Speichermedien gelten. Zusätzlich besteht die Möglichkeit, diese verschlüsselt zu speichern. Es ist wichtig, dass vertrauliche Daten vertraulich bleiben. Jede Sicherheitsmaßnahme verursacht Arbeit. Es ist deshalb ebenso ratsam, nicht vertrauliche Daten möglichst global zu administrieren, um den Verwaltungsaufwand in bezahlbaren Grenzen zu halten.

## 9.3 Hilfsmittel

---

Die Aufnahme der Daten ist eine aufwendige Angelegenheit. Beim Backup und v. a. bei der Archivierung reicht es nicht aus, nur die Informationen vom Server und Ordner zu haben. Vielmehr müssen detaillierte Informationen wie Name, Erstelldatum, Inhalt etc. über die Dateien enthalten sein. Unternehmen haben i. d. R. Tausende von Dateien. Eine manuelle Aufnahme wäre dementsprechend sehr zeitaufwendig. Aus diesem Grunde gibt es Software, die Sie bei der Registrierung der Dateien unterstützt. Eine saubere Registrierung hilft Ihnen, den Überblick zu bewahren und jederzeit mittels Stichwörtern Dateien zu suchen.

### ▷ Hinweis

Unter «nützliche Links zum Thema» finden Sie Anbieter solcher Tools zur Auflistung von Verzeichnissen und deren Inhalten. (Vgl. S. 10)

## 9.4 Reihenfolge der Wiederherstellung

---

Bereits bei der Aufnahme der Daten ist es von Vorteil, wenn Sie sich Gedanken machen, in welcher Reihenfolge die Programme, Konfigurationen und Dateien im Falle eines Datenverlusts wiederhergestellt werden müssen. Im Notfall können Sie sich auf die Wiederherstellung konzentrieren und müssen sich nicht erst Gedanken über die Priorität machen. Sie gewinnen so wertvolle Zeit. In vielen Fällen sind Sie bei der Reihenfolge an technische oder logische Gegebenheiten gebunden. So können Sie z. B. die Konfiguration vom Betriebssystem erst nach der vollständigen Installation vom Betriebssystem vornehmen.

Bei den Dateien ist es sinnvoll, die Reihenfolge zu bestimmen, in der diese im Falle eines Totalabsturzes wiederhergestellt werden müssen. Die Reihenfolge wird im Notfallhandbuch dokumentiert (Kap. 15.1, S. 81). Damit kann die Geschäftsleitung die Strategie der Wiederherstellung (schon heute) erkennen und bei Bedarf ändern.

Für die Erstellung eines Datensicherungskonzepts muss zuerst bestimmt werden, welche Daten gesichert werden müssen. Dabei ist zu klären, wo sich die jeweiligen Daten befinden (**Speicherort**), wie umfangreich sie sind und wie sich der Datenbestand in absehbarer Zukunft voraussichtlich entwickelt. Um an diese Informationen zu gelangen, empfiehlt es sich, ein **Erhebungsfomular** einzusetzen. Zur Vereinfachung der Datenerhebung stehen auch geeignete **Tools** zur Verfügung. Zudem lohnt es sich, die **Prioritäten des Restores** bereits in dieser Phase zu klären. Im Notfall kann man sich dann auf die rasche Wiederherstellung der Daten konzentrieren und muss sich nicht Gedanken darüber machen, welche Programme, Konfigurationen und Dateien in welcher Reihenfolge wiederhergestellt werden müssen.

## Repetitionsfragen

- 
- 10** Welchen Vorteil haben Sie, wenn Sie sich bereits bei der Aufnahme der Daten über die Reihenfolge der Wiederherstellung Gedanken machen?
- 
- 16** Nach dem vollständigen Ausfüllen des Datenaufnahmeformulars können Sie z. B. die aktuelle Speichermenge sowie die Veränderung pro Jahr berechnen. Welche weiteren Informationen können Sie aus den Inhalten des Formulars ableiten?
- 
- 22** Worauf müssen Sie bei streng vertraulichen Daten beim Backup achten?
-

## 10 Sicherungsmodalitäten festlegen

---

Bei dieser Aufgabe geht es darum, festzulegen, wann (z. B. tagsüber, in der Nacht), wie oft (z. B. stündlich, täglich, wöchentlich) ein Backup ausgeführt werden muss und wie viele Sicherungen aufbewahrt werden sollen.

### 10.1 Zeitpunkt des Backups bestimmen

---

Zunächst müssen Sie festlegen, wann der beste Zeitpunkt für den Backup ist. Die Rahmenbedingungen, die beim Zeitpunkt für den Backup beachtet werden müssen, sind Arbeitszeiten, Netzauslastung und Sicherungsbedarf.

#### 10.1.1 Arbeitszeiten

---

Während der Bürozeiten arbeiten die Mitarbeitenden und verändern konstant den Datenbestand. Es werden neue Dateien erstellt, mutiert und gelöscht. Somit wäre es am besten, wenn der Backup nach der Arbeitszeit wäre, also in der Nacht.

#### 10.1.2 Netzauslastung

---

Durch die Arbeit der Mitarbeitenden wird das Netz bereits belastet. Würde nun ebenfalls gleichzeitig der Backup ausgeführt, käme es zu einer erhöhten Netzauslastung. Daher ist es aus Sicht der Netzauslastung ebenfalls sinnvoll, den Backup in die Nacht zu verschieben. Jedoch ist zu beachten, dass in der Nacht bereits andere Arbeiten geplant sind, z. B. die Tagesendverarbeitung, Ladung und Aufbereiten der Daten für das Data Warehouse etc. Diese Services sind bei der zeitlichen Backup-Planung ebenfalls zu beachten.

#### 10.1.3 Sicherungsbedarf

---

Bei den Arbeitszeiten und der Netzauslastung ist es sinnvoll, den Backup auf die Nacht zu verschieben. Dies würde jedoch bedeuten, dass bei einem Ausfall die während des Tages neu erstellten bzw. mutierten Daten nicht in den Backup einfließen könnten. Bei einem sehr hohen Sicherungsbedarf ist es daher sinnvoll, auch mehr als einen Backup auszuführen oder ergänzende Sicherungen zu planen (siehe Kap. 8, S. 50).

### 10.2 Periodizität des Backups bestimmen

---

Bei der Bestimmung der **Periodizität** geht es darum das «wie oft» festzulegen. Oftmals reicht es aus, wenn einmal pro Nacht die Sicherung läuft. Weniger oft ist gefährlich und nicht zu empfehlen. Mehr Sicherungen durchzuführen erhöhen die Sicherheit, haben aber einen negativen Effekt auf die Netzauslastung sowie auf die Kosten, da mehr Speichermedien, Arbeitszeit etc. benötigt wird. Besonders heikel ist diese Frage bei Datenbanken und Online-Daten, die permanent der Veränderung unterliegen. Hier sollten unbedingt ergänzende Sicherungen (siehe Kap. 8, S. 50) eingeplant werden.

### 10.3 Art und Anzahl der Backups bestimmen

Bei diesem Punkt ist zu klären, wie viele verschiedene Sicherungen aufbewahrt werden sollen, also z. B. nur auf einem Band oder eventuell von diesem Band eine oder weitere Kopien erstellen. Werden z. B. Speichermedien falsch gelagert, können diese kaputtgehen. Da wäre es von Vorteil, wenn weitere Kopien dieses Bands vorhanden wären. Hingegen bedeutet jede weitere Kopie auch weitere Kosten. Daher ist dieser Punkt gut abzuwägen.

Möchte man aus Kostengründen nur eine Sicherung erstellen, sollte zumindest mit einem Wechselschema gearbeitet werden (vgl. Kap. 7, S. 46). Dies gewährleistet, dass Daten wenigstens mehrfach gesichert werden, wenn auch zu unterschiedlichen Zeiten.

Bei der **Festlegung der Sicherungsmodalitäten** geht es darum, folgende Details für den Backup zu bestimmen:

- **Wann?** Hier wird der beste Zeitpunkt für die Datensicherung bestimmt. Aufgrund der Arbeitszeiten und der Netzauslastung empfiehlt es sich, den Zeitpunkt auf die Nacht zu verlegen.
- **Wie oft?** Hier wird die Periodizität der Datensicherung bestimmt. Zu diesem Zweck wird definiert, wie oft der Backup durchgeführt wird (z. B. stündlich, täglich, wöchentlich).
- **Wie viele?** Hier wird bestimmt, wie viele Datensicherungen aufbewahrt werden. Dabei wird festgelegt, wie viele (unterschiedliche oder gleichartige) Speichermedien für eine bestimmte Datensicherung eingesetzt werden.

## Repetitionsfragen

- 28 Warum ist es wenig sinnvoll, tagsüber einen Backup zu machen? Nennen Sie zwei Gründe.
- 34 Wenn der Backup nur in der Nacht durchgeführt wird, können im Falle eines Festplattendefekts die Daten eines ganzen Arbeitstags verloren gehen. Was schlagen Sie als Gegenmassnahme vor?
- 40 Wenn von den gleichen Daten mehr als eine Sicherung aufbewahrt werden, erhöht sich automatisch die Datensicherheit. Welcher Aspekt spricht jedoch gegen allzu viele Sicherungen?

## 11 Speichermedien bestimmen

Sie haben bereits die wichtigsten Speichermedien kennengelernt (vgl. Kap. 3, S. 24) und wissen auch, welche Speichermedien sich im Allgemeinen für welche Zwecke eignen (vgl. Kap. 4, S. 32). Die Auswahl ist von den konkreten Bedürfnissen des Unternehmens abhängig. Kein Speichermedium weist nur Vorteile auf und erfüllt alle Kriterien des Datensicherungskonzepts. Es gilt daher, die Vor- und Nachteile der einzelnen Speichermedien sorgfältig abzuwägen. Eine Kombination von verschiedenen Speichermedien ist oft eine gute und in der Praxis weitverbreitete Möglichkeit.

### 11.1 Technische Aspekte beachten

Grundsätzlich steht jedes Unternehmen vor denselben Herausforderungen:

- Der Backup muss **rasch** ausgeführt werden. Verlorene Daten sollen so rasch wie möglich wiederhergestellt werden.
- Der Backup muss **sicher** sein. Von Vorteil ist eine Auslagerung der Daten an einen Drittstandort. So ist man im Falle von Feuer, Wasser etc. ausreichend geschützt.

Um diese Herausforderungen zu meistern, empfiehlt sich eine Kombination aus Festplatte und Magnetbändern.

Festplatten	Magnetbänder
Die Preise für Festplatten sind so weit gesunken, dass sie mit Bandlaufwerken problemlos konkurrieren können. Es macht also durchaus Sinn, Festplatten als Speichermedium in Betracht zu ziehen. Der Datendurchsatz bei einer Festplatte ist deutlich höher als bei einem Bandlaufwerk, Spulenzeiten gibt es keine. Auch bei einem Restore kann direkt auf die gewünschten Daten zugegriffen werden.	Punkto Mobilität sind die Bänder den Festplatten eindeutig überlegen. Soll also der Backup in einen feuerfesten Tresor eingeschlossen werden, so ist es sicher besser, diese Daten auf Bänder zu schreiben. Sollen Backups langfristig archiviert werden, ist nach wie vor das Band vorzuziehen.

Das Festplatten-Backup ist ein Element eines mehrstufigen Backup-Konzepts und bildet dort die erste Stufe. Es besticht durch die hohe Geschwindigkeit sowohl der Sicherungs- als auch v. a. der Restore-Zeit. Für eine langfristige Archivierung dagegen empfiehlt sich das Magnetband. Die Kombination von beidem, sinnvoll eingesetzt, vereinigt die Geschwindigkeit der Festplatte mit der Langlebigkeit des Bandmediums.

### 11.2 Betriebswirtschaftliche Aspekte beachten

Bei der Berechnung der Kosten für ein Backup- und Restore-System müssen einmalige und wiederkehrende Kosten berücksichtigt werden:

- **Einmalige Kosten** sind Kosten, die einmalig anfallen und nur einmalig zu bezahlen sind. Beispielsweise der Kauf einer Festplatte zu Backup-Zwecken.
- **Wiederkehrende Kosten** sind Kosten, die laufend erneut anfallen. Beispielsweise die Arbeitszeit eines Mitarbeiters, der Bänder manuell auswechseln muss.

Ein automatisiertes Backup- und Restore-System kostet in der Anschaffung meistens mehr als ein System, bei dem manuelle Eingriffe notwendig sind. Dieses verursacht jedoch mehr Betriebskosten.

**Beispiel**

Anstatt einer Kombination von Festplatte und Magnetbändern (Autoloadern) könnte die gleiche Datenmenge auch auf CD mit einem einfachen CD-Brenner erledigt werden. Der CD-Brenner wird dabei erheblich billiger sein.

Neben den **Beschaffungskosten** sind daher auch für jedes System die **Betriebskosten** zu ermitteln, d. h. wie viel Aufwand und Kosten der Systembetrieb verursacht.

[11-1] Gegenüberstellung Kosten (Beispiel)

Was	Manuelles System	Automatisiertes System
Anschaffung der Geräte	200.00	4 000.00
Benötigte Zeit für Backup pro Jahr	10 000.00 (rund 10 Stunden pro Woche <sup>[1]</sup> )	2 000.00 (rund 2 Stunden pro Woche <sup>[1]</sup> )
Benötigte Zeit für Restore pro Jahr	4 000.00 (rund 4 Stunden pro Woche <sup>[1]</sup> )	1 000.00 (rund 1 Stunde pro Woche <sup>[1]</sup> )
Totalkosten pro Jahr	14 200.00	7 000.00

[1] Stunde wurde mit CHF 20.– berechnet.

Alternativ zu einem eigenen Backup- und Restore-System kann die Datensicherung auch ausgelagert und extern abgewickelt werden (Outsourcing, siehe Kap. 5.5, S. 41).

### 11.3 Ablauf eines mehrstufigen Backups

Ein KMU entscheidet sich unter Beachtung von technischen und betriebswirtschaftlichen Aspekten für einen **mehrstufigen Backup**, der folgende Stufen umfasst.

- **Stufe 1:** Netzwerkspeicher (NAS)
- **Stufe 2:** Autoloader mit Magnetbändern

Der regelmässige Ablauf des Backups ergibt sich dann wie folgt:

- Täglicher inkrementeller Backup aller Daten auf die Festplatte des NAS.
- Der NAS kann aus den inkrementellen Sicherungen und dem bisherigen Voll-Backup eine neue Vollsicherung errechnen.
- Der wöchentliche und monatliche Voll-Backup sowie die täglichen inkrementellen Sicherungen werden vom NAS auf das Bandmagazin geschrieben. Dies geschieht im Hintergrund und ohne Netzwerkbelastung. Die Bänder werden als Sicherung der zweiten Stufe eingesetzt und an sicheren Orten ausgelagert.

Nachfolgend sehen Sie beispielhaft den Ablauf eines 4-stufigen Backups für eine aktuell bestehende Datenmenge von 31 GByte und ein angenommenes Datenwachstum von 7 GByte pro Jahr:

Nr.	Phase	Aktion	Zeit	Datenweg	Beteiligte Rechner	Beteiligte Medien	
						Festplatte	Band
1	<b>Backup auf NAS-Server</b>	Inkrementeller Backup aller Systeme	Nachts	Netzwerk	NAS-Backup-Server, alle Clients	X	
2	<b>Konsolidierung</b>	Berechnung des neuen Voll-Backups	Tagsüber	Lokal auf Backup-Server	Nur Backup-Server	X	
3	<b>Sekundär-Backup</b>	Speicherung der inkrementellen täglichen Daten oder des wöchentlichen / monatlichen Voll-Backups auf die Bänder	Tagsüber	Lokal auf Backup-Server	Nur Backup-Server	X	X
4	<b>Auslagerung wöchentlicher und monatlicher Voll-Backup</b>	Entfernung Bänder und Auslagerung an einen separaten Ort	Wöchentliches und monatliches bzw. jährliches Archivband	Manuell	–		X

Mit dieser Lösung wurden alle Entscheidungskriterien berücksichtigt.

Einflussfaktor	Beschreibung
<b>Datenmenge</b>	Die Datenmenge von 31 GByte sowie die Wachstumsmenge von 7 GByte pro Jahr sind für die gewählten Medien Festplatte und Bänder kein Problem.
<b>Speicherdauer</b>	Dadurch, dass lediglich die Differenzen täglich inkrementell transferiert werden müssen, ist die Speicherung rasch ausgeführt.
<b>Wiederherstellungs-dauer</b>	Auf dem Server sind die Daten jederzeit vorhanden und können rasch wiederhergestellt werden. Direkter Zugriff ist möglich. Müssen Daten von früheren Zeitpunkten hergestellt werden, können diese automatisch ab Autoloader innerhalb einer Woche zurückgespielt werden.
<b>Kosten</b>	Die Kosten für die Anschaffung der NAS-Server sowie des Autoloaders sind einzukalkulieren. Aufgrund der automatischen Verarbeitung und der geringen Netzbelastrung macht sich diese Investition aber bezahlt.
<b>Technikwechsel</b>	Bei der gewählten Technologie wird auf Neues und Bewährtes gesetzt.
<b>Haltbarkeit</b>	Bänder werden seit Jahren als Archivmedien benutzt und haben sich bewährt.
<b>Erweiterbarkeit</b>	NAS und Bänder können unabhängig erweitert werden. Bei der Anzahl an Daten ist dies jedoch kein Problem.

Jedes Speichermedium hat **spezifische Vor- und Nachteile**. Magnetbänder erlauben z. B. lange Aufbewahrungszeiten, weisen allerdings langsame Zugriffszeiten auf. Festplatten, die in ein Netzwerk eingebaut sind, garantieren zwar einen raschen Backup und einen effizienten Restore, lassen sich aber nicht sehr einfach sicher auslagern (und z. B. in einem feuerfesten Tresor einschliessen).

Ein **mehrstufiger Backup**, d. h. der Einsatz mehrerer Speichermedien, ist daher in vielen Fällen die beste Lösung. In der Praxis wird oftmals eine Kombination von Festplatten und Magnetbändern eingesetzt.

## Repetitionsfragen

- 
- 46 Warum empfiehlt es sich, verschiedene Speichermedien für einen Backup einzusetzen?
- 
- 52 Warum müssen neben den reinen Anschaffungskosten auch die Arbeitszeitkosten berechnet werden?
- 
- 5 Festplatten setzen sich als Backup-Medium immer mehr durch. Da die Festplatten i. d. R. mit dem Netzwerk verbunden sind, kann ein Restore rasch durchgeführt werden. Die Speichergeschwindigkeit ist sehr schnell und die Kosten sind eher günstig. Was spricht dagegen, nur Festplatten als Backup-Medium zu verwenden?
-

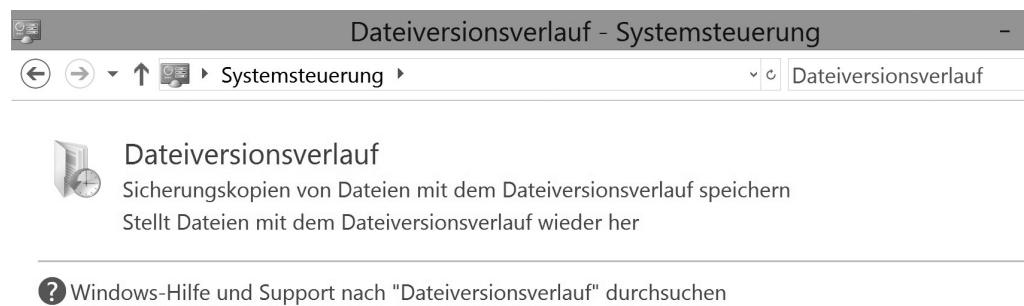
## 12 Sicherungssoftware bestimmen

Wenn Sie Ihre Datensicherung ausführen wollen, brauchen Sie neben den Speichermedien die passende Software dazu. Im Lieferumfang der Betriebssysteme, wie z. B. Windows, befinden sich Datensicherungstools. Daneben werden aber auch kommerzielle Sicherungsprogramme angeboten. Nachfolgend erhalten Sie einen Einblick in die Datensicherung unter Windows 8.1 sowie Standard-Unix-Tools. Zusätzlich werden kommerzielle Sicherungsprogramme vorgestellt.

### 12.1 Datensicherung unter Windows-Systemen

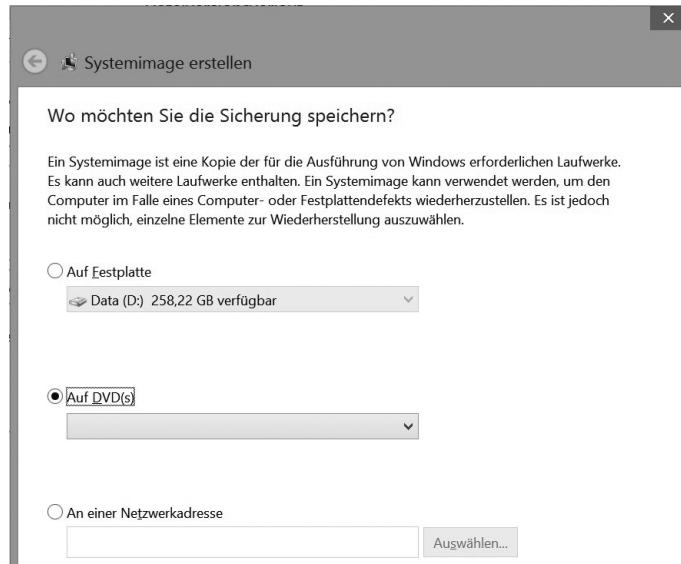
Praktisch jede Windows-Version verfügt über Hilfsmittel zur Sicherung von Daten. Diese sind i. d. R. über die Systemsteuerung aufrufbar. In diesem Abschnitt wird Ihnen aufgezeigt, wie mithilfe von Windows 8.1 ein Image, also ein System-Backup der kompletten Betriebssystem-Partition mitsamt allen Einstellungen, durchgeführt wird. Starten Sie die Systemsteuerung und tippen Sie rechts oben im Suchfeld den Begriff «Dateiversionsverlauf» ein, bestätigen Sie den einzigen Treffer.

[12-1] Dateiversionsverlauf



Ganz links unten erscheint die Funktion «Systemabbildsicherung», die Sie bitte mit der Maus auswählen. Es dauert nun einen Augenblick, während Windows nach geeigneten Sicherungsgeräten sucht. Ideal als Speichermedium eignet sich eine externe Festplatte. Nach Auswahl des Speicherziels klicken Sie auf «Weiter · Sicherung starten», um das System-Backup zu erstellen.

## [12-2] Systemabbildsicherung



Unter «Erweiterte Einstellungen» kann zudem eingestellt werden, wie oft und wie lange die Daten aufbewahrt werden sollen.

## 12.2 Standard Unix-Tools

Es gibt eine Vielzahl von Unix-Tools zur Speicherung bzw. Backup von Daten. In diesem Lehrmittel beschränken wir uns auf den Befehl `tar`, mit dem Dateien gesichert und wiederhergestellt werden können. Seinen Namen hat dieser Archivierungsbefehl durch die Verwendung von Magnetbändern (engl. tapes) erhalten (tape archiv). Mit `tar` können aber neben Magnetbändern auch alle anderen Speichermedien angesprochen werden. Um eine Sicherungsdatei zu erstellen bzw. zu extrahieren, verwenden Sie folgende Syntax:

```
# tar [Operation] [Optionen] [Zieldatei] [Quellordner oder Datei]
```

Operationen	Bedeutung	Optionen	Bedeutung
c	create: Archiv mit Sicherungsdateien erstellen	f	file: Archiv in einen selbst definierten Dateinamen schreiben bzw. von einem selbst definierten Dateinamen lesen.
x	extract: Sicherungsdateien aus dem Archiv wiederherstellen	v	verbose: in ein Archiv geschriebene Dateien anzeigen
r	append: Sicherungsdateien in ein Archiv einfügen		
t	list: Inhalt von Sicherungsdateien anzeigen		

### ▷ Hinweis

Weitere Operationen und Optionen erhalten Sie durch die Eingabe von `tar --help`.

### 12.2.1 Archiv erstellen

Um ein Sicherungsarchiv zu erzeugen, müssen Sie die Operation `c` verwenden. Sollen die gesicherten Daten in eine Archivdatei geschrieben werden, müssen Sie die Option `f` angeben.

#### Beispiel

Um das Verzeichnis `/muster` in einem Archiv mit dem Namen **sicherung.tar** auf dem Laufwerk **A:** zu sichern, geben Sie folgenden Befehl ein: `# tar -cf a/sicherung.tar /muster`

### 12.2.2 Sicherungsdaten wiederherstellen

Um die gesicherten Daten aus einem Archiv wiederherzustellen (zu extrahieren), müssen Sie die Operation `x` verwenden. Mithilfe der Option `f` legen Sie die Datei fest, aus der gelesen werden soll.

#### Beispiel

Um die Sicherungsdaten aus dem Archiv **sicherungs.tar** vom Laufwerk **A:** wiederherzustellen, geben Sie folgenden Befehl ein: `# tar -xf /a/sicherung.tar`

### 12.2.3 Einzelne Dateien wiederherstellen

Wenn Sie nicht ein ganzes Archiv, sondern nur eine bestimmte Datei wiederherstellen möchten, muss der Befehl `tar` um die gewünschte Datei ergänzt werden.

#### Beispiel

Um die Datei **Bilanz\_2013.docx** aus dem Archiv **sicherungs.tar** vom Laufwerk **A:** wiederherzustellen, geben Sie folgenden Befehl ein: `# tar -xf /a/sicherung.tar Bilanz_2013.docx`

## 12.3 Kommerzielle Sicherungsprogramme

Neben Backup-Lösungen, die in den Lieferumfang von Betriebssystemen gehören, stehen auch kommerzielle Sicherungsprogramme zur Verfügung. Hier einige Beispiele:

Anbieter	Beschreibung
<b>ARCserve</b>	Softwarelösung, die neben der Sicherung von Daten noch andere Funktionen anbietet (z. B. Servermigration und Datenkomprimierung).
<b>BackupExec</b>	Software von Symantec mit einem ähnlichen Funktionsumfang wie ARCserve. Symantec orientiert sich jedoch stärker an Windows-Systemen.
<b>Arkeia</b>	Software, die praktisch alle Betriebssysteme unterstützt. Speziell die Archivierungsfunktionen und Verschlüsselungsmöglichkeiten werden durch diese Software sehr gut abgedeckt.
<b>Acronis</b>	Image-basierte Software für Clients und Server, die unter Windows und Linux eingesetzt werden kann und auch mit virtuellen Umgebungen zusammenarbeitet. Spezielle Agents ermöglichen auch eine Sicherung von Datenbanken oder Exchange-Servern.

▷ **Hinweis**

Im Vorwort unter «Nützliche Links» finden Sie weitere Informationen über diese Anbieter. Teilweise werden auch Demoversionen zum Download angeboten. (Vgl. S. 10)

Die meisten **Betriebssysteme** verfügen über einfache Funktionen zur Sicherung von Daten, Programmen und Konfigurationseinstellungen. Für erweiterte Funktionen zur Datensicherung ist die Beschaffung eines **kommerziellen Sicherungsprogramms** in Betracht zu ziehen.

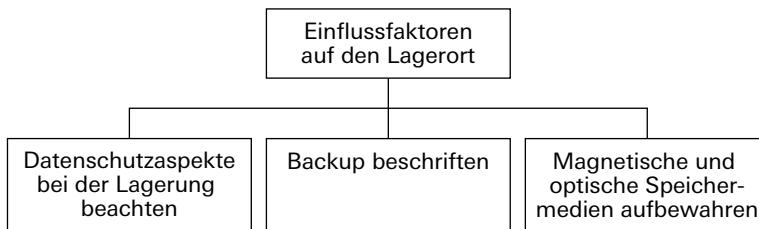
## Repetitionsfragen

- 
- 11 Sie verfügen zu Hause über einen Computer mit einem Windows-Betriebssystem. Brauchen Sie für den Backup ein kommerzielles Sicherungsprogramm?
- 
- 17 Was bewirkt der Unix-Befehl `tar tfv sicherung.tar`?
- 
- 23 In den gängigen Betriebssystemen sind bereits Backup-Tools enthalten. Wozu braucht es dann noch kommerzielle Sicherungsprogramme?
-

## 13 Aufbewahrung der Datenträger bestimmen

Nachdem Sie sich für die passenden Speichermedien entschieden haben, müssen Sie diese korrekt aufbewahren. Neben **gesetzlichen Vorschriften** sind dabei insbesondere **die Art und der Ort der Aufbewahrung** zu beachten. Behalten Sie jeweils folgende Aspekte im Auge:

[13-1] Aspekte der Aufbewahrung



### 13.1 Datenschutzaspekte beachten

Auf dem Server werden die Daten zur Datensicherung mit verschiedenen Massnahmen geschützt. Diese Massnahmen machen aber wenig Sinn, wenn die Speichermedien mit den gleichen Dateninhalten jedermann zugänglich sind. Dieses Thema wurde bereits in Kapitel 9.2, S. 60 angesprochen und hat neben technischen Massnahmen auch einen grossen Einfluss auf den Lagerort bzw. auf die Lagerung. In der Verordnung zum Bundesgesetz über den Datenschutz (235.11) Art. 9 (vgl. Kap. 1.6.2, S. 18) werden ebenfalls wichtige Aspekte zur Aufbewahrung vorgegeben. Die drei wichtigsten Punkte in Bezug auf die Wahl des Lagerorts werden im Folgenden kurz beschrieben.

#### 13.1.1 Zutrittskontrolle einrichten

Bei der Einrichtung einer Zugangs- oder Zutrittskontrolle ist darauf zu achten, dass nur befugte Personen auf die Speichermedien zugreifen können. Meist werden entsprechende Datenträger in einem abschliessbaren, separaten Raum als Aufbewahrungsort gelagert und die Zugangs- bzw. Zutrittsberechtigten erhalten einen Schlüssel, Badge oder Türcode.

#### 13.1.2 Schreibschutz aktivieren

Um eine (absichtliche oder unabsichtliche) Änderung der gesicherten Daten zu vermeiden, sollten Speichermedien nach Möglichkeit immer schreibgeschützt aufbewahrt werden.

#### 13.1.3 Persönliche Datenträgerkontrolle einführen

Um den Kreis der Personen, die mit Speichermedien arbeiten, möglichst klein zu halten, empfiehlt es sich, jeden Umgang mit Speichermedien zu dokumentieren, insbesondere die Herausgabe und Entgegennahme. Auf diese Weise wissen Sie immer, wer was wann mit einem Datenträger gemacht hat. Eventuell können so auch Rückschlüsse auf kriminelle Handlungen gezogen werden. Hier ein Beispiel für eine mögliche **Datenträgerkontrolle**:

[13-2] Datenträgerkontrolle (Auszug aus einem Beispieldokument)

Band Nr.	Wer	Wann	Was	Retour
1	René Wanner	13.7.2014 / 10:22	Die Datei <b>Bilanz.docx</b> wurde unter dem Namen <b>restore_Bilanz.docx</b> auf das Laufwerk X: zurückgespielt.	13.7.2014 / 11:22
2	Mara Rigotti	13.7.2014 / 16:30	Eine neues Band mit der Tagessicherung <b>von Laufwerk X:</b> wurde in das Lager gestellt.	-
...				

### 13.1.4 Zugriffsrechte einschränken

Auf vertrauliche Daten darf nur ein bestimmter Kreis von berechtigten Personen zugreifen. Auch beim Restore ist daher zu prüfen, ob die entsprechenden Personen dazu berechtigt sind. In vielen Fällen kann das Problem durch eine strenge Zutrittskontrolle gelöst werden.

## 13.2 Datenträger korrekt beschriften

LTO-Systeme, Autoloader und Libraries bieten automatisierte **Datenträgerbeschriftung** auf der Basis von Barcodes oder QR-Codes. Dies hat den Vorteil, dass die Bänder automatisch wieder gelesen werden können. Bei einem System ohne automatisierte Beschriftung sollten Sie wie folgt vorgehen:

1. Beschriften Sie die Datenträger nur an dafür vorgesehener Stelle. Das mag selbstverständlich klingen, in der Praxis sorgen falsch angebrachte Beschriftungen aber oft für vermeidbare Ausfälle.
2. Beschriften Sie Ihre Datenträger lesbar, übersichtlich und vollständig. Unlesbare oder unvollständige Beschriftungen sind ein grosses Ärgernis, wenn man nach bestimmten Daten sucht. Zusätzliche Hilfe bieten eindeutige, fortlaufende Nummern, die auch auf den Datenträgern gespeichert werden.

Hier ein Beispiel für eine mustergültige Beschriftung:

Eindeutige ID	Inhalt (Referenz auf Inhaltsdatenbank)	Speicherart	Sicherungsdatum Aufbewahrungsdatum	Band X von Y
Band 12 (Woche 1)	Server 1 / Buchungsdaten / Dateien siehe Datenbank Buchungen_GJ13.mdb	<input checked="" type="checkbox"/> Voll-Backup <input type="checkbox"/> Inkrementell <input type="checkbox"/> Differenziell <input type="checkbox"/> Archivierung	S: 01.03.2014 A: 07.03.2014	Band 2 von 3
...				

### 13.3 Datenträger korrekt lagern

Die korrekte **Datenträgerlagerung** ist notwendig, um eine möglichst lange Aufbewahrungsperiode ohne Datenverlust zu gewährleisten. Die physikalischen Eigenschaften von magnetischen und optischen Speichermedien sind unterschiedlich. Aus diesem Grunde müssen Sie je nach Speichermedium bei der Lagerung andere Regeln beachten.

#### 13.3.1 Magnetische Speichermedien

Magnetische Speichermedien werden mechanisch beschrieben und gelesen. Bei jedem Backup und Restore wird das Datenträgermaterial mechanisch belastet. Zusätzlich sind magnetische Speichermedien anfällig gegenüber äusseren Umwelteinflüssen wie Temperatur und Luftfeuchtigkeit. Je grösser die Schwankungen bei Temperatur und Luftfeuchtigkeit, desto kürzer die Lebensdauer der gelagerten Datenbestände. Für die Lagerung werden von den Herstellern folgende Bedingungen empfohlen:

Dauer	Temperatur	Luftfeuchtigkeit
Betrieb < 10 Jahre	17–25 °C	30–70%
Lagerung < 10 Jahre	15–23+ °C	40–55%
Lagerung > 10 Jahre	17 °C	30%
Langzeitlagerung	10 °C	20–50%

Im Weiteren sind die Datenbänder so aufzubewahren, dass sie vor Naturgewalten geschützt sind. Gefahren wie Feuer und Wasser (oder Löschmittel) sind der grösste «Feind der magnetischen Speichermedien». Ein sicherer Lagerort sollte also feuerfest und wasserdicht sein.

#### ▷ Hinweis

Wenn Sie Magnetbänder während langer Zeit übereinander lagern, können sich die Gehäuse verziehen. Stellen Sie die Bänder daher immer aufrecht und verwenden Sie am besten die Originalverpackung.

#### 13.3.2 Optische Speichermedien

Bei optimaler Lagerung haben optische Speichermedien eine Lebensdauer von bis zu 50 Jahren. Der Lagerort muss aber dunkel und kühl sein, da sie v. a. gegenüber Sonnenlicht empfindlich sind. Ein wichtiger Vorteil optischer Speichermedien gegenüber magnetischen Speichermedien liegt darin, dass sie gegenüber Feuchtigkeit nahezu unempfindlich sind.

Weil beim Lesevorgang keine mechanische Belastung stattfindet, erleiden optische Speichermedien keinen Oberflächenverschleiss. Die Hauptgefahr besteht darin, dass der Anwender die Oberfläche der Scheibe zerkratzt und dadurch Lesefehler auftreten. Sind die Beschädigungen umfangreich oder wird eine Scheibe gar zerbrochen, geht nichts mehr. Aus diesem Grunde sind optische Speichermedien sorgfältig und einzeln aufzubewahren.

Beschreibbare optische Speichermedien reagieren weit empfindlicher auf äussere Einflüsse als nicht beschreibbare Disks, da eine schützende Lackschicht fehlt. Bereits die Beschriftung mit einem Filzstift kann eine Disk nachhaltig beschädigen. Das Material des Datenträgers ist gegenüber verschiedenen organischen Substanzen wie Bakterien, Pflanzenresten oder Schimmel anfällig. Sogar ein fettiger, öriger Fingerabdruck kann im ungünstigen Fall zu einer lokalen Materialtrübung führen und Lesefehler hervorrufen.

Bei der **Wahl des Lagerorts** für ein Speichermedium kommen **gesetzliche Aspekte** ins Spiel, die beachtet werden müssen. So ist z. B. der Zugang zu schützenswerten Daten gemäss Datenschutzgesetz auf berechtige Personen zu beschränken. Datenträger, die zu Restore-Zwecken aus dem Lagerort entfernt werden, sind zu protokollieren. In diesem Fall hilft eine Nummerierung und Beschriftung der Speichermedien.

Weiter sind die unterschiedlichen **physikalischen Eigenschaften der Speichermedien** zu beachten. Während z. B. magnetische Datenträger keine Feuchtigkeit vertragen, macht dies optischen Datenträgern nichts aus.

## Repetitionsfragen

---

29 Nennen Sie Vorteile der optischen Datenträger gegenüber magnetischen Speichermedien.

35 Ergänzen Sie den folgenden Satz:

Je gemässigter und ausgeglichener die Temperaturen und je geringer die Luftfeuchtigkeit, desto ..... sind magnetische Speichermedien haltbar.

---

41 In der Nähe des betrieblichen Archivierungsraums mit Dutzenden von Sicherungs-DVDs kommt ein Elektromotor (Generator mit Elektromagnet) zum Einsatz. Müssen Sie sich um die Datenträger sorgen?

---

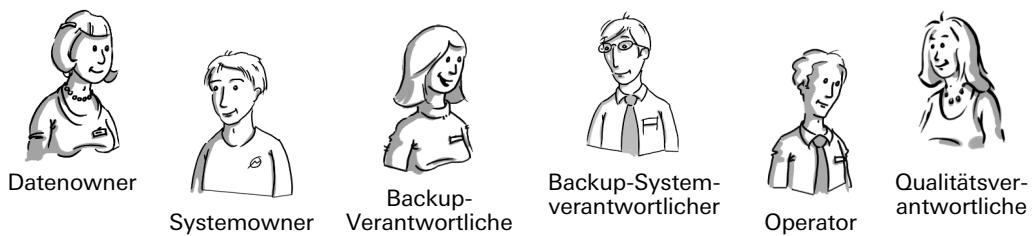
## 14 Verantwortung für das Backup und Restore festlegen

Nachdem die Speichermedien und die Sicherungssoftware bestimmt und der Lagerort der Datenträger geklärt worden ist, muss die organisatorische Verantwortung für das Backup- und Restore-System festgelegt werden.

### 14.1 Rollen und Verantwortungsbereiche

Damit das Backup- und Restore-Konzept wie geplant betrieben werden kann, müssen die entsprechenden Aufgaben und die zuständigen Personen festgelegt werden. In der Praxis sind meist folgende **Rollen** in ein Backup- und Restore-System involviert:

[14-1] Involvierte Rollen



Die **Verantwortungen** dieser Rollen in Bezug auf das Backup- und Restore-System lassen sich wie folgt beschreiben:

- Der **Datenowner** ist für die ihm zugeteilten Daten verantwortlich. Er bestimmt die Wichtigkeit der Daten und bestimmt somit indirekt, auf welche Art seine Daten gesichert werden.
- Der **Systemowner** ist für den unterbruchsfreien Betrieb seines Systems (z. B. Server, Netzwerk etc.) verantwortlich und dafür besorgt, dass die Datenbestände des Servers in ein Backup integriert werden. Er informiert den Backup-Verantwortlichen periodisch über die aktuellen Datenbestände, damit dieser ggf. die Planung anpassen kann.
- Der **Backup-Verantwortliche** ist dafür verantwortlich, dass die Daten vom Datenowner gemäss Konzept gesichert werden. Weiter erstellt er die Planung für die Backups und hält die Backup-Dokumente aktuell. Seine Aufgaben sind also mehr organisatorischer und planerischer Natur.
- Der **Backup-Systemverantwortliche** ist für den ordentlichen Betrieb des Backup- und Restore-Systems verantwortlich. Er sorgt sich um die Wartung der Speichermedien und -geräte und sorgt im Falle eines Defekts für deren Reparatur.
- Der **Operator** ist für das ordentliche Handling der Speichermedien, deren Beschriftung und eventuell den Transport an den Aufbewahrungsort verantwortlich. Zudem überwacht er den Backup-Vorgang auf Fehler und stellt einzelne Dateien auf Wunsch wieder her (Restore).
- Der **Qualitätsverantwortliche** kümmert sich um die Einhaltung der Qualität der Backups. Er überprüft die Dokumentationen und führt Stichproben und weitere Tests durch (siehe auch Kap. 16, S. 89).

#### ▷ Hinweis

In einem KMU werden diese Rollen oft von einer einzigen Person wahrgenommen (z. B. vom Systemadministrator).

## 14.2 Benutzer schulen

Für eine erfolgreiche Einführung eines Backup- und Restore-Systems ist es von zentraler Bedeutung, dass alle Benutzer den Sinn und Zweck sowie die grundlegende Funktionsweise dieses Systems kennen. Folgende Probleme sind in der Praxis häufig anzutreffen:

- Die Benutzer speichern ihre Daten auf der lokalen Festplatte und können diese im Fall eines Verlusts nicht mehr wiederherstellen, weil der Backup auf dem zentralen Server läuft.
- Die Benutzer wissen nicht, dass ihre Daten automatisch gesichert werden, und rekonstruieren sie im Fall eines Verlusts in aufwendiger, manueller Arbeit.
- Die Benutzer erinnern sich vage daran, dass sie einmal eine Datei hatten, können diese aber nicht mehr finden.
- Die Benutzer können im Fall eines Verlusts die notwendigen bzw. die vereinbarten Restore-Zeiten nicht abwarten, weil sie die Daten dringend benötigen.

Wie Sie anhand dieser Beispiele erkennen können, ist es notwendig, sämtliche Benutzer umfassend **über den Backup- und Restore-Prozess** aufzuklären. Es muss allen klar sein, was gesichert wird und welche Informationen für einen erfolgreichen Restore benötigt werden. Außerdem sind die benötigten Zeiten für Restores zu definieren und zu kommunizieren.

Damit die Aufgaben der Datensicherung während des Systembetriebs gemäss Konzept effektiv wahrgenommen werden, müssen die **Rollen** und **Verantwortlichkeiten** im Unternehmen festgelegt werden. In der Praxis hat sich folgende Aufgabenteilung bewährt:

- Der **Datenowner** ist für die ihm zugewiesenen Daten verantwortlich.
- Der **Systemowner** ist für den unterbrechungsfreien Betrieb seines Systems und für die Integration der darauf befindlichen Daten in ein Backup verantwortlich.
- Der **Backup-Verantwortliche** ist dafür verantwortlich, dass die Daten nach seinen Vorgaben gesichert werden.
- Der **Backup-Systemverantwortliche** ist für den ordentlichen physischen Betrieb des Backup-Systems verantwortlich.
- Der **Operator** führt den Backup und den Restore gemäss Konzept aus.
- Der **Qualitätsverantwortliche** ist für die Einhaltung der Backup-Qualität zuständig.

In kleinen Unternehmen können diese Rollen von einer einzigen Person wahrgenommen werden.

## Repetitionsfragen

47 Welche Rolle im Backup- und Restore-System führt den Restore aus?

6 Bei der Kontrolle eines Backups ist Ihnen aufgefallen, dass das Bandlesegerät defekt ist. Welche Rolle ist dafür zuständig?

12 Warum müssen alle Benutzer über den Backup- und Restore-Prozess informiert werden?



## **Teil D Backup- und Restore-System sicher betreiben**

---

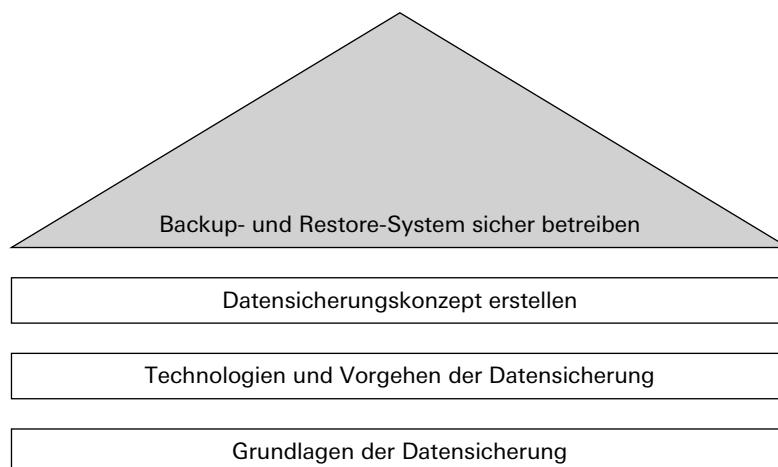
## Einleitung, Lernziele und Schlüsselbegriffe

### Einleitung

Nachdem das Datensicherungskonzept erstellt worden ist, geht es darum, alle nötigen Voraussetzungen zu schaffen, damit das Backup- und Restore-System sicher betrieben werden kann. Dazu gehören in erster Linie eine gewissenhafte **Notfall- und Testplanung**. In diesem Teil des Lehrmittels erfahren Sie, was ein Notfallhandbuch beinhalten sollte und was bei der Planung und Dokumentation von Tests in Bezug auf ein Backup- und Restore-System zu beachten ist.

Folgende Grafik zeigt auf, wo Sie sich innerhalb des Lehrmittels befinden:

[14-2] Inhalt von Teil D



### Lernziele und Lernschritte

Lernziele	Lernschritte
<input type="checkbox"/> Sie können ein Notfallhandbuch für Ihr Unternehmen erstellen.	Notfallhandbuch erstellen
<input type="checkbox"/> Sie können die korrekte Ausführung Ihres Backup- und Restore-Systems mittels Tests und Stichprobenkontrollen gewährleisten.	Backup- und Restore-System testen

### Schlüsselbegriffe

Alarmierungsplan, Aufgabenbeschreibung, Cold Standby, Datensicherungsplan, Dokumentation der Testergebnisse, Hot Standby, Kontaktinformation, Meldeweg, Notfallhandbuch, Notfallmassnahme, Notfallorganisation, Notfallverantwortlicher, Replikation, Sofortmassnahme, Testvorbereitung, Testziele, Wiederanlaufplan, Wiederbeschaffung

## 15 Notfallmassnahmen planen

Stellen Sie sich einen Totalausfall des Servers vor, mit dessen Daten täglich Dutzende von Benutzern in Ihrem Unternehmen arbeiten. Diese Daten sind nun von einem Moment auf den anderen nicht mehr verfügbar und Sie werden mit Anrufen und Reklamationen der Benutzer eingedeckt. In dieser hektischen Situation gilt es, Ruhe zu bewahren und die zuletzt gesicherten Daten möglichst rasch wiederherzustellen. Damit dies gelingen kann, ist es ratsam, ein **Notfallhandbuch** zu erstellen, das Ihnen und anderen Verantwortungsträgern im Unternehmen als zuverlässige Hilfe dient. In diesem Kapitel erfahren Sie, wie ein solches Handbuch aufgebaut wird und was die einzelnen Abschnitte enthalten sollten.

### 15.1 Notfallhandbuch erstellen

Im Anhang des BSI<sup>[1]</sup>-Standards 100-4<sup>[2]</sup> finden Sie Muster für Notfallhandbücher und Geschäftsfortführungspläne. Bei der Gestaltung der betrieblichen Notfallpläne können Sie sich an diesen Beispielen orientieren und die Inhalte und die Struktur nach Bedarf anpassen. Das folgende Inhaltsverzeichnis eines Notfallhandbuchs wurde auf die Bedürfnisse eines KMU angepasst.

[15-1] IT-Grundschutzhandbuch

#### Teil A: Sofortmassnahmen

- 1 Alarmierung im Notfall
  - 1.1 Alarmierungsplan und Meldewege
  - 1.2 Adresslisten betroffener Mitarbeitender
  - 1.3 Festlegung konkreter Aufgaben für einzelne Personen / Funktionen im Notfall
  - 1.4 Notrufnummern (z. B. Feuerwehr, Polizei, Notarzt, Wasser- und Stromversorger, Ausweichrechenzentrum, externes Datenträgerarchiv, externe Telekommunikationsanbieter)
- 2 Handlungsanweisung für spezielle Ereignisse
  - 2.1 Brand
  - 2.2 Wassereinbruch
  - 2.3 Stromausfall
  - 2.4 Ausfall der Klimaanlage
  - 2.5 Explosion
  - 2.6 Sabotage
  - 2.7 Ausfall der Datenfernübertragungseinrichtung
  - 2.8 Einbruch
  - 2.9 Vandalismus
  - 2.10 .....

#### Teil B: Regelungen für den Notfall

- 3 Allgemeine Regelungen
  - 3.1 Notfallverantwortliche
  - 3.2 Benennung der an der Durchführung der Notfallpläne beteiligten Organisationseinheiten, Kompetenzverteilung
  - 3.3 Organisationsrichtlinien, Verhaltensregeln
- 4 Tabelle der Verfügbarkeitsanforderungen

[1] Abkürzung für: Bundesamt für Sicherheit in der Informationstechnik (Deutschland). Vergleichen Sie dazu auch das Linkerverzeichnis auf S. 10.

[2] BSI-Standard für das Notfallmanagement.

**Teil C: Wiederanlaufpläne für kritische Komponenten**

- 5 Wiederanlaufplanung
  - 5.1 Wiederanlaufplan für Komponente 1 (z. B. Host)
    - 5.1.1 Wiederbeschaffungsmöglichkeiten
    - 5.1.2 Interne / externe Ausweichmöglichkeiten
    - 5.1.3 DFÜ-Versorgung
    - 5.1.4 Eingeschränkter IT-Betrieb
    - 5.1.5 Wiederanlaufreihenfolge
  - 5.2 Wiederanlaufplan für Komponente 2 (z. B. Dateiserver)

**Teil D: Dokumentation**

- 6 Beschreibung der IT-Systeme
  - 6.1 Beschreibung des IT-Systems A (im Überblick)
    - 6.1.1 Beschreibung der Hardware-Komponenten
    - 6.1.2 Beschreibung der Software-Komponenten
      - 6.1.2.1 Bestandsverzeichnis der Systemsoftware
      - 6.1.2.2 Bestandsverzeichnis der zu dem IT-System gehörenden Systemdaten
      - 6.1.3 Beschreibung der Netzanbindungen des IT-Systems
      - 6.1.4 Beschreibung der IT-Anwendungen
        - 6.1.4.1 Bestandsverzeichnis der Anwendungssoftware
        - 6.1.4.2 Bestandsverzeichnis der zu einer IT-Anwendung gehörenden Daten
        - 6.1.4.3 Kapazitätsanforderungen einzelner IT-Anwendungen im Normalfall
        - 6.1.4.4 Minimale Kapazitätsanforderungen der IT-Anwendungen für den Notfall
        - 6.1.4.5 Wiederanlaufverfahren der IT-Anwendungen
      - 6.1.5 Datensicherungsplan
      - 6.1.6 Beschreibung der notwendigen Infrastruktureinrichtungen
      - 6.1.7 Sonstige Unterlagen (Handbücher etc.)
  - 7 Wichtige Informationen
    - 7.1 Ersatzbeschaffungsplan
    - 7.2 Hersteller- und Lieferantenverzeichnis

Nachfolgend werden einzelne Abschnitte des Notfallhandbuchs näher beschrieben, weil sie für die betriebliche Notfallplanung für die meisten Unternehmen wichtig sind.

## **15.2 Sofortmassnahmen**

Der erste Abschnitt des Notfallhandbuchs enthält Informationen über sofort einzuleitende Massnahmen im Falle eines Notfalls. Diese Informationen müssen möglichst übersichtlich und prägnant dargestellt werden. Oft sind Tabellen hervorragend geeignet, um sie klar und verständlich zu strukturieren.

### 15.2.1 Alarmierung im Notfall

Am Anfang steht immer die Frage, ob es sich bei einem Ereignis um einen echten Notfall handelt.

- Ist es wirklich ein Notfall?
- Welche Art von Notfall liegt vor?
- Wer muss ggf. alarmiert werden?

Betroffene Mitarbeitende neigen dazu, ein Ereignis bzw. Problem möglichst rasch zu lösen und die Information oder Kommunikation zu vernachlässigen. So kann eine nachhaltige Lösung auch verhindert und der Schaden eventuell vergrößert werden. In Notfällen sind daher eindeutige Richtlinien bzw. Anweisungen mit klaren Entscheidungsregeln gefragt. Hier ein Beispiel für eine solche Richtlinie:

[15-2] Richtlinie für den Ausfall des Dateiservers (Auszug)

Vorfall	Regel	Massnahmen
Ausfall Dateiserver	Die Reparatur des Dateiservers muss spätestens nach 1 Stunde aufgegeben werden. Eine Neuinstallation des Servers inklusive Daten-Restore ist schneller und verspricht mehr Erfolg.	Restore einleiten

### 15.2.2 Alarmierungsplan

Je nach Situation müssen in einem Notfall gleich mehrere Personen alarmiert werden.

#### Beispiel

Wenn in einem Rechnerraum Feuer ausbricht, sind neben der Feuerwehr auch der zuständige Abteilungsleiter und das verantwortliche Mitglied der Geschäftsleitung zu benachrichtigen.

Im **Alarmierungsplan** muss die zeitliche Reihenfolge aller zu alarmierenden Personen sowie von ihren Stellvertretern (für den Fall der Nacherreichbarkeit) festgelegt bzw. benannt sein. Daneben spielt auch der Informationskanal eine enorm wichtige Rolle. Der **Meldeweg** beschreibt, welche Personen in welcher Reihenfolge über welchen Weg alarmiert werden. Hier ein Beispiel für einen solchen Alarmierungsplan:

[15-3] Alarmierungsplan mit Meldeweg

Vorfall	Innerhalb von	Personen	Stellvertreter	Medium
Ausfall Dateiserver	30 Minuten	IT-Leiter	Leiter Information	Telefon, SMS
Ausfall Dateiserver	1 Stunde	Logistikleiter	Geschäftsleitung	Fax, Mail

#### ▷ Hinweis

Die benachrichtigten Personen müssen über die Inhalte des Notfallhandbuchs informiert sein, damit sie korrekt reagieren können.

### 15.2.3 Kontaktinformationen

Sobald klar ist, bei welchem Ereignis welche Personen über welches Medium informiert werden, müssen die entsprechenden **Kontaktinformationen** bereitliegen. Für diesen Zweck haben sich gleichartig aufgebaute Tabellen bewährt. Hier ein Beispiel dazu:

[15-4] Kontaktinformationen

Name	Hans Muster
Funktion	IT-Leiter
Telefon Büro	043 888 34 54
Fax Büro	043 888 34 55
Telefon Privat	043 999 34 67
Telefon Natel	079 555 33 22
Adresse Privat	Musterstrasse 20, 8000 Zürich

Die Tabellen mit den Kontaktinformationen können bei Bedarf nach internen und externen Personen bzw. Informationsempfängern gegliedert werden. Zu den externen Informationsempfängern gehören beispielsweise die Feuerwehr, die Polizei, der Notarzt, der Wasser- und Stromversorger, der Telefonanbieter, der Service Provider etc.

### 15.2.4 Aufgabenbeschreibungen

Die im Alarmierungsplan festgehaltenen (internen) Personen müssen über die weiteren Aufgaben und Schritte Bescheid wissen, die von ihnen in der jeweiligen Notfallsituation erwartet werden. Neben der Zuordnung der Verantwortung und der Kompetenzen ist es daher wichtig, die Aufgaben der einzelnen Teams oder Personen klar zu beschreiben. Hier ein Beispiel für eine solche **Aufgabenbeschreibung**:

[15-5] Beispiel Festlegung konkreter Aufgaben für einzelne Personen

Vorfall	Wer	Aufgabe
Absturz Dateiserver	Backup-Verantwortlicher	Restore ausführen
	IT-Leiter	Restore-Vorgang überwachen und bei Problemen Massnahmen vorbereiten
	Leiter Logistik	Betroffene Benutzer informieren

## 15.3 Regelungen für den Notfall

Bei den Sofortmassnahmen wird festgehalten, wie im Falle eines Notfalls vorgegangen wird, um den Schaden möglichst rasch zu begrenzen und die reguläre Geschäftstätigkeit fortführen zu können. In solchen Situationen muss ggf. ein «**Notstandsregime**» eingeführt werden, das besondere organisatorische Regelungen vorsieht.

### 15.3.1 Notfallverantwortliche

Jedes Unternehmen sollte erfahrene Personen bestimmen, die für die Behebung eines Notfalls bzw. Notstands verantwortlich sind. Ihre Aufgabe besteht darin, die **Risiken** eines Notfalls abzuwägen und geeignete **Gegenmassnahmen** festzulegen. In grossen Unternehmen werden je nach Situation ganze Abteilungen damit betraut. In einem KMU wird diese Aufgabe meist vom Unternehmensleiter wahrgenommen.

### 15.3.2 Notfallorganisation

In einem Notfall müssen ggf. weitreichende Entscheidungen getroffen und beispielsweise Ersatzgeräte beschafft, Ersatzsysteme aufgebaut oder externe Spezialisten beigezogen werden. In der **Notfallorganisation** wird definiert, welche Aufgaben, Kompetenzen und welche Verantwortung den einzelnen Mitarbeitenden bzw. Mitarbeitergruppen zugesprochen werden, damit diese bei einem Notfall auch handeln können.

## 15.4 Wiederanlaufpläne für kritische Komponenten

Dieser Abschnitt des Notfallhandbuchs beschreibt, welche Möglichkeiten bestehen, um kritische Systemkomponenten im Notfall möglichst rasch wieder in Betrieb nehmen zu können.

### 15.4.1 Wiederanlauf

Je nachdem, wie problematisch der Ausfall eines Systems für ein Unternehmen ist, kann der Wiederanlauf unterschiedlich gehandhabt werden. Bei unkritischen Systemen oder Einzelservern wird häufig das Cold-Standby-Verfahren eingesetzt. Bei kritischen Systemen oder zentralen Komponenten (wie z. B. der Host mehrerer virtueller Server) wird dagegen meist das Hot-Standby-Verfahren eingesetzt.

- Mit **Cold Standby** ist der Offline-Einsatz redundanter Komponenten in einem IT-System gemeint. Bei einem Ausfall einer Komponente wird nicht automatisch (wie beim Hot Standby) die Ersatzkomponente aktiviert, sondern diese wird manuell durch einen Systemadministrator gestartet oder in Betrieb genommen. Das können Komponenten wie Festplatten oder Netzteile sein, aber auch ein ganzer Server, der auf Reserve in einem ausgeschalteten Zustand bereitsteht. Diese Vorgehensweise ist kostengünstiger als das Hot Standby, bringt aber eine unvermeidbare Ausfallzeit des Systems mit sich. Deshalb wird ein Cold-Standby-System nicht für Anwendungen eingesetzt, die ständig zur Verfügung stehen müssen.
- Beim **Hot Standby** (auch Hot Site genannt) ist die Komponente dauernd aktiv, z. B. als redundantes Bauteil (Netzteil, Memory, Spare-Disks) oder als ganzer Server, der aufgesetzt, aber im Leerlauf in Betrieb ist.

Die nächste Stufe ist der Einsatz **redundanter Infrastrukturen**. Damit ist der parallele Betrieb gröserer ICT-Systeme gemeint. So kann z. B. ein Server in einem gemieteten Rechenzentrum stehen, der dort betrieben und bei Bedarf mit den aktuellen Daten versorgt wird. Als redundant wird ein System bezeichnet, wenn die Daten regelmässig automatisch auf diesen Server übertragen werden (**Replikation**), sodass so gut wie keine Ausfallzeit resultiert. Manche Banken und Versicherungen verfügen nicht nur über redundante ICT-Systeme, sondern auch über «redundantes» bzw. eigenes Personal an beiden Standorten.

#### ▷ Hinweis

Die Reihenfolge eines Wiederanlaufs muss im Vorfeld geklärt und schriftlich festgehalten werden (vgl. Kap. 9.4, S. 60). In einem Notfall müssen diese Vorgaben strikt eingehalten werden.

### 15.4.2 Wiederbeschaffung

---

Es ist nicht immer sinnvoll, Komponenten oder ganze Infrastrukturen redundant (doppelt) zu führen. Manchmal ist es günstiger und effektiver, mit einem Systemlieferanten oder mit einem Händler Vereinbarungen über Ersatzbeschaffungen auszuhandeln. In vielen Fällen werden beispielsweise mit den Lieferanten von Hardware oder Anwendungssoftware **Wartungs- und Supportverträge** abgeschlossen, die Vereinbarungen über schnelle Ersatzlieferungen beinhalten. Oft ist es auch möglich, diese Geräte bereits vorinstalliert zu liefern. Ein sogenanntes Image mit der Standardsoftware (Betriebssystem und Programme) und deren Konfigurationen können bei Bedarf dem Lieferanten mitgeteilt und dort hinterlegt werden.

Beachten Sie, dass alle wichtigen Angaben zur Wiederbeschaffung dokumentiert und im Notfall rasch verfügbar sein müssen. Dazu gehören die Kontaktinformationen des Lieferanten, die Zeiten seiner Erreichbarkeit sowie die Zeiten des möglichen Austauschs.

### 15.4.3 Ausweichmöglichkeiten

---

Meist besteht auch die Möglichkeit, einen Notbetrieb aufzunehmen, bei dem die Benutzer nicht zentrale Ressourcen nutzen, sondern auf **dezentrale Ressourcen** ausweichen und lokal arbeiten. Dies bedeutet z. B., dass Benutzer ohne Zugriff auf einen zentralen Server oder Abteilungsdrucker mit den auf ihren Computern installierten Anwendungen bzw. mit den an ihrem Computer angeschlossenen Peripheriegeräten arbeiten.

Für besonders kritische Aufgaben oder bei schwerwiegenden Störungen sollte erwogen werden, Möglichkeiten zu schaffen, auf **externe Arbeitsplätze** ausweichen zu können. Voraussetzung dafür sind entsprechende Vereinbarungen, Reservationen und Ausstattungen.

#### Beispiel

Die «Basler Zeitung» hat mit anderen Zeitungsverlagen für Notfälle die Bereitstellung von Kapazitäten in ihrer Druckerei vereinbart.

## 15.5 Dokumentation

---

Systeme, Programme und Datensicherungskonzepte müssen bis ins letzte Detail dokumentiert sein. Diese Dokumentationen sind Bestandteil des Notfallhandbuchs.

### 15.5.1 Datensicherungsplan

---

Im **Datensicherungsplan** wird festgehalten, wo die Datensicherungsmedien aufbewahrt werden und nach welchem Prinzip die Speichermedien angeschrieben sind. Dank dieser Information finden Sie gezielt und rasch den gewünschten Datenträger.

### 15.5.2 Sonstige Unterlagen

---

Jedes Gerät und jede Anwendungssoftware sollte über eine eigene Dokumentation bzw. **Gebrauchsanleitung** verfügen. Diese Unterlagen gehören ebenfalls ins Notfallhandbuch.

#### Beispiel

Stellen Sie sich vor, Sie stehen vor dem Backup-Server und es erscheint die Fehlermeldung «A213». Sicherlich sind Sie in einem solchen Moment froh, wenn das Handbuch des Servers vorliegt.

## 15.6 Beispiel eines Notfallhandbuchs

Im Folgenden sehen Sie beispielhaft ein Notfallhandbuch für Backup und Restore.

### Notfallhandbuch Backup und Restore

#### Teil A: Sofortmassnahmen

A/1: Alarmierung im Notfall, Alarmierungsplan und Meldewege

Vorfall	Regel	Massnahmen	Alarmierungsplan
Täglicher Datentransfer auf NAS nicht korrekt ausgeführt.	Der Ursache während 30 Minuten nachgehen. Falls keine Lösung, Backup erneut starten.	Backup-Vorgang erneut ausführen (auch während des Tages).	Notierung in Wochenbericht. Keine direkte Alarmierung notwendig.
Täglicher Datentransfer auf NAS nicht möglich.	Reparatur im Rahmen der Möglichkeiten vornehmen. Nach 30 Minuten Verbindung mit Hardwarelieferant aufnehmen.	Verbindung mit Hardwarelieferant aufnehmen.	1. Hardwarelieferant 2. IT-Leiter (1 Stunde)
Transfer NAS auf Autoloader nicht korrekt ausgeführt.	Der Ursache während 30 Minuten nachgehen. Falls keine Lösung, Backup erneut starten.	Bänder auswechseln. Backup erneut starten.	Notierung in Wochenbericht. Keine direkte Alarmierung notwendig.
Transfer Datentransfer auf Autoloader nicht möglich.	Reparatur im Rahmen der Möglichkeiten vornehmen. Nach 30 Minuten Verbindung mit Hardwarelieferant aufnehmen.	Verbindung mit Hardwarelieferant aufnehmen.	1. Hardwarelieferant 2. IT-Leiter (1 Stunde)

A/2: Notrufnummern

Wer	Nummer	Beschreibung
Feuerwehr	118	
Polizei	117	
Elektrizitätswerk	043 333 33 33	
Wasserwerk	043 444 44 44	
Hardwarelieferant	043 555 55 55	7x24 h-Hotline
Telekommunikationsanbieter	043 666 66 66	

#### Teil B: Regelung für den Notfall

B/1: Notfallverantwortliche

Notfallverantwortlich für Backup und Restore ist Mara Rigotti. Stellvertretung übernimmt Kurt Meiner.

B/2: Benennung der an der Durchführung der Notfälle beteiligten Organisationseinheiten, Kompetenzverteilung

Bei einem Totalausfall der Server wird Mara Rigotti ermächtigt, den Betrag von maximal CHF 10 000.– einzusetzen. Innerhalb dieses Betrags darf Hardware beschafft oder es dürfen externe Spezialisten beauftragt werden.

#### Teil C: Wiederanlaufpläne für kritische Komponenten

C/1: Wiederbeschaffungsmöglichkeiten

Mit dem Hardwarelieferanten wurde vereinbart, dass innerhalb von 3 Stunden nach Meldung ein Ersatz-Backup-Server geliefert wird. Ein komplettes Image (Betriebssystem, Programme sowie Einstellungen) ist beim Hardwarelieferanten hinterlegt.

C/2: interne und externe Ausweichmöglichkeiten

Im Falle eines Ausfalls von einem Speichermedium (NAS-Backup-Server oder Autoloader) kann jederzeit auf das funktionierende Speichermedium umgestiegen werden. Eine Anleitung hierfür liegt in der Beilage.

C/3: Wiederanlaufreihenfolge

Die Reihenfolge wird wie folgt wiederhergestellt:

- Betriebssystem
- Programme
- Konfigurationen
- Dateien Buchungsdaten, Kundenbriefe, Buchhaltungsdaten

**Teil D: Dokumentation**

D/1: Datensicherungsplan

Aufbewahrung

- NAS-Backup-Server: im Raum U202
- Bänder: Monatsbänder in Bern / wöchentliche / tägliche Bänder im Tresor U202

Anschrift der Bänder

Eindeutige ID	Inhalt (Referenz auf Inhaltsdatenbank)	Speicherart	Sicherungsdatum Aufbewahrungs- datum	Band X von Y
Band 12 (Woche 1)	Server 1 / Buchungsdaten / Dateien siehe Datenbank XY.mdb	<input checked="" type="checkbox"/> Voll-Backup <input type="checkbox"/> Inkrementell <input type="checkbox"/> Differenziell <input type="checkbox"/> Archivierung	S: 01.03.200X A: 07.03.200X	Band 2 von 3

D/2: sonstige Unterlagen (Handbücher)

- Anleitung Umstellung von NAS-Backup-Server auf Autoloader
- Handbuch NAS-Backup-Server
- Handbuch Autoloader

Im Falle eines Notfalls muss rasch gehandelt werden können. Hierfür empfiehlt es sich, sich im Vorfeld bereits Gedanken zu einem Notfall zu machen und ein **Notfallhandbuch** zu erstellen. Das BSI stellt unterschiedliche Standards bzw. Vorlagen zur Verfügung, die aufgrund ihrer vordefinierten Struktur helfen, keine wichtigen Inhalte zu vergessen. In einem Notfallhandbuch sollten folgende **Inhalte** definiert werden:

- Sofortmassnahmen, um bei einem Notfall rasch handeln zu können, wird die komplette Alarmierung inklusive Kontaktpersonen festgehalten.
- Regelungen für den Notfall, es werden die Notfallverantwortlichen und die Notfallorganisation definiert.
- Wiederanlaufpläne für kritische Komponenten, es wird definiert, wie kritische Komponenten wiederbeschafft und installiert werden.
- Dokumentation, in diesem Kapitel wird bestimmt, welche Dokumentationen vorliegen müssen bzw. wo und mit welchem Inhalt diese abgelegt sind.

## Repetitionsfragen

18 Warum gehören Unterlagen wie z. B. Handbücher in ein Notfallkonzept?

24 Warum wird im Notfallhandbuch die Kompetenz der Mitarbeitenden festgelegt?

30 Ist die Erstellung eines Notfallhandbuchs eine Preloss- oder eine Postloss-Aufgabe? Begründen Sie kurz Ihren Entscheid.

## 16 Backup- und Restore-System testen

Alle Konzepte, Pläne und Dokumente nützen wenig, wenn die betroffenen Mitarbeitenden beim praktischen Umgang damit nicht geschult wurden. In einem Notfall ist es auch zu spät, mit dem Studium des Notfallhandbuchs zu beginnen. Weiter muss das Backup- und Restore-System vor dessen Inbetriebnahme getestet und nach dessen Inbetriebnahme regelmäßig überprüft werden, ob es (noch) korrekt funktioniert. Es kommt immer wieder vor, dass ein Unternehmen viel zu spät merkt, dass der Backup seit Tagen oder Wochen nicht mehr ausgeführt wurde. In diesem Kapitel erfahren Sie, wie Sie ein Backup- und Restore-System testen können, um zu gewährleisten, dass es einwandfrei läuft.

### 16.1 Tests planen und vorbereiten

Die Planung und Durchführung von Tests kann in folgende Schritte gegliedert werden:

[16-1] Testablauf



#### 16.1.1 Testziele festlegen

Ein vollständiges Backup- und Restore-System ist meist komplex und enthält viele Daten. Es wäre zu aufwendig, alle funktionalen und nichtfunktionalen Anforderungen zu testen. Aus diesem Grund werden i. d. R. stichprobenartig eine Auswahl an wichtigen Funktionen und Features getestet. So wird beispielsweise überprüft, ob beim Backup sämtliche Daten korrekt gespeichert und die Bänder richtig angeschrieben werden. Oder die Durchführung eines Restores wird in Bezug auf Vollständigkeit und Geschwindigkeit kontrolliert.

#### 16.1.2 Zeitpunkt festlegen

Nach der Inbetriebnahme des Backup- und Restore-Systems ist der Zeitpunkt der Tests so zu wählen, dass der Systembetrieb und das reguläre Backup nicht gestört werden. Unter keinen Umständen darf es aufgrund von Tests zu Fehlern im aktuellen Backup kommen.

#### 16.1.3 Beteiligte informieren

Ein Testlauf muss im Voraus kommuniziert werden. Sinn und Zweck der Übung ist es, die Verantwortlichen zu trainieren. Diese können im Vorfeld und ohne Hektik das Backup- und Restore-Konzept sowie das Notfallhandbuch nochmals studieren. Ebenfalls können so technische Massnahmen getroffen werden, damit der reguläre Backup ordnungsgemäß ausgeführt wird. Bei der Durchführung der Tests werden Beobachter eingesetzt, die die Übung dokumentieren.

Für die **Vorbereitung von Tests** eignet sich z. B. folgende Checkliste:

[16-2] Checkliste für die Testvorbereitung (Beispiel)

Checkliste Testvorbereitung	
Checkpunkte	Bemerkung
<input type="checkbox"/> Wurde die Durchführung der geplanten Tests durch das Management bestätigt?	
<input type="checkbox"/> Sind alle Beteiligten benachrichtigt worden?	
<input type="checkbox"/> Wurden auch die externen Partner benachrichtigt?	
<input type="checkbox"/> Wurde überprüft, ob die normale Datensicherung ordnungsgemäß durchgeführt wurde?	
<input type="checkbox"/> Sind die beteiligten Personen im Besitz des aktuellen Notfallhandbuchs?	
<input type="checkbox"/> Wurden unabhängige Testbeobachter bestellt?	
<input type="checkbox"/>	
<input type="checkbox"/>	

## 16.2 Tests durchführen und dokumentieren

Bei der Durchführung der Tests werden stichprobenartig alle wichtigen funktionalen und nichtfunktionalen Anforderungen an das Backup- und Restore-System getestet. Danach werden die Testergebnisse dokumentiert und in einem Testbericht zusammengefasst. Je nach den Befunden müssen im Nachgang eventuell Anpassungen vorgenommen oder geeignete Massnahmen eingeleitet werden. Für die **Dokumentation der Testergebnisse** eignet sich z. B. folgendes Formular:

[16-3] Dokumentation der Testergebnisse (Beispielvorlage)

Testergebnisse	
Folgende Tests wurden durchgeführt.	
1	Stichprobe auf 2 Bändern, ob die ausgewählten Daten korrekt gespeichert wurden.
2	Kontrolle, ob wöchentlicher Voll-Backup korrekt ausgeführt wurde.
3	Kontrolle des Bandinventars der letzten 3 Monate.
4	

Checkpunkte	Bemerkungen
<input checked="" type="checkbox"/> Backup	In Ordnung
<input type="checkbox"/> Restore-Konfiguration	
<input checked="" type="checkbox"/> Archivierung	1 Band fehlt
<hr/>	
<b>Bemerkungen zu den Tests</b>	
1	Stichprobe auf 2 Bändern i. O.
2	Voll-Backup wurde komplett ausgeführt.
3	Bänder der letzten 3 Monate kontrolliert. Es fehlt Band 12 vom Voll-Backup vom 5.3.2014.
4	
<hr/>	
Bestätigt durch:	Datum:
Mara Rigotti	12.4.2014

Jedes Backup- und Restore-System muss vor der Inbetriebnahme getestet und nach der Inbetriebnahme regelmässig daraufhin überprüft werden, ob es (noch) korrekt funktioniert. Die **Vorbereitung und Durchführung solcher Tests** kann in folgende Schritte gegliedert werden:

1. Ziele des Tests festlegen
2. Zeitpunkt des Tests festlegen
3. Beteiligte über Testablauf informieren
4. Test nach Testplan durchführen
5. Testergebnisse dokumentieren

## Repetitionsfragen

- 
- 36** Was müssen Sie beachten, wenn Sie den Zeitpunkt für den Test des Backup- und Restore-Systems festlegen?
- 
- 42** Warum ist es nicht möglich, beim Test des Backup- und Restore-Systems alle Funktionen, Daten und Features zu überprüfen?
- 
- 48** Warum müssen die Mitarbeitenden über den anstehenden Test eines Backup- und Restore-Systems informiert werden?
-



## **Teil E Anhang**

---

## Gesamtzusammenfassung

---

### 1 Warum müssen Daten gesichert werden?

---

Daten sind unbezahlbar und sind konstant verschiedenen Bedrohungen ausgesetzt:

- Höhere Gewalt
- Menschliches Versagen
- Technisches Versagen
- Kriminelle Handlung

Mit organisatorischen, personellen, technischen und baulichen Massnahmen können die Daten geschützt werden. Aus betrieblichen Gründen ist darauf zu achten, dass Daten jederzeit und in korrekter Weise den Mitarbeitenden zur Verfügung stehen. Bei einem Verlust könnte die Existenz des Unternehmens bedroht sein. Zudem existieren auch gesetzliche Vorschriften zur Datenhaltung und -sicherung.

### 2 Was bedeutet Datensicherung?

---

In diesem Kapitel haben Sie unterschiedliche Begriffe kennengelernt:

- Ein Backup ist die Ausführung einer Sicherheitskopie. Sinn und Zweck des Backups ist, die Daten im Falle eines Verlusts gesichert zu haben.
- Ein Restore ist der Vorgang, gesicherte Daten wieder zurückzuholen.
- Ein Image ist eine komplette Kopie eines Systems (Programme, Konfiguration und Daten), damit eine Inbetriebnahme schneller durchgeführt werden kann.

Der Begriff Disaster Recovery bezeichnet alle Massnahmen, die nach einem Unglücksfall in der Informationstechnik eingeleitet werden. Dazu zählt sowohl die Datenwiederherstellung als auch das Ersetzen nicht mehr benutzbare Infrastruktur, Hardware und Organisation.

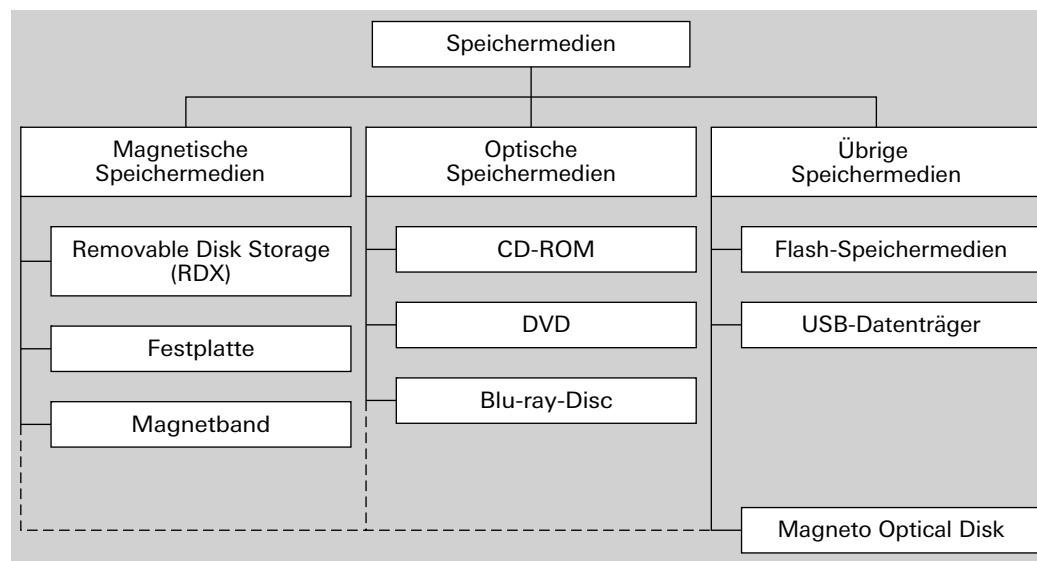
Ein Backup- und Restore-Konzept ist ein schriftliches Konzept, bei dem alle relevanten Informationen zur Datensicherung definiert und dokumentiert werden. Aufgrund unterschiedlicher Bedürfnisse werden danach Backup- und Restore-Systeme mit diversen Medien, Rollen (z. B. Backup-Verantwortlicher) und Abläufen aufgebaut.

Mittels Backup sollen unfreiwillig gelöschte oder zerstörte Daten wiederhergestellt und ein durchgängiger Systembetrieb gewährleistet werden. Mittels Archivierung hingegen werden gesetzliche Anordnungen befolgt.

### 3 Wo werden Daten gesichert?

Historisch kann zwischen magnetischen und optischen Speichermedien unterschieden werden. In jüngster Zeit wurden diese Technologien kombiniert, um die jeweiligen Vorteile zu nutzen und die jeweiligen Nachteile zu minimieren. Hier ein Überblick über die wichtigsten Speichermedien:

#### Speichermedien im Überblick



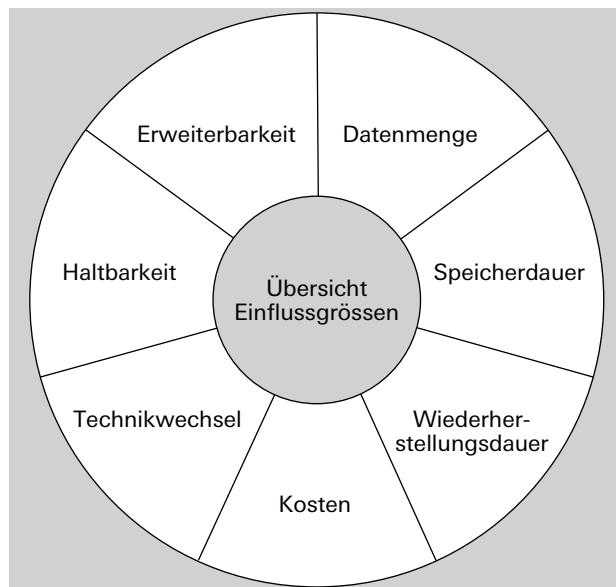
Jedes Speichermedium hat seine Vor- und Nachteile und nicht alle Datenträger eignen sich für einen vollständigen Backup. Hier die wichtigsten Merkmale:

Medium	Kapazität	Vorteile	Nachteile
Festplatten	2–200 GByte und grösser	Grosse Kapazität, schneller Zugriff	Rotierender Lese- und Schreibkopf erhöht das Abnutzungsrisko
Magnetbänder	120 MByte bis 400 GByte und grösser	Grosse Kapazität, lange haltbar	Sequenzieller Zugriff
CD	650–700 MByte	Mittlere Kapazität, geringe Kosten	CD-Brenner erforderlich
DVD	4.7 GByte	Grosse Kapazität	DVD-Brenner erforderlich
USB-Datenträger	1 000 GByte und grösser	Keine Mechanik, rasche Übertragung, einfach verwendbar	Hoher Preis im Verhältnis zur Kapazität
Magneto Optical Disk	Bis 5 GByte	Vereinte Vorteile von magnetischen und optischen Speichermedien	Spezielles Gerät erforderlich

## 4 Welches Speichermedium wähle ich?

Die Wahl des Speichermediums ist von den Bedürfnissen des Unternehmens abhängig.  
Bei der Entscheidung müssen folgende Einflussfaktoren berücksichtigt werden:

Einflussfaktoren für Speichermedien



## 5 Arten der Datensicherung

Es gibt verschiedene Möglichkeiten, wie eine Datensicherung ausgeführt werden kann. In der Regel geben die Grösse des Unternehmens sowie die Grösse der Datenmenge die geeignete Option vor:

- Beim Einzelplatz-Backup wird ein Speichermedium direkt mit dem Computer verbunden und die Daten werden vom Computer direkt auf dieses Medium gesichert.
- Beim automatischen Backup steht ein System zur Verfügung, das den Austausch der Medien automatisch vornimmt.
- Beim LAN-Backup wird ausgehend vom Server rückwärts ein zweites, separates Netzwerk aufgebaut, auf dem die Sicherung durchgeführt wird. Dadurch können die Clients und Server im LAN wie gewohnt arbeiten und der Sicherungsrhythmus wird nicht von der Netzwerkbela stung im LAN bestimmt.
- Beim Storage Area Network (SAN) wird über Glasfaserkabel oder iSCSI ein ganzes Speichernetzwerk realisiert.
- Bei der Online-Datensicherung werden Daten via Internet transportiert und gesichert.
- Beim Backup als Cloud-Service werden die Daten durch einen externen Service Provider gesichert und bei Bedarf zur Verfügung gestellt.

## 6 Grosse Datenmengen sichern

---

Unternehmen haben i. d. R. sehr grosse Datenbestände, die aus technischen und finanziellen Gründen nicht immer mittels Voll-Backup gesichert werden können. Beispielweise würde der Voll-Backup aufgrund der grossen Datenmenge länger dauern, als Zeit zur Verfügung steht. Stattdessen können die Daten differenziell oder inkrementell gesichert werden.

Als Basis für eine differenzielle Datensicherung dient der Voll-Backup. Danach werden bei jeder differenziellen Datensicherung nur noch diejenigen Daten gesichert, die sich seit der letzten Volldatensicherung geändert haben.

Bei einer inkrementellen Datensicherung wird zuerst ebenfalls ein Voll-Backup durchgeführt. Danach werden nur noch diejenigen Dateien gesichert, die sich seit der letzten Voll-datensicherung bzw. seit der letzten inkrementellen Datensicherung geändert haben.

## 7 Wechselschema anwenden

---

Damit auf Datensicherungen möglichst lange zurückgegriffen werden kann, werden häufig folgende Wechselschemata eingesetzt.

- Grossvater-Vater-Sohn: Bei diesem Verfahren wird ein tägliches Set (Sohn), ein wöchentliches Set (Vater) und ein monatliches Set (Grossvater) an Speichermedien eingesetzt. So steht jederzeit eine Datensicherung zur Verfügung, die über ein Jahr zurückreicht.
- Turm von Hanoi: Dieses Verfahren wird verwendet, um einen guten Kompromiss zwischen der Anzahl der vorgehaltenen Datensicherungen und der zur Verfügung zu stellenden Hardware zu erreichen. Mit n Speichermedien kann man dabei  $2^n - 1$  Tage auskommen, bis das letzte Medium überschrieben wird. Somit hat man bei 3 Medien noch Backups von vor 4 Tagen, am 5. Tag wird der Backup C überschrieben. Bei 4 Medien hat man 8 Tage, bis am 9. Tag Medium D überschrieben wird, und bei 5 Medien hat man 16 Tage, bis am 17. das Medium E überschrieben wird, usw. Mit jedem zusätzlichen Set verdoppelt sich also der Zeitraum einer möglichen Rücksicherung von Daten.

## 8 Daten während des Systembetriebs sichern

---

In der Regel wird der Backup in der Nacht ausgeführt. Die Mitarbeitenden verändern jedoch konstant die Daten auf den Systemen. Würde nun eine Festplatte während des Tages ausfallen, so wären diese nicht auf dem Backup vorhanden. Aus diesem Grunde sollte neben einem Backup- und Restore-Konzept ebenfalls ein RAID-System betrieben werden.

RAID (Redundant Array of Independent Disks) sind mehrere unabhängige Festplatten, die zu einem logischen Laufwerk verbunden werden. Die Daten werden redundant gespeichert, d. h., sie werden so gespeichert, dass sie bei einem Hardwarefehler wiederhergestellt werden können. Die Benutzer greifen nun nicht mehr auf die einzelnen Festplatten zu, sondern auf das logische Laufwerk, das eine virtuelle Festplatte darstellt. Fällt eine Festplatte in diesem Verbund aus, werden die verlorenen Daten mittels der doppelt gespeicherten Daten der noch funktionierenden Festplatten rekonstruiert.

Gegen Stromausfälle empfiehlt es sich, eine unterbruchsfreie Stromversorgung (USV) anzuschaffen.

## 9 Zu sichernde Daten bestimmen

---

Für die Erstellung eines Datensicherungskonzepts muss zuerst bestimmt werden, welche Daten gesichert werden müssen. Dabei ist zu klären, wo sich die jeweiligen Daten befinden (**Speicherort**), wie umfangreich sie sind und wie sich der Datenbestand in absehbarer Zukunft voraussichtlich entwickelt. Um an diese Informationen zu gelangen, empfiehlt es sich, ein **Erhebungsformular** einzusetzen. Zur Vereinfachung der Datenerhebung stehen auch geeignete **Tools** zur Verfügung. Zudem lohnt es sich, die **Prioritäten des Restores** bereits in dieser Phase zu klären. Im Notfall kann man sich dann auf die rasche Wiederherstellung der Daten konzentrieren und muss sich nicht Gedanken darüber machen, welche Programme, Konfigurationen und Dateien in welcher Reihenfolge wiederhergestellt werden müssen.

## 10 Sicherungsmodalitäten festlegen

---

Bei der Festlegung der Sicherungsmodalitäten geht es darum, folgende Details für den Backup zu bestimmen:

- Wann? Hier wird der beste Zeitpunkt für den Backup bestimmt. Aufgrund der Arbeitszeiten und der Netzauslastung empfiehlt es sich, den Zeitpunkt auf die Nacht zu versetzen.
- Wie oft? Hier wird die Periodizität des Backups bestimmt. Zu diesem Zweck wird definiert, wie oft der Backup durchgeführt wird (z. B. stündlich, täglich, wöchentlich).
- Wie viele? Hier wird bestimmt, wie viele Sicherungen aufbewahrt werden sollen. Dabei wird definiert, wie viele unterschiedliche oder gleiche Speichermedien für die gleiche Datensicherung eingesetzt werden.

## 11 Speichermedien bestimmen

---

Jedes Speichermedium hat Vor- und Nachteile. Ein Medium mit nur Vorteilen existiert leider nicht. Magnetbänder z. B. haben den grossen Vorteil, dass sie lange Aufbewahrungszeiten garantieren. Hingegen ist der Zugriff sehr langsam. Im Netz verbaute Festplatten garantieren einen raschen Backup und einen ebenso effizienten Restore. Diese Festplatten lassen sich aber nicht so einfach in einen feuerfesten Tresor einschliessen. Die Kombination von verschiedenen Medien, sogenannter mehrstufiger Backup, ist daher eine gute Lösung. In der Praxis wird oftmals eine Kombination aus Festplatte und Magnetband eingesetzt.

## 12 Sicherungssoftware bestimmen

---

Die meisten Betriebssysteme verfügen über Funktionalitäten zur Sicherung von Daten, Programmen und Einstellungen. Um erweiterte Funktionen zu erhalten, ist die Beschaffung einer kommerziellen Sicherungssoftware in Betracht zu ziehen.

## 13 Aufbewahrung der Datenträger bestimmen

---

Bei der **Wahl des Lagerorts** für ein Speichermedium kommen **gesetzliche Aspekte** ins Spiel, die beachtet werden müssen. So ist z. B. der Zugang zu schützenswerten Daten gemäss Datenschutzgesetz auf berechtigte Personen zu beschränken. Datenträger, die zu Restore-Zwecken aus dem Lagerort entfernt werden, sind zu protokollieren. In diesem Fall hilft eine Nummerierung und Beschriftung der Speichermedien.

Weiter sind die unterschiedlichen **physikalischen Eigenschaften der Speichermedien** zu beachten. Während z. B. magnetische Datenträger keine Feuchtigkeit vertragen, macht dies optischen Datenträgern nichts aus.

## 14 Verantwortung für das Backup und Restore festlegen

---

Damit die Aufgaben der Datensicherung während des Systembetriebs gemäss Konzept effektiv wahrgenommen werden, müssen die **Rollen** und **Verantwortlichkeiten** im Unternehmen festgelegt werden. In der Praxis hat sich folgende Aufgabenteilung bewährt:

- Der **Datenowner** ist für die ihm zugeteilten Daten verantwortlich.
- Der **Systemowner** ist für den unterbrechungsfreien Betrieb seines Systems und für die Integration der darauf befindlichen Daten in einen Backup verantwortlich.
- Der **Backup-Verantwortliche** ist dafür verantwortlich, dass die Daten nach seinen Vorgaben gesichert werden.
- Der **Backup-Systemverantwortliche** ist für den ordentlichen physischen Betrieb des Backup-Systems verantwortlich.
- Der **Operator** führt den Backup und den Restore gemäss Konzept aus.
- Der **Qualitätsverantwortliche** ist für die Einhaltung der Backup-Qualität zuständig.

In kleinen Unternehmen können diese Rollen von einer einzigen Person wahrgenommen werden.

## 15 Notfallmassnahmen planen

---

Im Falle eines Notfalls muss rasch gehandelt werden können. Hierfür empfiehlt es sich, sich im Vorfeld bereits Gedanken zu einem Notfall zu machen und ein Notfallhandbuch zu erstellen. Das BSI stellt unterschiedliche Standards bzw. Vorlagen zur Verfügung, die aufgrund ihrer vordefinierten Struktur helfen, keine wichtigen Inhalte zu vergessen. In einem Notfallhandbuch sollten folgende Inhalte definiert werden:

- Sofortmassnahmen, um bei einem Notfall rasch handeln zu können, wird die komplette Alarmierung inklusive Kontaktpersonen festgehalten.
- Regelungen für den Notfall, es werden die Notfallverantwortlichen und die Notfallorganisation definiert.
- Wiederanlaufpläne für kritische Komponenten, es wird definiert, wie kritische Komponenten wiederbeschafft und installiert werden.
- Dokumentation, in diesem Kapitel wird bestimmt, welche Dokumentationen vorliegen müssen bzw. wo und mit welchem Inhalt diese abgelegt sind.

## **16 Backup- und Restore-System testen**

---

Jedes Backup- und Restore-System muss vor der Inbetriebnahme getestet und nach der Inbetriebnahme regelmässig daraufhin überprüft werden, ob es (noch) korrekt funktioniert. Die Vorbereitung und Durchführung solcher Tests kann in folgende Schritte gegliedert werden:

- 1.** Ziele des Tests festlegen
- 2.** Zeitpunkt des Tests festlegen
- 3.** Beteiligte über Testablauf informieren
- 4.** Test nach Testplan durchführen
- 5.** Testergebnisse dokumentieren









## Glossar

---

### A

<b>AIT</b>	AIT ist die Abkürzung für Advanced Intelligent Tape. Dabei handelt es sich um einen speziellen Typ von einem Magnetband.
<b>Alarmierungsplan</b>	Im Alarmierungsplan werden die zeitliche Reihenfolge sowie der Kanal (z. B. Telefon) der zu informierenden Personen definiert. Ebenso müssen Stellvertreter für den Fall einer Nichterreichbarkeit benannt sein.
<b>Archivierung</b>	Als Archivierung wird die Auslagerung nicht mehr angeforderter Daten bezeichnet. Bei der Archivierung werden im Gegensatz zum Backup die Originaldaten gelöscht.
<b>Ausweich-möglichkeiten</b>	Bei Ausfall vom Hauptsystem können die Mitarbeitenden auf anderen Systemen so lange arbeiten, bis das Hauptsystem wiederhergestellt wird.
<b>Autoloader</b>	Autoloader haben i. d. R. nur ein Bandlaufwerk und nur wenige Magnetbänder (8, 10 bis 16). Die Bänder sind ähnlich einem Karussell angeordnet. Mit der entsprechenden Software können so ohne manuelles Bandwechseln des Betreibers automatische Backups durchgeführt werden.

---

### B

<b>Backup</b>	Sicherheitskopie von Daten, um gegen Zerstörung oder unabsichtliche Löschung diese wiederherstellen zu können.
<b>Benutzerkontrolle</b>	Massnahme aus dem Datenschutz. Unbefugten Personen soll die Benutzung von Anlagen mit Personendaten verwehrt werden.
<b>Bit</b>	Abkürzung für «binary digit». Ein Bit kann nur zwei Werte annehmen. 1 oder 0.
<b>Blu-ray Disc</b>	Die Blu-ray Disc ist ein digitales optisches Speichermedium. Sie wurde als High-Definition-Nachfolger der DVD entwickelt und bietet ihrem Vorfänger gegenüber eine erheblich gesteigerte Datendichte und Speicherkapazität.
<b>Byte</b>	Eine Grundeinheit für Computerspeicher. 1 Byte sind 8 Bit.

---

### C

<b>CD-R</b>	CD-ROM, die nur einmal beschrieben werden kann.
<b>CD-RW</b>	CD-ROM, die mehrfach (bis 1 000x) beschrieben werden kann.

---

### D

<b>DAS</b>	Direct Attached Storage (DAS) oder Server Attached Storage bezeichnet an einen einzelnen Host angeschlossene Festplatten, die sich in einem separaten Gehäuse befinden.
<b>DAT</b>	DAT ist die Abkürzung für Digital Audio Tape. Dabei handelt es sich um einen speziellen Typ von einem Magnetband.
<b>Datenschutz</b>	Gesamtheit der gesetzlichen und betrieblichen Regelungen zum Schutz der Persönlichkeitsrechte vor Verletzung durch missbräuchliche Bearbeitung personenbezogener Daten.

<b>Datensicherheit</b>	Gesamtheit der Massnahmen, die zum Schutze der Daten vor Zerstörung, unbefugter Einsichtnahme und Veränderung, Diebstahl oder Verlust getroffen werden, um einen definierten Sicherheitsgrad zu erreichen.
<b>Datensicherung</b>	Datensicherung ist der Vorgang, Daten auf andere Speichermedien zu speichern. Dabei spielt es keine Rolle, ob diese Daten für einen Backup oder für die Archivierung gesichert wurden.
<b>Datensicherungsplan</b>	Im Datensicherungsplan wird festgehalten, wo die Datensicherungsmedien aufbewahrt sind und nach welchem Prinzip die Speichermedien angeschrieben sind.
<b>Datenträgerkontrollen</b>	Massnahme aus dem Datenschutz. Gesicherte Datenträger dürfen nachträglich nicht abgeändert werden oder sogar verloren gehen.
<b>DDS</b>	DDS ist die Abkürzung von Digital Data Storage. DDS bezeichnet den für den Computerbereich gültigen Standard für 4-mm-Bänder im DAT-Bereich. DDS wurde von den Firmen Hewlett Packard und Sony entwickelt.
<b>Differentielle Datensicherung</b>	Es werden grundsätzlich immer alle Dateien, die seit dem letzten Voll-Backup verändert wurden, gesichert. Diese Variante von Backup ermöglicht eine relativ schnelle Wiederherstellung der Daten. Es werden nur der letzte Voll-Backup und der letzte differenzielle Backup benötigt.
<b>Disaster Recovery</b>	Schnelle und einfache Wiederherstellung von Daten nach einem Systemausfall durch spezielle Datensicherung mit allen notwendigen Betriebssystemen und Anwendungsinformationen.
<b>DVD</b>	Abkürzung für Digital Versatile Disc (engl. für digitale, vielseitige Scheibe). Besitzt die gleiche Grösse wie eine CD, verfügt aber über 4.7 GByte Speicherplatz.

---

**F**

<b>Fibre-Channel- Technologie</b>	Glasfaserkabel, in dem per Licht die Datenübertragung erfolgt.
<b>Firewall</b>	Soft- oder Hardware zur Kontrolle der Zugriffe von fremden Benutzern auf innere Ressourcen.
<b>Flash-Speichermedien</b>	Dabei handelt es sich um kompakte, wiederbeschreibbare Speichermedium, auf dem beliebige Daten wie Text, Bilder, Audio und Video gespeichert werden können. Die Daten werden mittels der Flash-Speichertechnik gespeichert. Verwendet werden sie i. d. R. für kleine, mobile Geräte wie Digitalkameras oder Mobiltelefone.

---

**G**

<b>Gigabyte (GByte)</b>	Gigabyte = 1 024 MB = 1 073 741 824 Bytes
<b>Grossvater- Vater-Sohn</b>	Der Name für das Wechselschema von Speichermedien. Der Grossvater ist der monatliche Voll-Backup. Der Vater ist der wöchentliche Voll-Backup. Der Sohn ist der tägliche inkrementelle oder differenzielle Backup.

---

**H**

<b>Haltbarkeit</b>	Die Haltbarkeit sagt aus, wie lange die Daten auf einem Speichermedium ohne Verlust an Daten verfügbar sind. Besonders bei der Archivierung sind Medien mit langer Haltbarkeit zu wählen.
<b>HD</b>	Abkürzung für Harddisk = Festplatte

<b>Helical-Scan-Verfahren</b>	Als Schrägspräraufzeichnung, Schrägspurverfahren oder Helical Scan wird ein von Eduard Schüller erfundenes Verfahren zur Aufzeichnung von Signalen bei einem Videorekorder oder Bandlaufwerk bezeichnet. Im Gegensatz zur linearen Aufzeichnung wird die Spur schräg zum Band aufgezeichnet.
<b>Host</b>	Der Host-Rechner (Wirtrechner) ist in einem Datenverarbeitungssystem die zentrale Datenverarbeitungsanlage, auf der die grossen Anwendungsprogramme laufen und die die Datenbanken des Unternehmens verwaltet.

**I**

<b>Image</b>	Beim Image werden die Standardsoftware (Betriebssystem und Programme) und deren spezifische Einstellungen komplett gespeichert. Im Falle eines Notfalls kann das Image 1:1 auf die neue Festplatte übertragen werden und ist per sofort einsatzbereit.
<b>Inkrementelle Datensicherung</b>	Datensicherung, bei der nur Änderungen (Zuwachssicherung) aufgezeichnet werden, die seit der letzten vollständigen oder Zuwachssicherung durchgeführt wurden.
<b>iSCSI</b>	iSCSI (internet Small Computer System Interface) ist ein Verfahren, das die Nutzung des SCSI-Protokolls über TCP ermöglicht. iSCSI spezifiziert die Übertragung und den Betrieb direkter Speicherprotokolle nativ über TCP und erlaubt grosse Datenübertragungsraten.
<b>IT-Grundschutz</b>	Ziel des IT-Grundschutzes ist es, durch Standard-Sicherheitsmaßnahmen ein Sicherheitsniveau für IT-Systeme aufzubauen, das auch für sensiblere Bereiche ausbaufähig ist.

**K**

<b>Kapazität</b>	Die Menge der Daten, die auf einem Band bzw. mit einem Gerät gespeichert werden kann.
<b>KByte</b>	Kilobyte = 1 024 Bytes
<b>Konfiguration</b>	Unter Konfiguration versteht man die persönlichen Einstellungen von Benutzern. Dies können z. B. ein geänderter Bildschirmhintergrund oder Einstellungen im Office-Bereich sein.

**L**

<b>Laufwerkkosten</b>	Kosten für die Geräte, denen es Speichermedien erlaubt zu lesen bzw. zu beschreiben.
<b>Library</b>	Diese Bandsicherungsautomation ist eine Kombination von Robotertechnik mit mehreren Laufwerken und passender Software, die eine bestimmte Anzahl von Speichermedien ohne Eingriffe des Betreibers laden, entladen und auswechseln kann.
<b>Lizenz</b>	Zertifikat zur Benutzung einer Software.
<b>LTO</b>	Linear Tape Open. Aktuelle Datensicherungstechnologie für Bandlaufwerke, die entsprechend ihrer Entwicklung aufwärts nummeriert wird, von LTO1 bis aktuell LTO6.

**M**

<b>MByte</b>	Megabyte = 1 024 KB = 1 048 576 Bytes
<b>Meldeweg</b>	Der Meldeweg beschreibt, welche Personen auf welchem Weg und in welcher Reihenfolge im Falle eines Notfalls alarmiert werden müssen.

<b>MOD</b>	Magneto Optical Disk. Eine wiederbeschreibbare optische Speichertechnologie, die eine Kombination aus magnetischen und optischen Techniken darstellt. Die Daten werden mittels Laser und Magnetkopf auf die Disk geschrieben.
------------	---

---

**N**

<b>NAS</b>	NAS-Systeme (Network Attached Storage) sind externe Datenspeicher oder Fileserver mit integriertem Netzwerkanschluss, die unabhängig von den Applikationsservern im Netz arbeiten. NAS basiert auf einem integrierten Server mit einem schlanken, abgespeckten Betriebssystem.
<b>Notfallhandbuch</b>	Komplette Dokumentation, die im Falle eines Notfalls eingesetzt wird. Enthält unter anderem Sofortmassnahmen, allgemeine Organisationen und weitere Dokumentationen.
<b>RAID</b>	Redundant Array of Independent Disk. Verknüpfung einzelner Festplatten in einem Gehäuse, die an einen einzigen Controller angeschlossen sind. Dieser steuert die Schreib- und Leseaktivitäten des Systems, als wäre nur eine Festplatte existent (virtuelles Laufwerk). Die Speichermenge wird somit entsprechend der Anzahl der Festplatten erhöht.
<b>Redundant</b>	Doppelte Führung von Komponenten. Eine Komponente darf ausfallen, ohne das gesamte System zu beeinflussen.
<b>Restore</b>	Das Zurückspielen der Daten von den Sicherungsdatenträgern, die mittels Backup gesichert wurden.

---

**S**

<b>SAN</b>	Das Storage Area Network (SAN) ist ein Netzwerk zwischen Computern und Speichereinheiten.
<b>Server</b>	Ein leistungsstarker Computer, der von mehreren Benutzern oder Anwendungen gleichzeitig genutzt wird. In einigen Fällen erfüllen Sie Einzelaufgaben wie Druckserver, Internetzugang oder Dateiserver.
<b>Sofortmassnahmen</b>	Massnahmen, die sofort bei Eintreffen eines Notfalls ausgeführt werden müssen.
<b>Speichermedien</b>	Oberbegriff für alle Techniken und Typen, auf denen Daten gespeichert werden können.

---

**T**

<b>TByte</b>	Terabyte = 1 024 GB = 1 099 511 627 776 Bytes
<b>Turm von Hanoi</b>	Ein Rotationsschema für Speichermedien. Jedes Speicherset wird unterschiedlich oft genutzt.

---

**U**

<b>USV</b>	Die USV (unterbruchsfreie Stromversorgung) gleicht die Stärke der Stromversorgung aus und überbrückt bei einem totalen Stromausfall.
------------	--

---

**V**

<b>Voll-Backup</b>	Eine Kopie aller Informationen in einem System. Dabei wird der gesamte Dateninhalt auf externe Medien übertragen.
--------------------	---

---

## W

<b>Wechselschema</b>	Wechselschema sind Planungsabläufe, in denen die zu verwendenden Speichermedien definiert werden. Dabei wird berücksichtigt, dass der Zugriff auf ältere Versionen (z. B. Wochenbänder) gewährleistet wird.
<b>Wiederbeschaffungsmöglichkeit</b>	Damit teure Hardware nicht redundant beschafft werden muss, kann mit dem Lieferanten eine Wiederbeschaffungsvereinbarung getroffen werden. Diese beschreibt, dass eine rasche Lieferung von Hardwareersatz im Notfall ausgeführt wird.
<b>Wiederherstellpunkt</b>	Ein Wiederherstellpunkt ist eine Speicherung aller Einstellungen zu einem gewünschten Zeitpunkt. Im Notfall kann so auf einen gewünschten Punkt zurückgesprungen werden, um die Einstellungen wiederherzustellen.

---

## Z

<b>Zugangskontrolle</b>	Massnahme aus dem Datenschutz. Unbefugten Personen soll der Zugang zu Einrichtungen verwehrt werden.
<b>Zugriffskontrolle</b>	Massnahme aus dem Datenschutz. Zugriff auf Daten erhalten nur diejenigen Personen, die die Daten bei der Ausführung ihrer Arbeit benötigen.

## Stichwortverzeichnis

### A

Acronis	70
Advanced	27
Advanced Intelligent Tape	27
AIT	27
Alarmierungsplan	83
Arbeitszeiten	62
Archivierung	22, 59
ARCserve	70
Arkeia	70
Aufgabenbeschreibung	84
Autoloader	26
Automatischer Backup	39

### B

Backup- und Restore-Konzept	22
Backup- und Restore-System	22
BackupExec	70
Backup-Systemverantwortliche	76
Backup-Verantwortliche	76
Bandlaufwerken	26
Bauliche Massnahmen	15
BD	28
Bedrohungen	13
Beschaffungskosten	65
Besonders schützenswerte Daten	18
Betriebskosten	65
Block Striping	51
Blu-ray	28
Blu-ray Disc	28
BRD	28

### C

CD-R	28
CD-ROM	28
CD-RW	28
Cloud-Service	42
Cold Standby	85
Compact Flash (CF)	29

### D

DAS	25
DAT	27
Data Striping	50
Datenart	59
Datenerhebung	58
Datenerhebungsformular	58
Datenmenge	32
Datenowner	76
Datenschutzgesetz	18, 72
Datensicherung	20
Datensicherungsplan	86
Datenträgerbeschriftung	73
Datenträgerkontrolle	72
Datenträgerlagerung	74
Datenumfang	59
Datenwachstum	59
Dauerbetrieb	52
DDS	27
Dezentrale Ressourcen	86
Differenzielle Datensicherung	43
Digital Audio Tape	27
Digital Data Storage	27
Digital Linear Tape	27
Direct Attached Storage	25
Disaster Recovery	21
DLT	27
Dokumentation der Testergebnisse	90
Drive Duplexing	51
Drive Mirroring	51
DSG	18
DVD	28

### E

Einmalige Kosten	64
Einzelplatz-Backup	39

### F

Festplatte	25
Flash-Speichermedien	29

## G

GByte	32
Gebrauchsanleitung	86
Grossvater–Vater–Sohn	46

## H

Höhere Gewalt	13
Hot Standby	85

## I

Image	21
Inkrementelle Datensicherung	44
Integrit	17
Integrität	17

## K

KByte	32
Konfigurationseinstellungen	59
Kontaktinformationen	84
Kriminelle Handlung	14

## L

LAN-Backup	40
Library	26
Linear Tape Open	27
Lizenzen	59
LTO	27

## M

Magnetband	26
Magnetische Speichermedien	
• Beschreibung	24
Magneto Optical Disk	29
MByte	32
Mehrstufiger Backup	65
Meldeweg	83
Menschliches Versagen	14
Mitlaufbetrieb	52
MOD	29

## N

NAS	25
Network Attached Storage	25
Netzauslastung	62
Notfallhandbuch	81
Notfallmassnahmen	81
Notfallorganisation	85
Notfallverantwortliche	84
Notstandsregime	84

## O

Obligationenrecht	17
Offline-USV	52
Online-Datensicherung	41
Online-USV	52
Operator	76
Optische Speichermedien	
• Beschreibung	28
OR	17
Organisatorische Massnahmen	15
Originaldateien	59

## P

Periodizität	62
Personelle Massnahmen	15
Postloss	16
Preloss	16

## Q

Qualitätsverantwortliche	76
--------------------------	----

## R

RAID	50
RAID 0	50
RAID 1	51
RAID 5	51
RDX	24
Redundante Infrastruktur	85
Removable Disk Storage	24
Replikation	85
Restore	21
Rollen	76

## S

SAN	41
Schreibschutz	72
Secure Digital (SD)	29
Sicherungsbedarf	62
Sicherungsmodalitäten	62
Sicherungssoftware	68
Sofortmassnahmen	82
Spannungseinbruch	52
Spannungsspitze	52
Speicherdauer	33
Speichermedien	24
Speichermenge pro Sekunde	33
Speicherort	59
Standby-USV	52
Storage Area Network	41
Streng vertrauliche Daten	60
Systemowner	76

## T

TByte	32
Technische Massnahmen	15
Technisches Versagen	14
Testvorbereitung	90

## Testziele

89

## Turm von Hanoi

47

## U

Unterbruchsfreie Stromversorgung	52
USB-Datenträger	29
USB-Stick	29
USV	52

## V

VDSG	18
Verfügbarkeit	17, 59
Verordnung zum Datenschutzgesetz	18
Vertraulichkeit	17
Voll-Backup	43

## W

Wechselschema	46
Wiederbeschaffung	86
Wiederherstellungsdauer	33
Wiederkehrende Kosten	64

## Z

Zugriffsrechte	73
Zutrittskontrolle	72